AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

Seyfullayev İbrahim Əli oğlu

Həsənov Fərid Asəf oğlu

Xıdırova Sevda Elman qızı

Həsənov Kənan Zahid oğlu

Əliyev Yasin Aydın oğlu

VEB-SAYTLARDA BOŞLUQLARIN VƏ TƏHDİDLƏRİN AŞKARLANMASI VƏ QARŞISININ ALINMASI ÜSULLARI mövzusunda

MAGİSTRLİK DİSSERTASİYASI

İxtisas: **060632 – "İnformasiya texnologiyaları və sistemləri mühəndisliyi"**

İxtisaslaşma**: –"Kibertəhlükəsizlik (SABAH)"**

Elmi rəhbər: **tex.f.d. Babək Nəbiyev**

BAKI-2024

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

SABAH MƏRKƏZİ

MAGİSTRANTIN ANDI

"Veb-saytlarda boşluqların və təhdidlərin aşkarlanması və qarşısının alınması üsulları" mövzusunda təqdim etdiyimiz magistrlik dissertasiyasını elmi əxlaq normalarına və istinad qaydalarına tam riayət etməklə və istifadə etdiyimiz bütün mənbələri ədəbiyyat siyahısında əks etdirməklə yazdığımıza and içirik və magistrlik dissertasiyasının AzTU Kitabxana İnformasiya mərkəzində saxlanılması, həmin mərkəz tərəfindən AzTU Rəqəmsal Repozitoriyasına daxil edilərək repozitoriyanın veb saytında yerləşdirilməsinə icazə veririk.

Yasin Əliyev

Fərid Həsənov

Kənan Həsənov

Sevda Xıdırova

İbrahim Seyfullayev

Tarix

XÜLASƏ

İşin adı: Veb-Saytlarda Boşluqların Və Təhdidlərin Aşkarlanması Və Qarşısının Alınması Üsulları

Bu magistr dissertasiya işində veb-saytlarda boşluqların və təhdidlərin aşkarlanması və qarşısının alınması üsulları ilə bağlı məsələlər müzakirə olunmuşdur və əsas diqqət veb-saytlardakı boşluqların və təhdidlərin aşkarlanması və qarşısının alınması modellərin yaradılmasına yetirilir. İşdə qarşıya qoyulmuş bir neçə məsələ istiqamətində tədqiqatlar aparılmaqla aşağıdakı nəticələrlə yekunlaşmışdır:

- Veb-sayt və veb əsaslı platformalar analiz edilmişdir.
- Veb-saytlarda və platformalarda kibertəhlükəsiz konsepsiyası analizi edilmişdir.
- Vebdə mövcud boşluqlar və təhdidlərin analizi aparılmışdır.
- Vebdə mövcud boşluqlar və təhdidlərin aşkarlama metodları araşdırılmışdır.
- Aşkarlama alətlərinin analizi ,müqayisəli təhlili və qiymətləndirilməsi aparılmışdır.
- Veb təhdidlərin qarşısının alınması üçün mövcud modellərin işləmə prinsipi araşdırılmışdır.

SUMMARY

Title of work: Methods for Detecting and Preventing Vulnerabilities and Threats in Websites

In this master's thesis, issues related to methods of detection and prevention of vulnerabilities and threats in websites are discussed, and the main focus is on creating models for detection and prevention of vulnerabilities and threats in websites. Researches were carried out in the direction of several issues and concluded with the following results:

- Website and web based platforms were analyzed.
- Analyzed the concept of cyber security on websites and platforms.
- An analysis of existing web gaps and threats was carried out.
- Methods of detection of vulnerabilities and threats on the web were investigated.
- The analysis, comparative analysis and evaluation of detection tools was carried out.
- The working principle of the existing models for the prevention of web threats has been investigated.

MÜNDƏRİCAT

İXTİSARLARIN SİYAHISI

AES	Advanced Sncryption Standard - *Qabaqcıl şifrələmə standartı*
API	Application Programming Interface - *Tətbiq proqramlaşdırma interfeysi*
CDN	Content Delivery Network - *Məzmun çatdırılma şəbəkəsi*
CLF	Common Log Format - *Ümumi jurnal formatı*
CRLF	Carriage Return and Line Feed
CRS	Core Rule Set - *Əsas qaydalar dəsti*
CSRF	Cross-Site Request Forgery - *Saytlararası sorğuların saxtalaşdırılması*
CSP	Content-Security-Policy - *Məzmun Təhlükəsizlik Siyasəti*
DAST	Dynamic Application Security Testing – *Dinamik proqram təhlükəsizliyi testi*
DDoS	Distributed Denial of Service – *Paylanmış xidmətdən imtina*
DFARS	Defense Federal Acquisition Regulation Supplement - *Müdafiə üçün federal satınalma qaydalarına əlavə*
DNS	Domain Name System - *Domen adı sistemi*
FAR	Fuzzy Association Rule-based - *Qeyri-səlis assosiativ qaydalara əsaslanmış*
FISMA	Federal Information Security Management Act – *İnformasiya təhlükəsizliyinin idarə edilməsi haqqında federal qanun*
HİPPA	Health Insurance Portability and Accountability Act - *Tibbi sığorta daşınabilərlik və hesabatlılıq Qanunu*
HTML	HyperText Markup Language – *Hiper mətin işarələnmə dili*
HTTP	HyperText Transfer Protocol – *Hiper mətinlərin ötürülməsi protokolu*
HTTPS	Hypertext Transfer Protocol Secure
XML	Extensible Markup Language - *Genişləndirilə bilən işarələmə dili*

XSS	Cross-Site Scripting – *Saytlararası skript*
IDP	İntrusion Detection and Prevention - *Müdaxilənin aşkarlanması və qarşısının alınması*
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IDS	İntrusion Detection Systems - *Müdaxilənin aşkarlanması sistemləri*
LDAP	Lightweight Directory Access Protocol - *Sadələşdirilmiş kataloq giriş protokolu*
NIST	National Institute of Standards and Technology Cybersecurity Framework
OWASP	Open Web Application Security Project - *Açıq veb tətbiq təhlükəsizliyi layihəsi*
PBAC	Policy-based Access Control - *Siyasətə əsaslanan girişə nəzarət*
RBAC	Role-based Access Control - *Rola əsaslanan girişə nəzarət*
RCE	Remote code execution – *Uzaqdan kod icrası*
SQL	Structured Query Language – *Strukturlaşdırılmış sorğu dili*
SSRF	Server-Side Request Forgery - *Server tərəfində sorğuların saxtalaşdırılması*
SSL/TLS	Secure Sockets Layer/Transport Layer Security
URFDS	Unvalidated Redirects and Forwards Detection System – *Etibarsız yönləndirmə və aşkarlama sistemi*
URL	Uniform Resource Locator
VAPT	Vulnerability Assessment & Penetration Testing - *Zəifliklərin qiymətləndirilməsi və nüfuz testi*
WAVSEP	Web Application Vulnerability Scanner Evaluation Project - *Veb tətbiq zəifliklərinin skanerinin qiymətləndirilməsi layihəsi*
WWW	World Wide Web - *Ümumdünya şəbəkəsi*

GİRİŞ

Mövzunun aktuallığı. Veb-saytlardan istifadənin geniş yayılması və informasiya texnologiyalarının sürətli inkişafı ilə birlikdə saytlardakı təhlükəsizlik boşluqları və potensial təhdidlərin artması, bu sahədə aparılan tədqiqatların və həll təkliflərinin əhəmiyyətini artırır. Bu məqamda veb saytlarda mövcud olan təhlükəsizlik boşluqlarının müəyyən edilməsi və onların effektiv şəkildə həll edilməsi aktual bir tədqiqat mövzusu kimi özünü göstərir. Bu proses, internetdə məlumat mübadiləsinin və digər fəaliyyətlərin artması ilə birləşərək, təhlükəsizlik prinsiplərinin və texnologiyalarının davamlı olaraq yenilənməsini və inkişaf etdirilməsini tələb edir.

Tədqiqatın məqsədi və məsələləri. Tədqiqatın məqsədi, veb-saytlar və veb əsaslı platformaların kibertəhlükəsizlik risklərinin araşdırılması, mövcud boşluqların müəyyənləşdirilməsi və kibertəhlükələrin qarşısını almaq üçün effektiv həllər təklif etməkdir. Bu məqsədə nail olmaq üçün qarşıya aşağıdakı məsələlər qoyulmuşdur:

1. Veb-saytlar və veb əsaslı platformaların texnoloji prinsiplərinin araşdırılması;
2. Veb əsaslı platformaların təhlükəsizlik analizinin aparılması;
3. Veb-saytlar və platformaları əhatə edən mümkün hücum ssenarilərinin və təhdidlərin analizi;
4. Kibertəhlükələrin qarşısının alınması üçün müasir müdafiə mexanizmlərinin işlənməsi;
5. Veb hücumların qarşısının alınması üçün öyənmə modellərinin analizi;

Tədqiqatın obyekti və metodikası. Bu dissertasiya işindəki tədqiqat veb-saytlar və veb əsaslı platformalar üzərində mövcud olan kibertəhlükəsizlik problemlərinin araşdırılması ilə bağlı təkmilləşdirilmiş bir analitik perspektiv təmin edir. Tədqiqatın məqsədi, bu platformaların məlumat təhlükəsizliyi ilə əlaqədar potensial zəiflikləri və təhlükələri müəyyənləşdirmək və daha sonra bu təhlükələrin səviyyəsini qiymətləndirməkdir. Bu məqsədə nail olmaq üçün, tədqiqatda SQL inyeksiyası (ing. İnjection), əmr (ing. Command) inyeksiyası və zərəli kod yeritmə texnikaları kimi müxtəlif metodlar istifadə olunmuşdur.

Tədqiqatın elmi yeniliyi və praktik əhəmiyyəti. Bu dissertasiya işi, veb-saytlar və veb əsaslı platformalarda informasiya təhlükəsizliyinin yaxşılaşdırılmasında istifadə edilə bilər. Təklif olunan həllər və metodlar praktiki olaraq tətbiq edilərək kibertəhlükəsizlik səviyyəsinin artırılmasına kömək edə bilər.

Dissertasiya işinin strukturu: Dissertasiya işi giriş, dörd fəsil, nəticə və 37 ədəbiyyat mənbəyindən ibarət olmaqla 99 səhifədən təşkil olunmuşdur.

Birinci fəsildə, veb-saytlar və veb əsaslı platformaların strukturu, funksionallığı və kibertəhlükəsizlik anlayışı araşdırılmışdır.

İkinci fəsildə, veb-saytlar və platformalarda mövcud olan zəifliklər və təhdidlər analiz edilmiş,veb hücum metodlarının növlərinə geniş aspektdə nəzər salınmışdır. Kritik infrastrukturları əhatə edən hücumlar və onların təsirləri elmi əsaslarla təhlil edilmişdir.

Üçüncü fəsildə, kiber təhdidlərin aşkarlanması üsulları müzakirə olunmuşdur. Bu bölmə, müxtəlif təhlükəsizlik tədbirləri və strategiyaların təsvirini təqdim edərək, kiber hücumların aşkar edilməsi üçün effektiv həll yollarını göstərəcəkdir.

Dördüncü fəsildə, kiber təhdidlərin qarşısının alınması üsulları araşdırılmışdır. SQLI, XSS və RCE kimi hücum növlərinin qarşısının alınması üçün metodlar işlənib hazırlanmışdır.

Magistrantların dissertasiyada gördüyü işlər: Dissertasiya işinin birinci fəsli ümumi olaraq, Veb saytlarda və platformalarda kibertəhlükəsizlik anlayışından ibarətdir. **Həsənov Kənan Zahid oğlu və Xıdırova Sevda Elman qızı** tərəfindən yazılmışdır.

Dissertasiya işinin ikinci fəsli Veb-saytlardakı, platformalardakı boşluqlar və təhdidlərin araşdırılmasından ibarətdir. **Həsənov Fərid Asəf oğlu** tərəfindən yazılmışdır.

Dissertasiya işinin üçüncü fəsli Veb-saytlarda, platformalarda mövcud olan boşluqların və təhdidlərin aşkarlanması üsullarından ibarətdir. **Əliyev Yasın Aydın oğlu, Xıdırova Sevda Elman qızı** tərəfindən yazılmışdır.

Dissertasiya işinin dördüncü fəsli Mövcud Boşluqların və Təhdidlərin Qarşısının alınması Modeli haqqındadır. **Seyfullayev İbrahim Əli oğlu** tərəfindən yazılmışdır

FƏSİL I VEB-SAYTLARDA KİBERTƏHLÜKƏSİZLİYİN TƏMİN OLUNMASI SAHƏSİNDƏ AKTUAL MƏSƏLƏLƏR

1.1 Veb-sayt və veb əsaslı platformalar

Veb-sayt, internet üçün nəzərdə tutulmuş, ən azı bir hiperkeçiddə malik olan, xüsusi format olunmuş və özündə mətn, qrafika, istinadları və animasiyaları göstərən sənəddir. Veb-sayt yalnız internet üzərində işləyən bir servisdir. Hər bir sayt ən azı bir serverdə yerləşdirilmiş faylların bir-biri ilə əlaqələndirilməsindən yaradılmış bir qovluqdur. Saytlara internet şəbəkəsi vasitəsilə baxmaq imkanı yaradılır və beləliklə informasiya mübadələsini qat-qat asanlaşdırılmış olur (Benson V, Saridakis G, Tennakoon H, Ezingeard JN ,2015).

Vebsaytın yaradılması prosesi

Vebsaytın yaradılması mürəkkəb və vaxt aparan prossesdir. Ona görə bu prossesi asanlaşdırmaq üçün onun necə işlədiyini tam anlamaq lazımdır. Ümumi olaraq bu prossesi 9 mərhələyə ayırmaq olar:

1. Planlaşdırma və analiz
2. Dizayn
3. Front-end
4. Back-end
5. Server tənzimlənməsi
6. Test və sınaq
7. Optimizasiya və təkmilləşdirmə
8. Deployment
9. Dəstək və baxım

Aşağıdakı blok-sxem bütün prossesinin gedişatını özündə ehtiva edir **şək.1.1.1**.


Planlaşdırma və Analiz
Müştəri ilə görüş
Tələblərin müəyyənləşdirilməsi
Hədəf kütlənin müəyyənləşdirilməsi
Görünüş tələblərinin müəyyənləşdirilməsi
Planlaşdırma və analiz prosesinin nəticəsi, veb saytının məqsəd və tələblərinin doğru anlaşılması və təyin edilməsidir. Bu mərhələ, veb saytının inkişafının digər addımlarına yönəlmiş doğru bir temel qoyur.
Dizayn
Wireframe və Mockupların Yaradılması
Dizayn elementlərinin seçilməsi
UI/UX Dizaynı
Prototipin yaradılması
Dizayn prosesi, veb saytının görsəl tərəfinin müştərilərin tələblərinə uyğun olaraq hazırlanmasını və məqsədlərinə cavab verəcək şəkildə işləməsini təmin edir. Bu mərhələ, veb saytının inkişafında kritik əhəmiyyətə malikdir və müştərilər üçün ən yaxşı təcrübəni təmin etmək üçün yaxşı hazırlanmalıdır.
Front-end
HTML (HyperText Markup Language)
JavaScript
CSS (Cascading Style Sheets)
Responsive Design
Frameworklar və kitabxanalar
Front-end prosesi, veb saytının istifadəçilərə görsəl olaraq cazibəli və effektiv şəkildə təqdim edilməsini təmin edir. Bu mərhələ, veb saytının istifadəçilər tərəfindən rahat və effektiv şəkildə istifadə edilməsini və müştərilərə yaxşı bir təcrübə təmin etməsini təmin edir.
Back-end
Proqramlaşdırma dilləri
PHP, Python, Ruby, Java, Node.js,C#,C++
Database
MySQL, PostgreSQL, MongoDB, SQLite
API (Application Programming Interface) İstifadəsi
Optimizasiya və performans
Back-end inkişafı, veb saytının düzgün və effektiv şəkildə işləməsini təmin edir və istifadəçilərin müraciət etdikləri funksionallığı təmin edir. Bu proses, veb saytının arxa tərəfindəki texniki strukturu və funksionalını idarə edir və veb saytının qlobal işləməsini təmin edir.
Server Tənzimlənməsi
Server seçimi
Programlaşdırma dilinin quraşdırılması
Əməliyyat sistemi quraşdırılması
Verilənlər bazası serverinin quraşdırılması
Web Server Quraşdırılması
Serverin təhlükəsizliyini təmin etmək
firewall, antivirus proqramları, yamaqları
Təhlükəsizlik
Server tənzimlənməsi, veb saytınızın performansını və təhlükəsizliyini təmin etmək üçün əhəmiyyətli bir mərhələdir. Bu proses, serverin düzgün işləməsini və istifadəçilərin müraciət etdikləri zaman effektiv şəkildə cavab verməsini təmin edir.

Şək.1.1.1 Veb saytların hazırlanması prosseslərinin blok-sxemi (İbrahim Seyfullayev, 2024)

Veb Hostinq

Veb hostinq, veb-saytınızı təşkil edən fayllar üçün yaddaş təmin edən bir xidmət olub veb-saytınızı internetdəki digər istifadəçilər üçün əlçatan edən

proqram təminatı, fiziki avadanlıq və şəbəkə infrastrukturudur.

Ümumi hostinq seçimləri

Paylaşılan hostinq (ing. Shared hosting)

Birgə yerləşdirildikdə, hostinq provayderi veb-saytınızı və bir neçə digər (kirayəçiləri) eyni kompüterə yerləşdirir—prosessor, yaddaş, saxlama sahəsi və veb server proqramını (veb məzmunu tələb edən brauzerlərə çatdıran proqram) paylaşırsınız.

Bu mənbələri digər veb-saytların sahibləri ilə paylaşdığınız üçün onlar üçün daha az pul ödəyirsiniz. Bununla birlikdə, paylaşılan bir kompüter ümumiyyətlə çox güclü olsa da, yerləşdirilən saytlardan birinə gözlənilmədən yüksək trafik digər mənbələri ləğv edə və əhəmiyyətli dərəcədə ləngidə bilər. Ayrıca, bir sayt bir virusun və ya təhlükəsizlik hücumuna məruz qalırsa, serverdəki digər saytlar həssas ola bilər. Paylaşılan hostinq şəxsi veb-saytlar, şəxsi bloglar, kiçik əməliyyat olmayan iş saytları (şəxsi portfel kimi) və ya qeyri-iş saytları üçün yaxşı bir seçimdir.

Virtual şəxsi server əsaslı Hostinq (ing. Virtual private server, VPS) və ya bulud əsaslı VPS (ing. Cloud-based VPS)

VPS hostinq istifadə edərkən veb-saytınız öz xüsusi virtual serverini alır. Virtual hostinqdə olduğu kimi, siz bir kompüterin aparat resurslarını birlikdə istifadə edirsiniz (əksər hallarda), lakin siz onları daha az digər istifadəçilərlə istifadə edirsiniz və onların problemləri - təhlükəsizlik pozuntuları, nasazlıqlar, saytınıza təsir etmək ehtimalı daha azdır.

VPS ilə əməliyyat Sisteminiz, CMS və digər proqram təminatı üzərində tam nəzarət əldə etməyə verir, bu da onu xüsusi veb proqramlarda yerləşdirmək üçün ən yaxşı seçim edir. Yəqin ki, təxmin etdiyiniz kimi, VPS paylaşılan hostinqdən daha bahalıdır.VPS Hostinq resursları daha az veb-sayt arasında bölüşdürsə də, hər bir sayt böyüdükcə və daha çox trafik cəlb etdikcə, onlar bir kompüterin resurslarını çox yükləyə bilərlər. Bu səbəbdən bir çox hostinq provayderi, hər bir saytın bir məlumat mərkəzində (və ya hətta fərqli coğrafi yerlərdə) birdən çox kompüterin birləşdirilmiş mənbələrindən istifadə etdiyi bulud əsaslı VPS hostinq təklif edir. Bu, hesablama gücünü, saxlama qabiliyyətini və bant genişliyini lazım olduqda ölçməyi asanlaşdırır

və aparat nasazlıqları və ya təbii/texnogen fəlakətlər zamanı əlavə nasazlıq problermlərinin həllini təmin edir.VPS və ya bulud əsaslı VPS hostinq əksər iş saytları üçün idealdır.

Xüsusi hostinq (ing. Dedicated hosting)

Xüsusi hostinq sizə öz veb serverinizin aparatına əlavə giriş imkanı verir. VPS istifadə etdiyiniz sistem və tətbiq proqramı üzərində eyni nəzarəti əldə edirsiniz, ancaq saytınız aparatdan istifadə edən yeganə sayt olduğundan daha sürətli işləyir. Digər veb-saytlardakı performans və ya təhlükəsizlik problemlərindən də tamamilə qorunursunuz.

Virtual şəxsi server hostinq (ing. Virtual Private Server Hosting, VPS Hosting)

Bir fiziki serverdə bir neçə virtual server yaradılır.

Vasitəçi hostinq (ing. Reseller Hosting)

Hostinq şirkətlərindən hostinq resurslarını alaraq başqalarına satır.

WordPress Hosting

Xüsusi olaraq WordPress saytları üçün optimallaşdırılmış hostinq xidmətləri aşağıdakılardır:

Menecment hostinq (ing. Managed Hosting)

Menecment Hostinq,yüksək səviyyəli hostinq xidmətidir, burada hostinq təminatçısı serverin idarə olunmasını və texniki dəstəyini üzərinə götürür.

Kolokasiya Hosting (ing. Colocation Hosting)

Müştəri öz serverini bir data mərkəzinə yerləşdirir və həmin mərkəzin resurslarından istifadə edir.

E-poçt hostinq (ing.Email Hosting)

Müəyyən bir domen üçün e-poçt xidmətləri təqdim edir.

Fayl ötürmə protokolu hostinqi (ing. File Transfer Protocol Hosting, FTP Hosting)

Fayl ötürmə protokolu vasitəsilə fayl yükləmə və paylaşma üçün optimallaşdırılmış hostinq xidmətidir.

2024-cü ildə 10 ən yaxşı veb hostinq xidmətləri bunlardır:

HostGator: "Hamısı bir yerdə" hostinq paketləri arasında ən yaxşısı

Bluehost: yeni veb-saytlar üçün ən yaxşısı

DreamHost: təcrübəsiz istifadəçilər üçün ən yaxşısı

Inmotion hosting: veb-sayt performansını artırmaq üçün ən yaxşısı

IONOS: istifadə rahatlığı üçün ən yaxşısı

Hostwinds: təhlükəsizlik baxımından ən yaxşısı

MochaHost: mövcud saytları köçürmək üçün ən yaxşısı

GoDaddy: sadə bir veb-sayt qurmaq üçün ən yaxşısı

InterServer: limitsiz saxlama üçün ən yaxşı həll

TMDHosting: sürətli böyüyən biznes üçün ən yaxşısı

Dünya üzrə ən çox istifadə olunan 5 ən yaxşı hostinqləri sıralasaq, birinci yerdə **Paylaşılan hostinqin** olduğunu görərik. Paylaşılan hostinq, birdən çox istifadəçinin eyni server resurslarını paylaşdığı bir hostinq növüdür. Bu, yeni başlayanlar və kiçik veb saytlar üçün idealdır çünki, texniki bilik tələb etmir.

VPS hostinq isə daha yüksək performans və özəlliklər tələb edən istifadəçilər üçün nəzərdə tutulmuşdur. VPS hostinqdə, hər bir istifadəçi virtual olaraq özəl bir serverin bir hissəsini idarə edir, bu da paylaşılan hostinqə nisbətən daha çox resurs və daha yüksək performans təmin edir. VPS hostinq, orta və iri miqyaslı veb saytlar və tətbiqlər üçün uyğundur və istifadəçilərə kök səviyyəsində giriş imkanı verir.

Bulud Hostinq isə genişlənə bilən və etibarlı bir hostinq növüdür. Bulud hostinq birdən çox serverin resurslarını birləşdirərək, istifadəçilərə yüksək keyfiyyət və genişlənilə bilənlik təklif edir. Bu hostinq növü, trafik dalğalanmaları olan veb saytlar və tətbiqlər üçün ideal seçimdir, çünki resurslar ehtiyac duyulduqda avtomatik olaraq artırıla bilər. Bulud hostinq, həmçinin məlumatların təhlükəsizliyini və davamlılığını artırır.

Dedicated Server Hosting isə tamamilə bir istifadəçiyə məxsus fiziki server təklif edir. Bu hostinq növü, yüksək performans, təhlükəsizlik və özəlliklər tələb edən iri müəssisələr və yüksək trafikli veb saytlar üçün nəzərdə tutulub. Dedicated server hosting istifadəçilərə server üzərində tam nəzarət imkanı verir və resurslar tamamilə həmin istifadəçiyə aiddir.

WordPress Hosting isə xüsusilə WordPress platformasında işləyən veb saytlar üçün optimallaşdırılmış bir hostinq növüdür. WordPress hostinq, WordPress-in spesifik tələblərinə uyğunlaşdırılmış server konfiqurasiyaları və xüsusiyyətlər təqdim edir. Bu, performansın artırılması və təhlükəsizlik tədbirlərinin gücləndirilməsi üçün optimallaşdırılmışdır. WordPress istifadəçiləri üçün asan idarəetmə və avtomatik yeniləmələr təklif edir, bu da istifadəçilərin texniki işlərlə məşğul olmasını minimuma endirir.

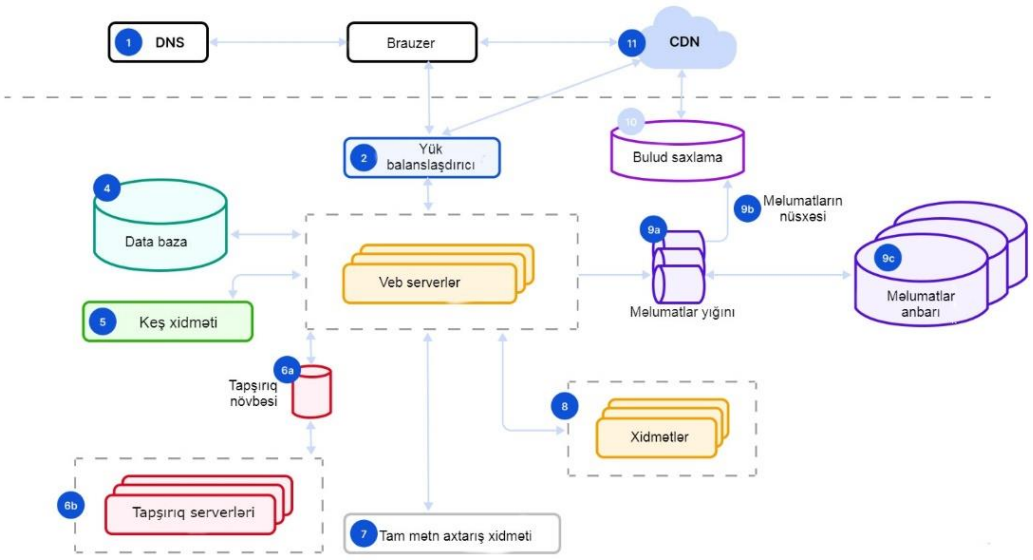
Veb tətbiq arxitekturası

Veb tətbiq arxitekturası, onun komponentləri arasındakı qarşılıqlı əlaqə modelidir. Xüsusi bir veb tətbiq arxitekturası, tətbiqin məntiqinin müştəri və server tərəfləri arasında necə paylanacağından asılıdır. Texniki olaraq, elementlərini, verilənlər bazalarını, sistemlərini, serverlərini, interfeyslərini və aralarında baş verən bütün rabitələri özündə birləşdirən bir veb tətbiqetmə çərçivəsidir. Daha mücərrəd baxımdan, müştəri və server sorğularına cavabların arxasındakı məntiqi göstərir.

Ən yaxşı veb tətbiq arxitekturasını seçərkən nəyi seçəcəyimizə qərar vermək çətin ola bilər, çünki müasir veb tətbiqetmələrin inkişafı üçün təsvir olunan bir çox fərqli veb arxitekturası və metodu mövcuddur. Hansı həll növünü seçməlisiniz və hansı hallarda bir alternativ digərindən daha yaxşıdır? Veb tətbiqetmə arxitekturasının ümumi problemi təhlükəsizlik, performans, texniki xidmət, dəstək, dizayn, inteqrasiya, xərc və test, genişləndirilə bilmək kimi məsələləri necə idarə etməkdir.. Məqsədlərə və ya tələblərə uyğun olan düzgün arxitekturanı seçmək çox vacibdir **şək.1.1.2**.

Veb tətbiqləri yaratmaq üçün statik veb saytlar, SSG, SSR , SPA, PVA kimi müxtəlif növ veb tətbiq arxitekturası var və hamısının öz müsbət və mənfi cəhətləri var.Veb tətbiqi arxitekturasının komponentləri. Tətbiqin o qədər sadə olması ola bilər ki, bütün veb tətbiq arxitekturasını bir yerdə saxlayaraq monolit kimi işləyir.

Veb tətbiqin arxitetkurasının sxemi:Komponentlərin və aralarındakı qarşılıqlı əlaqələrin sxematik təsvirini təqdim edir.



Şək.1.1.2 Veb tətbiq arxitekturası

1. DNS: DNS qısaltması domen adlar sistemi deməkdir. IP ünvanlarını domen adları ilə uyğunlaşdıran əsas elementdir. Beləliklə, müəyyən bir server son istifadəçi tərəfindən göndərilən bir sorğu alır.

2. Yük balanslaşdırıcısı: Tətbiq istifadəçilərindən gələn istəkləri bir neçə serverdən birinə yönəldir və eyni zamanda çox sayda istifadəçi aktiv olduqda yükü daha bərabər paylamağa imkan verir. Ümumiyyətlə, veb tətbiqetmə xidmətləri bir-birini əks etdirən müxtəlif nüsxələr şəklində mövcuddur ki, bu da bütün serverlərin sorğuları eyni şəkildə idarə etməsinə imkan verir. Bundan əlavə, yük balanslaşdırıcısı tapşırıqları həddindən artıq yüklənməməsi üçün paylayan elementdir.

3. Veb Tətbiq Serverləri: Veb tətbiqetmə serverləri istifadəçi istəklərini idarə etmək, tətbiq məntiqini yerinə yetirmək və dinamik məzmun yaratmaq üçün verilənlər bazası ilə qarşılıqlı əlaqə yaratmaq məqsədi ilə hazırlanmışdır.

Serverlər veb brauzer və tətbiqin arxa hissəsi arasında əlaqə təmin edir. Yaradılan məzmunu göstərmək üçün brauzerə geri göndərirlər və istifadəçilərin tətbiqlə problemsiz qarşılıqlı əlaqə qurmasına imkan verirlər.

Veb tətbiq serverlərinin ümumi nümunələrinə Apache Tomcat, Nginx və Microsoft Internet Information Services (IIS) daxildir.

4. Verilənlər bazası: Verilənlər bazası, proqramın sorğulara cavab vermək, proqrama daxil ola bilmək üçün kompüterdə saxlanılan strukturlaşdırılmış qeydlər və ya məlumatlar toplusudur. Sorğularla əldə edilən qeydlər qərar qəbul etmək üçün istifadə edilə bilən məlumatlara çevrilir. İstəklərin yerinə yetirilməsi, məlumatların bütövlüyünün qorunması və ya dəyişən ehtiyaclara uyğun miqyaslandırılması olsun, verilənlər bazaları müasir veb tətbiqetmələrin düzgün işləməsi üçün çox vacibdir.

Veb tərtibatçıları tez-tez strukturlaşdırılmış məlumat anbarı ilə tanınan MySQL və PostgreSQL kimi əlaqəli verilənlər bazaları ilə strukturlaşdırılmamış məlumatlar üçün rahatlıq təmin edən MongoDB kimi NoSQL verilənlər bazaları arasında seçim edirlər.

5. Keşləmə xidməti: Keşləmə xidmətinin əsas funksiyası tez-tez istifadə olunan məlumatların axtarışını saxlamaq və sürətləndirməkdir. İstifadəçilər serverdən məlumat istədikdə, bu əməliyyatların nəticələri keşə alınır və eyni məlumatlar üçün sonrakı sorğuların daha sürətli işlənməsinə imkan verir.

Əsasən, keşə alma əvvəlki nəticələrə istinad edərək performansı əhəmiyyətli dərəcədə artırır, bu da hesablamaların yavaş və ehtimal ki, tez-tez aparıldığı ssenarilərdə xüsusilə faydalıdır.

6. İş Növbəsi (Ümumi): İki komponentə malikdir: iş növbəsi və bu işləri idarə edən serverlər. Bir çox veb server kiçik əhəmiyyət kəsb edən çox sayda işi yerinə yetirir. Tamamlanması lazım olan tapşırıq növbəyə qoyulur və cədvələ uyğun olaraq yerinə yetiriləcəkdir. Bu mütəşəkkil sistem veb serverlərə daha az vaxt aparan işlərin sistematik işlənməsində kritik əməliyyatların prioritetliyini təmin edərək çoxsaylı tapşırıqları səmərəli idarə etməyə imkan verir.

Beləliklə, iş növbəsi veb serverin ümumi səmərəliliyinə və səmərəliliyinə töhfə verən server resurslarının paylanmasını optimallaşdırmaq üçün strateji bir mexanizm rolunu oynayır.

7. Tam Mətn Axtarış Xidməti (Ümumi): Mətn axtarış funksiyasını dəstəkləyən bir çox veb tətbiqetmə var. Bundan sonra tətbiq müvafiq nəticələri son

istifadəçiyə göndərir. Bütün proses tam mətn axtarışı adlanır və sistemdə mövcud olan bütün sənədlər arasında tələb olunan açar söz məlumatlarını tapa bilər.

8. CDN: CDN qısaltması məzmun çatdırılma sistemi deməkdir. Bu sistem şəkillər və digər sənədlər daxil olmaqla statik məzmun göndərir. Əsasən, tətbiqin verilənlər bazasından daha çox son istifadəçilərin coğrafi mövqeyinə yaxın olan bir neçə server daxildir. Nəticədə, CDN bütün dünyada istifadəçilərə məzmun təqdim etməkdə daha səmərəlidir və yükləmə müddətini xeyli azaldır.

1-tier - Tək səviyyəli arxitektura olaraq da bilinən 1 səviyyəli arxitektura, tətbiqin işləməsi üçün lazım olan bütün komponentlərin bir paketdə mövcud olduğu bir proqram arxitekturasına aiddir. Bu o deməkdir ki, istifadəçi interfeysi, tətbiq, təbəqələr eyni yerli sürücü altında tətbiq tərəfindən əldə edilə bilər. Həm müştəri, həm də server eyni maşında yerləşir. İstifadə olunan ən sadə proqram arxitekturasıdır. Lakin bu səviyyə veb tətbiqi üçün uyğun deyil. Çünki o, yalnız bir kompüterdə və ya serverdə mövcud olan məlumatlara daxil ola bilər.

MS Office 1-ci səviyyəli arxitekturanın bariz nümunəsidir. Bu, qənaətcil arxitekturadır və ona əsaslanan proqramlar yaratmaq daha asandır. Bu arxitekturanın əsas çatışmazlığı məlumatların bir müştəri kompüterindən digərinə ötürülməsinə imkan verməməsidir. Bəzən kompüterdə hər hansı bir dəyişiklik edildiyi təqdirdə 1-ci səviyyəyə əsaslanan tətbiqlər işləyə bilməz.

2-tier arxitektura - istifadəçi interfeysi qatının və verilənlər bazası qatının iki fərqli kompüterdə yerləşdiyi arxitekturadır. Bu, müştəri və serverin fərqli kompüterlərdə olması deməkdir. İstifadəçi tərəfindəki cihaz olan müştəri təlimat verir. Bütün məlumatları və məlumatları saxlayan server daha sonra lazımi məlumatları təmin etmək və ya mövcud məlumatlara dəyişiklik etmək üçün tələb olunur. Tətbiq səviyyəsi Server kompüterində mövcuddur. Həm istifadəçi interfeysi, həm təqdimat səviyyəsi, həm də verilənlər bazası səviyyəsi İnternet, ötürmə idarəetmə protokolu, İnternet protokolu vasitəsilə bir-biri ilə qarşılıqlı əlaqə qurur.

Tətbiqin iki səviyyəli arxitekturasını qorumaq və dəyişdirmək asandır. Müştəri ilə server arasında sorğu və cavab şəklində məlumat mübadiləsi də çox sürətlidir. Lakin bu arxitekturanın mənfi tərəfi odur ki, müştərilərin sayı icazə verilən imkanları aşarsa,

server müştərilərin göndərdiyi sorğulara cavab verə bilməz. Bu server performansını azaldır. Bundan əlavə, tətbiqdə hər hansı bir dəyişiklik edildiyi təqdirdə tətbiqin müştəri üzərində yenidən qurulması tələb olunur. Tətbiq səviyyəsi müştəri tərəfində olduğundan, müştəri yüksək emal gücünə malik olmalıdır.

3 səviyyəli arxitektura

Əksər veb tətbiqlər əsas funksiyaları səviyyələrə bölməklə yaradılır. Buna görə, bu səviyyələri bir-birindən asılı olmayaraq tez və səylə dəyişdirməyə və ya yeniləməyə imkan verir. Buna çox səviyyəli və ya üç səviyyəli arxitektura deyilir **şək.1.1.3**.

3 səviyyəli veb arxitekturasında üç təbəqə/qat var:

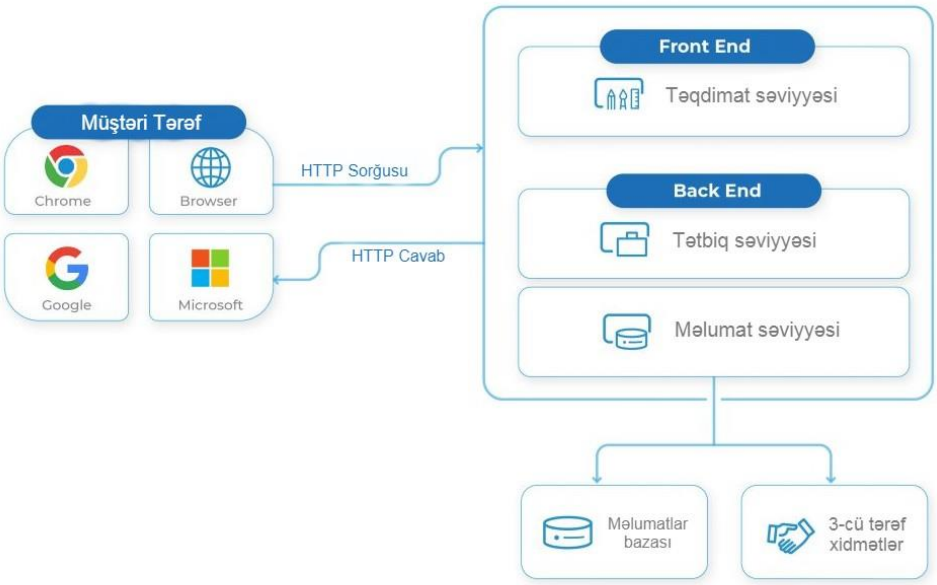
- Təqdimat səviyyəsi (müştəri)
- Tətbiq səviyyəsi
- Məlumat səviyyəsi

Müştərinin məlumatlara birbaşa çıxışı olmaması səbəbi ilə bu arxitekturanın ən etibarlı və sürətli olduğunu söyləmək olar. Tətbiq serverləri müxtəlif maşınlarda yerləşdirilə bilər ki, bu da performansın artırılması deməkdir.

Təqdimat/müştəri səviyyəsi - Təqdimat səviyyəsində sadəcə tətbiqin interfeysini nəzərdə tututlur. Bu səviyyə son istifadəçilərə görünən statik məzmun və dinamik interfeys kimi elementləri əhatə edir. Bu səviyyənin mühiti hər hansı bir brauzerdir. Bu səviyyədə istifadə olunan texnologiyalara HTML, CSS və ya JavaScript əlavə olaraq Angular, React və Vue daxildir.

Tətbiq səviyyəsi - Tətbiq təbəqəsi olaraq da adlandırılan tətbiq səviyyəsindən danışarkən, proqramın back-endinin bir hissəsidir. Veb tətbiqinin arxa hissəsi tətbiq məntiqini və təqdimat qatına göndərilən brauzer sorğularına cavabları müəyyən edir. O, əsas tətbiq məntiqindən ibarətdir və məlumat və sorğular üçün bütün daxili axını təsvir edir. Bu halda ən əlverişli mühit serverlər, serversiz bulud platformaları və ya PaaS-dir. Bu halda istifadə olunan proqramlaşdırma dilləri arasında biz C#, JavaScript,

Java, Python və PHP dillərini qeyd edə bilərik. İstifadə edilən back-end framework-lərə ASP.NET, express.js, nest.js, Spring, Flask, Django və Symfony daxildir.



Şək.1.1.3 3 səviyyəli arxitektura (Matt Kafami, 2024)

Məlumata giriş səviyyəsi

Verilənlər bazası, veb tətbiqi üçün məlumatları saxlayan və idarə edən bir veb tətbiqinin əsas komponentidir. Funksiyadan istifadə edərək istifadəçinin sorğusuna əsasən məlumatları axtara, süzə və çeşidləyə və son istifadəçiyə lazımi məlumatları verə bilər. Məlumatların bütövlüyünü təmin etmək üçün rollara əsaslanan giriş imkanı verirlər.

Veb tətbiq arxitekturası üçün verilənlər bazası seçərkən ölçü, sürət, quruluş nəzərə alınmalıdır. Strukturlaşdırılmış məlumatlar üçün SQL əsaslı verilənlər bazalarından istifadə etmək yaxşıdır.

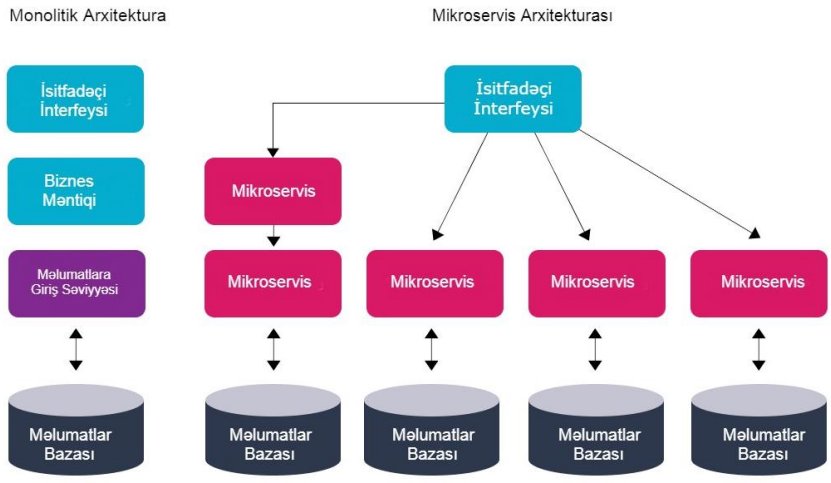
Monolitik arxitektura

Monolitik arxitektura, bütün proqramların ənənəvi kaskad modelindən keçən tək bir kod parçası kimi inkişaf etdirildiyi veb inkişaf arxitekturası olaraq da bilinən ənənəvi bir proqram inkişaf modelidir. Bu o deməkdir ki, bütün komponentlər bir-birindən asılıdır və bir-birinə bağlıdır; tətbiqi işə salmaq üçün hər bir komponent

lazımdır. Müəyyən bir funksiyanı dəyişdirmək və ya yeniləmək üçün yenidən yazılmalı və tərtib edilməli olan bütün kodu dəyişdirməlisiniz.

Mikroservis arxitekturası - Mikroservis arxitekturası monolitik bir mühitdə olan bir neçə problemi həll edir. Mikroservis arxitekturasında kod RESTful API vasitəsilə qarşılıqlı əlaqədə olan sərbəst əlaqəli müstəqil xidmətlər kimi hazırlanır. Hər bir mikroservis öz məlumat bazasını ehtiva edir və müəyyən bir iş məntiqini idarə edir, beləliklə müstəqil xidmətləri asanlıqla inkişaf etdirə və yerləşdirə bilərsiniz. Zəif qarşılıqlı əlaqə sayəsində mikroservis arxitekturası müstəqil xidmətləri yeniləmək/dəyişdirmək və genişləndirmək üçün rahatlıq təmin edir. İnkişaf sadə və səmərəli olur və davamlı təchizatı təmin edir. Yaradıcılar yeniliyə tez uyğunlaşa bilərlər. Yüksək miqyaslı və mürəkkəb tətbiqetmələr üçün mikroservislər yaxşı seçimdir **şək.1.1.4**.

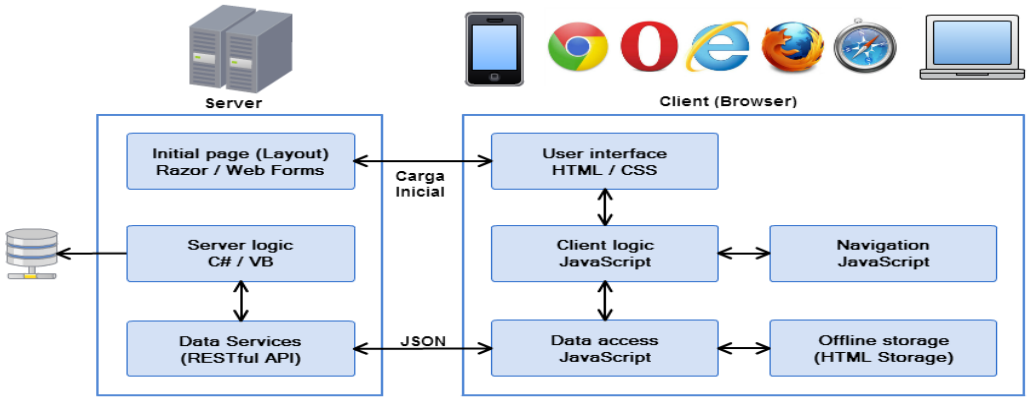
Serversiz arxitektura - Adının əksinə olaraq, bu yenilikçi yanaşma serverləri tamamilə istisna etmir. Bunun əvəzinə, bu, inkişaf etdiriciləri idarəetmə və nəzarət proqramının quraşdırıldığı serverləri konfiqurasiya etməkdə çətinlik çəkməkdən azad edir. Bütün infrastruktur üçüncü tərəf satıcılarına həvalə edilmişdir ki, bu da veb tətbiqetmələrin inkişafına yanaşmamızda bir paradiqma dəyişikliyini göstərir. Bu, təkcə tərtibatçıların yükünü azaltmır, həm də infrastrukturun ekspertlər tərəfindən dəstəklənməsini təmin edir ki, bu da etibarlılığı və səmərəliliyi artırır.



Şək.1.1.4 Monolitik və mikroservis arxitekturası (Roman Beekeeper, 2021)

Server idarəetmə nüanslarına girmədən yalnız kod məntiqinə diqqət yetirməyi üstün tutan veb inkişaf etdiriciləri üçün serversiz memarlıq tamamilə yeni bir şeydir. Bu, inkişaf etdiricilərə Server konfiqurasiyasından narahat olmadan kodlarını yerinə yetirməyə imkan verərək inkişaf prosesini asanlaşdırır.

Tək səhifə arxitekturası - Tək Səhifə Tətbiqi (SPA) arxitekturası istifadəçinin proqramla qarşılıqlı əlaqəsi zamanı tək bir HTML səhifəsini dinamik olaraq yeniləyən veb proqram arxitekturasıdır. Hər qarşılıqlı əlaqə üçün serverdən yeni səhifələr yükləmək əvəzinə, SPA-lar tək bir HTML səhifəsini yükləyir və məzmunu dinamik şəkildə yeniləmək üçün JavaScript-dən istifadə edir. Bu yanaşma masa üstü proqramlara bənzər daha çox çevik və həssas istifadəçi təcrübəsi təmin edir **şək.1.1.5**.



Şək.1.1.5 SPA arxitekturası (Samuel Santos, 2022)

Sosial Media Platformaları

İnternetin müasir həyatın ayrılmaz hissəsi olduğu inkar edilməzdir. İnternet istifadəçiləri olaraq 197,6 milyon e-mail göndərir, onlayn olaraq 1,6 milyon dollar xərcləyir və hər dəqiqə demək olar ki, 415,000 proqram yükləyirik. Lakin internetdən artan istifadəmiz bizə sonsuz ünsiyyət, öyrənmə və texnoloji imkanlar təqdim etsə də, bu, bizi çoxlu sayda veb əsaslı təhlükələrlə üz-üzə qoyur. Veb-saytlarda və platformalarda kibertəhlükəsizlik bu rəqəmsal aktivləri kiber təhdidlərdən və hücumlardan qorumaq üçün görülən təcrübə və tədbirlərə aiddir. Bu veb-saytlar və platformalar vasitəsilə saxlanılan, emal edilən və ya ötürülən məlumatların məxfiliyinin, bütövlüyünün və əlçatanlığının qorunmasını əhatə edir.

Veb platformalar istifadəçilərə internet üzərindən bir-biri ilə və ya müəssisələrlə qarşılıqlı əlaqə qurmağa və əməkdaşlıq etməyə imkan verən proqram sistemləri və ya

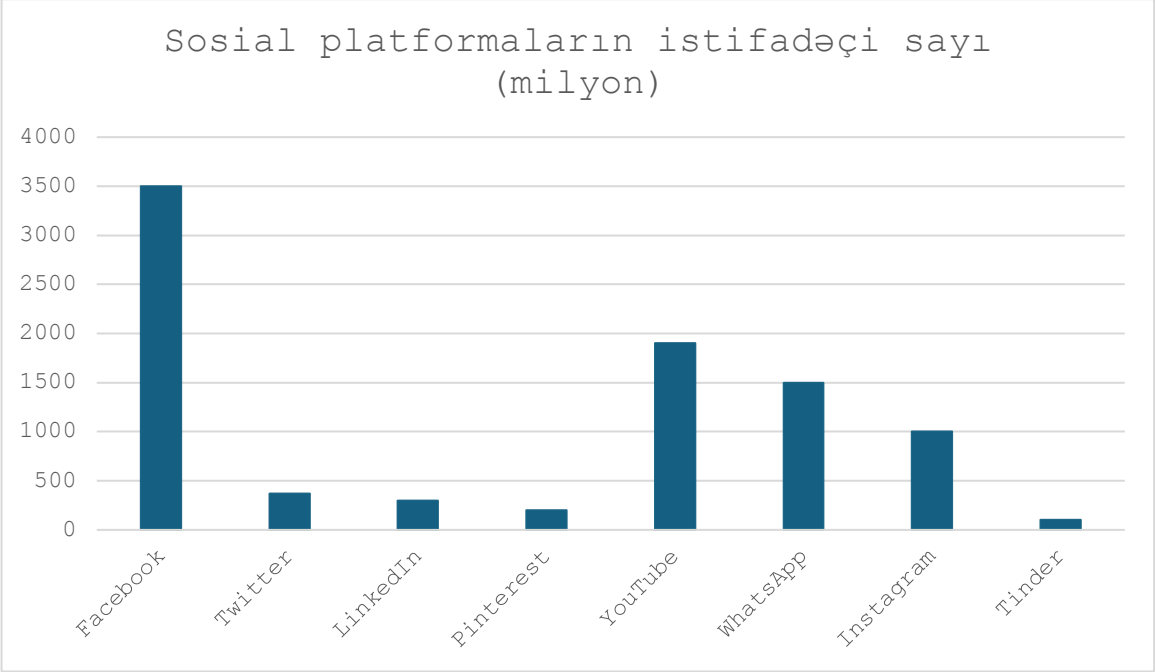
xidmətlərdir. Bu platformalar sosial şəbəkə, e-ticarət, məzmunun idarə edilməsi və s. kimi müxtəlif məqsədlərə xidmət edə bilər (Gregory Terzian 2023). Aşağıdakı bəzi veb platforma növlərini nəzərdən keçirək:

1. Sosial Media Platformaları
2. Elektron Ticarət Platformaları

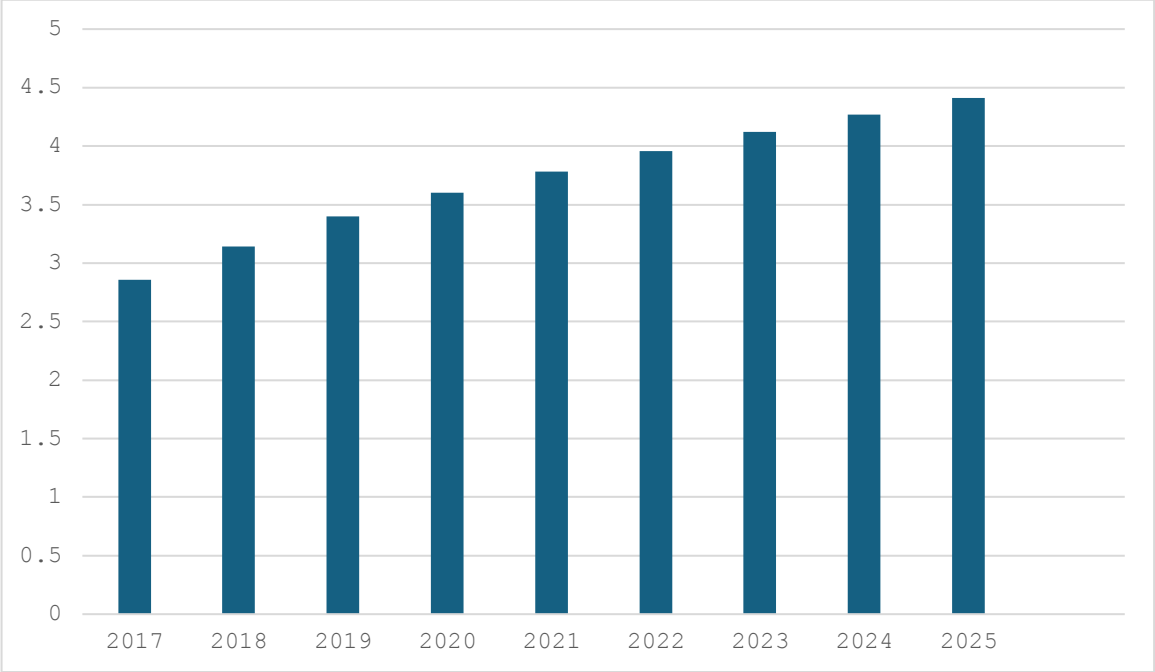
1990-cı illərin ortalarında internet populyarlaşdıqca, əvəllər paylaşılması mümkün olmayan məlumatları,asan bir şəkildə paylaşmağa imkan yaratdı. Daha sonra, 2000-ci illərin əvvəllərində kütlələr tərəfindən sosial şəbəkə və veb-saytlarda qəbul edilən onlayn məlumat mübadiləsinə üstünlük verildi. Bu Facebook, Twitter, İnstagram, LinkedIn kimi sosial media platformaları vasitəsilə digər şəxslərlə ünsiyyətini genişləndirmək artıq hər zaman olduğundan daha asan bir hala çevrildi. Həm şəxsi, həm də kommersiya məqsədləri üçün istifadə edilməyə başlanıldı.Sosial media platformaları,insanları danışmaq, fikir və maraqları bölüşmək və yeni dostlar qazanmaq üçün bir araya gətirdi (Sahoo SR, Gupta BB 2020). İnternetin onlayn məkanında təxminən 4 milyard istifadəçi var. 30 dekabr 2020-ci il tarixinə, ümumi internet istifadəçilərinin 2,7 milyardı Facebook, 330 milyon Twitter aktiv istifadəçisi və 320 milyon Pinterest aktiv istifadəçisidir. **Şək.1.1.6** müxtəlif sosial media platformalarında istifadəçilərin sayını göstərir. Zephoria-nın hesabatına görə, Facebook-un aylıq aktiv istifadəçilərinin sayı əvvəlki ilə nisbətən 16% artıb. Hər saniyədə yeddi yeni profil yaradılır. İstifadəçilər gündə cəmi 350 milyon foto yükləyirlər. Orta hesabla hər 60 saniyədə Facebook-da 510.000 şərh yerləşdirilir, 298.000 status yenilənir və 136.000 foto yüklənir. Facebook-da çox sayda məlumat yükləndiyindən təhlükəsizlik təhdidlərinin baş vermə ehtimalı yüksəkdir.

Şək.1.1.7-də göstərilən məlumatlara görə, sosial media saytlarının istifadəsi günü-gündən böyük sürətlə artmaqdadır, buna görə də bu saytlardan çox sayda məlumat və informasiya əldə edilə bilər, bu da məlumat sızması riski , məlumatların ələ keçirilməsi, məxfiliyə nəzarət, müəllif hüquqlarının pozulması və informasiya saxtakarlığı kimi bir sıra kibercinayətlərə qapı açmaqdadır. Twitter kimi bəzi iş sosial media saytları şəxsi məlumatların istifadəçilərə açıqlanmasına icazə verməsə də, bəzi təcrübəli kibercinayətkarlar istifadəçilərin yazılarını və onlayn paylaşdıqları

məlumatları təhlil edərək həssas məlumatlar əldə edə bilərlər. İnternetdə paylaşdığımız şəxsi məlumatlar kibercinayətkarlara e-mail və şifrələrimizə daxil olmaq üçün kifayət qədər məlumat verə bilər.



Şək.1.1.6 Sosial şəbəkə platformalarının istifadəçi sayları (Sahoo SR, Gupta BB 2020)



Şək.1.1.7 Dünyada sosial şəbəkə istifadəçilərinin illərə görə sayı (Internet Live Stats, 2020)

Elektron Ticarət Platformaları - sadə sözlə desək, e-ticarət termini tamamilə internet vasitəsilə həyata keçirilən alış-verişi, satışı və ödənişləri əhatə edir. Belə bir biznes demək olar ki, bütün ölkələrdə inkişafa təsir edən nəhəng bir sistemə çevrilib və buna görə də qlobal iqtisadiyyatın ayrıca bir hissəsini formalaşdırır.

Onlayn ticarət sizə internet üzərindən sahibkarlıq fəaliyyətini həyata keçirməyə imkan verməklə yanaşı həmçinin, təchizatçıların və alıcıların axtarışı, hesabların ödənilməsi, müqavilələrin tərtib olunması kimi prosesləri həyata keçirməyə şərait yaradır. Təbii ki, bunun üçün xüsusi qaydalar hazırlanır, unikal proqram təminatı yaradılır.

1.2 Veb-saytlarda və platformalarda kibertəhlükəsiz konsepsiyasının analizi

İnternetin qlobal kommunikasiya, ticarət və qarşılıqlı əlaqənin onurğa sütunu olduğu bir dövrdə kibertəhlükəsizlik əvəzolunmaz hala gəldi. Veb tətbiqləri və platformalarının əlavə edilməsi ilə rəqəmsal aktivlərin zərərli hücumlara qarşı gücləndirilməsi zərurəti heç vaxt bu qədər kritik olmamışdır. İnternet milyardlarla gündəlik mübadilə və əməliyyatları asanlaşdırır və qlobal miqyasda ən mürəkkəb bir-biri ilə əlaqəli sistemlərdən birini yaradır. Lakin bu geniş yayılmış əlaqə interneti veb-saytlarda və tətbiqlərdə zəiflik axtaran kibercinayətkarlar üçün də əsas hədəfə çevirib. Uğurlu kiberhücum maliyyə itkilərindən tutmuş həssas məlumatların və nüfuzun zədələnməsinə qədər dağıdıcı nəticələrə gətirib çıxara bilər (H. Tabrizchi and M. K. Rafsanjani,2020).

Veb təhlükəsizliyi təmin edə bilmək üçün bir neçə təhlükəsizlik aspektlərini nəzərdən keçirmək lazımdır.

Autentifikasiya və avtorizasiya veb təhlükəsizliyinin əsas aspektlərindən sayılır və yalnız səlahiyyətli istifadəçilərin veb tətbiqi daxilində xüsusi resurslara və ya funksiyalara çıxışının təmin edilməsində mühüm rol oynayır.

1. Autentifikasiya (ing. Authentication) istifadəçinin və ya sistemin şəxsiyyətinin yoxlanılması prosesidir. Bu proqrama və ya onun resurslarına giriş icazəsi

verməzdən əvvəl istifadəçinin iddia etdiyi şəxs olmasını təmin edir. Ümumi autentifikasiya mexanizmlərinə aşağıdakılar daxildir:

- İstifadəçi adı və Şifrə: İstifadəçilərin proqrama daxil olmaq üçün istifadəçi adı və parol daxil etməli olduğu identifikasiyanın ən əsas forması.
- Biometrik Doğrulama: İstifadəçinin şəxsiyyətini yoxlamaq üçün barmaq izləri və ya üz tanıma kimi unikal bioloji xüsusiyyətlərdən istifadə edir.
- Çox faktorlu Doğrulama (ing. Multi-factor Authentication ,MFA): İstifadəçilərdən parol, təhlükəsizlik nişanı və ya barmaq izi skanı kimi giriş əldə etmək üçün iki və ya daha çox yoxlama faktoru təqdim etmələrini tələb edir. Bu əlavə təhlükəsizlik tədbiri kimi çıxış edən bir üsuldur.
- OAuth - açıq giriş protokuludur. Bu protokol istifadəçiyə üçüncü tərəfə login və şifrə təqdim etmədən müxtəlif təhlükəsiz resurslara vahid hesabla giriş etmək imkanı verir.
- OpenID - mərkəzləşdirilmiş autentikasiya sisteminin açıq standartıdır. Bu standart istifadəçiyə bir-biri ilə əlaqəli olmayan internet resurslarda autentikasiya üçün vahid hesab yaratmağa imkan verir.

2. Avtorizasiya (ing. Authorization) autentifikasiya edilmiş istifadəçinin proqram daxilində hansı hərəkətləri yerinə yetirməsinə icazə verildiyini müəyyən edir. O, istifadəçilərin xüsusi resurslara daxil olmaq və ya müəyyən əməliyyatları yerinə yetirmək üçün lazımi icazələrə malik olmasını təmin edir. Avtorizasiya mexanizmlərinə aşağıdakılar daxildir:

- Rola əsaslanan girişə nəzarət: İstifadəçilərə təşkilat daxilindəki rollarına əsasən icazələr təyin edərək, resurslara girişi idarə etməyi asanlaşdırır.

Müəssisədə RBAC tətbiq etməzdən əvvəl təşkilat hər bir rol üçün icazələri mümkün qədər hərtərəfli müəyyən etməlidir. Bura aşağıdakı sahələrdə icazələrin dəqiq müəyyənləşdirilməsi daxildir:

- Məlumatların dəyişdirilməsi üçün icazələr (məsələn, oxumaq, yazmaq, tam giriş)
- Şirkət proqramlarına daxil olmaq üçün icazə
- Tətbiq daxilində icazələr

Bütün RBAC modelləri aşağıdakı qaydalara əməl etməlidir:

Rol tapşırığı - subyekt yalnız rol təyin edildikdə imtiyazlardan istifadə edə bilər.

Rol avtorizasiya - sistem subyektin aktiv roluna icazə verməlidir.

İcazə avtorizasiya - subyekt yalnız subyektin aktiv roluna verilmiş icazələri tətbiq edə bilər.

- Atribut əsaslı giriş nəzarəti (ing. Attribute-based access control, ABAC): Giriş icazələrini müəyyən etmək üçün atributlardan (məsələn, istifadəçi atributları, resurs atributları, davranış atributları, ətraf mühit atributları) istifadə edir.

- İstifadəçi atributlarına şəxsiyyət vəsiqəsi, iş rolları, qrup üzvlükləri, şöbə və təşkilati üzvlükləri, idarəetmə səviyyəsi, təhlükəsizlik rəsmiləşdirilməsi və digər müəyyənedici meyarlar daxildir.
- Resurs atributları faylın yaranma tarixi, onun sahibi, fayl adı və növü və məlumat həssaslığı kimi bütün müəyyənedici xüsusiyyətlərdir.
- Ümumi davranış atributlarına "oxumaq", "yazmaq", "redaktə etmək", "kopyalamaq" və "silmək" daxildir. Bəzi hallarda bir neçə hərəkət atributu təsvir edə bilər.
- Ətraf mühitin bütün atributları giriş cəhdinin vaxtı və yeri, subyektin cihazı, rabitə protokolu və şifrələmə gücü kimi kontekstual amilləri özündə ehtiva edir.

- Siyasətə əsaslanan girişə nəzarət: Kimin hansı şərtlərdə hansı resurslara daxil ola biləcəyini müəyyən edən giriş siyasətlərini müəyyən edir.

- İyerarxik girişə nəzarət (ing. Hierarchical access control): İyerarxik struktur daxilində istifadəçinin mövqeyinə əsasən girişə nəzarət edir.

Doğrulama və avtorizasiya veb təhlükəsizliyinin mühüm komponentləridir və onların effektiv şəkildə həyata keçirilməsi icazəsiz girişdən və resurslardan sui-istifadədən qorunmağa kömək edir. Veb tətbiqinizin xüsusi tələblərinə və təhlükəsizlik ehtiyaclarına əsaslanaraq müvafiq autentifikasiya və avtorizasiya mexanizmlərini seçmək vacibdir.

3. Şifrələmə veb təhlükəsizliyin vacib komponentidir, çünki o, həssas məlumatların icazəsiz şəxslər tərəfindən əldə edilməsindən qorunmağa kömək edir. Veb təhlükəsizliyi kontekstində şifrələmə aşağıdakıları özündə ehtiva edir:

1. Məlumatların şifrələnməsi məlumatların yalnız düzgün şifrələmə açarı olan biri tərəfindən oxuna və ya başa düşülə bilən formata çevrilməsini nəzərdə tutur. Bu, məlumatların tutulsa belə, açar olmadan oxunmaz qalmasını təmin edir.
2. Şifrələmə protokolları :
   - HTTPS: HTTPS veb server və müştərinin brauzeri arasında ötürülən məlumatları şifrələmək üçün SSL/TLS protokollarından istifadə edən HTTP-nin uzantısıdır. O, şəbəkə üzərindən mübadilə edilən məlumatların şifrələndiyini və dinləmə və ya saxtakarlığa qarşı təhlükəsiz olmasını təmin edir.
   - SSL/TLS: Bunlar kompüter şəbəkəsi üzərindən təhlükəsiz rabitə təmin edən kriptoqrafik protokollardır. Onlar tranzit zamanı məlumatları şifrələyərək müştəri və server arasında təhlükəsiz əlaqə yaradırlar.
3. Şifrələmə alqoritmləri :
   - AES: AES geniş istifadə olunan simmetrik şifrələmə alqoritmidir. O, müxtəlif proqramlarda məlumatları şifrələmək və deşifrə etmək üçün istifadə olunur və güclü açarla istifadə edildikdə təhlükəsiz sayılır.

Şifrələmə veb təhlükəsizliyinin əsas aspektidir və həssas məlumatları icazəsiz girişdən və ya ələ keçirmədən qorumaq üçün çox vacibdir. Güclü şifrələmə protokollarının və alqoritmlərinin tətbiqi veb proqramların və onların istifadəçilərinin təhlükəsizliyini və məxfiliyini təmin etmək üçün vacibdir.

4. Girişin doğrulanması (ing. Input validation) istifadəçi tərəfindən daxil edilən məlumatların düzgünlüyünü və təhlükəsizliyini təmin etmək üçün yoxlanması prosesidir. Bu, tətbiqin yanlış və ya zərərli məlumatları qəbul etməsinin qarşısını almaq üçün vacibdir. Daxil edilən məlumatların yoxlanılması prosesi, istifadəçinin daxil etdiyi məlumatların gözlənilən formatda, aralıqda və tipdə olduğunu təsdiq edir. Bu, SQL inyeksiyası, XSS və yaddaş daşması (ing. Buffer overflow) kimi hücumların qarşısını almağa kömək edir. Daxil edilən məlumatların yoxlanılması əsasən iki növdə həyata keçirilir: server tərəfdə yoxlama (ing. server-side validation) və müştəri tərəfdə yoxlama (ing. client-side validation). Server tərəfdə yoxlama daha etibarlıdır, çünki klient tərəfdə yoxlama istifadəçi tərəfindən bypass edilə bilər.

5. Sessiyanın idarə edilməsi (ing. Session management) istifadəçi sessiyalarının yaradılması, saxlanması və idarə edilməsi prosesidir. Sessiya, istifadəçinin tətbiqə daxil olduğu müddət ərzində onun vəziyyətini izləmək üçün istifadə olunur. Sessiya idarəçiliyi, istifadəçinin daxil olduğu anda ona unikal sessiya identifikatoru (ing. session ID) təyin edir və bu identifikator vasitəsilə istifadəçinin fəaliyyəti izlənilir. Sessiya identifikatorları adətən çərəzlər (ing. cookies), URL parametrləri və ya gizli sahələr (ing. hidden fields) vasitəsilə saxlanılır. Sessiya idarəçiliyi təhlükəsizlik baxımından vacibdir, çünki düzgün idarə olunmayan sessiyalar sessiya oğurluğu (ing. session hijacking) kimi hücumlara məruz qala bilər. Təhlükəsizlik tədbirləri olaraq sessiya identifikatorlarının təsadüfi və unikal olması, HTTPS istifadəsi və sessiyaların müəyyən müddət ərzində fəaliyyətsizlikdən sonra avtomatik olaraq bitməsi təmin edilməlidir.

6. Təhlükəsizlik başlıqları (ing.Security Headers)

Təhlükəsizlik başlıqları (Security Headers) veb tətbiqlərin təhlükəsizliyini artırmaq üçün HTTP cavablarına əlavə edilən xüsusi başlıqlardır. Bu başlıqlar, müəyyən təhlükəsizlik siyasətlərini tətbiq edərək müxtəlif hücum vektorlarını məhdudlaşdırır. Məsələn, CSP başlığı, məzmunun hansı mənbələrdən yüklənəcəyini tənzimləyir və XSS hücumlarını azaldır. X-Frame-Options başlığı, veb səhifələrin iframe içərisində göstərilməsini məhdudlaşdıraraq clickjacking hücumlarından qoruyur. X-Content-Type-Options başlığı, brauzerlərə məzmun növünü avtomatik olaraq təyin etməmələrini bildirir və MIME tip əlaqəli hücumların qarşısını alır. Strict-Transport-Security (HSTS) başlığı, brauzerlərə yalnız HTTPS üzərindən əlaqə qurmağı məcbur edir. Referrer-Policy başlığı, istifadəçinin hansı məlumatların referer başlığına daxil ediləcəyini tənzimləyir. Permissions-Policy başlığı, brauzer funksiyalarının (məsələn, kamera, mikrofon) hansı domenlər tərəfindən istifadə ediləcəyini məhdudlaşdırır. Expect-CT başlığı, sertifikat şəffaflığı problemlərini aşkarlayır və hesabat verir. X-Permitted-Cross-Domain-Policies başlığı, Adobe Flash və ya PDF oxuyucuları kimi plugin-lərin hansı siyasətlərə əməl edəcəyini müəyyənləşdirir. Bu başlıqların düzgün

konfiqurasiyası veb tətbiqlərin təhlükəsizlik səviyyəsini əhəmiyyətli dərəcədə artırır. Təhlükəsizlik başlıqlarının istifadəsi, müasir veb tətbiqlərdə təhlükəsizlik tədbirlərinin vacib bir hissəsidir.

7.Təhlükəsiz kodlaşdırma təcrübələri (ing.Secure Coding Practices)

Təhlükəsiz kodlaşdırma təcrübələri proqram təminatının inkişafı zamanı təhlükəsizlik zəifliklərinin qarşısını almaq üçün tətbiq olunan metod və texnikalardır. Bu təcrübələr, kodun mümkün olan ən təhlükəsiz şəkildə yazılmasını təmin edir və potensial hücumların qarşısını alır. Təhlükəsiz kodlaşdırma təcrübələri aşağıdakı əsas prinsiplərə əsaslanır:

1. **Girişlərin doğrulanması və təmizlənməsi**: İstifadəçilərdən və ya digər mənbələrdən gələn bütün girişlər doğrulanmalı və təmizlənməlidir. Bu, SQL Injection, XSS və digər təhlükələrə qarşı müdafiəni təmin edir.
2. **Məlumatların şifrələnməsi**: Həssas məlumatlar (parollar, şəxsi məlumatlar və s.) saxlanarkən və ötürülərkən şifrələnməlidir. Bu, məlumatların üçüncü tərəflər tərəfindən ələ keçirilməsinin qarşısını alır.
3. **Kod icazələri və məhdudiyyətləri**: Kodun yalnız zəruri səlahiyyətlərə malik olmasını təmin edin. Minimum hüquq siyasəti tətbiq olunmalıdır, yəni kod yalnız icrası üçün lazım olan minimal hüquqlara malik olmalıdır.
4. **Təhlükəsizlik yoxlamaları və testlər**: Kod yazıldıqdan sonra müntəzəm təhlükəsizlik yoxlamaları və testləri aparılmalıdır. Penetrasiya testləri və avtomatlaşdırılmış təhlükəsizlik skanerləri istifadə edilməlidir.

Bu təcrübələrin tətbiqi proqram təminatının daha təhlükəsiz və etibarlı olmasını təmin edir, istifadəçi məlumatlarını qoruyur və ümumi sistem təhlükəsizliyini artırır.

8. Müntəzəm yeniləmələr və yamaqlama (ing.Regular Updates and Patching)

Müntəzəm yeniləmələr və yamaqlama proqram təminatının təhlükəsizliyini və sabitliyini təmin etmək üçün vacibdir. Bu proses, mövcud zəiflikləri aradan qaldıraraq sistemlərin və tətbiqlərin təhlükəsizlik səviyyəsini yüksəldir. Yamaqlar, proqram təminatında aşkar edilən təhlükəsizlik boşluqlarını və xətaları düzəltmək üçün yayımlanır.

Təhlükəsizlik yamaqlarının tətbiq olunmaması, sistemləri hakerlərə və zərərli proqramlara qarşı həssas edir. İstifadəçilər və təşkilatlar, yamaqların vaxtında tətbiq olunmasını təmin etməlidirlər. Avtomatik yeniləmə mexanizmləri, bu prosesi asanlaşdırır və insan səhvlərini minimuma endirir.

Yamaqlama prosesi, həm əməliyyat sistemləri, həm də tətbiqlər üçün vacibdir. Yamaqların tətbiqindən əvvəl, onların sınaqdan keçirilməsi vacibdir ki, bu da sistemdə uyğunsuzluqların yaranmasının qarşısını alır. Müntəzəm yeniləmələr və yamaqlama, təşkilatların məlumatlarını və infrastrukturlarını qorumaq üçün əsas addımlardan biridir.

Təhlükəsizlik təhdidlərinin davamlı olaraq inkişaf etdiyi müasir dövrdə, yamaqlama və yeniləmə proseslərinə laqeyd yanaşmaq böyük risklər yaradır. Təşkilatlar, effektiv yamaqlama strategiyaları hazırlamalı və bu strategiyaları müntəzəm olaraq icra etməlidirlər.

9. Təhlükəsizlik Testləri (ing. Security Testing)

Təhlükəsizlik testləri bir sistemin zəif nöqtələrini tapmaq və onu qorumaq üçün edilən testlərdir. Əsas təhlükəsizlik test növləri:

Pen Test (ing. Penetration Testing): Bir sistemin zəif nöqtələrini aktiv olaraq axtarmaq üçün edilən simulyasiya edilmiş hücumlar.

Zəiflik Skanlanması (ing.Vulnerability Scanning): Avtomatik vasitələrlə sistemdə mövcud olan zəif nöqtələri müəyyən etmək üçün istifadə edilir.

Təhlükəsizlik Auditi (Security Auditing): Bir sistemin təhlükəsizlik siyasətlərinin, prosedurlarının və konfiqurasiyalarının yoxlanması.

10. İcazəsiz girişin aşkarlanması sistemi və icazəsiz girişin qarşısını alınması sistemi

IDS və IPS sistemləri şəbəkədə və ya sistemdə olan anormal fəaliyyəti və zərərli hücumları müəyyən edir və qarşısını alır.

IDS: Şəbəkədə və ya sistemdə olan fəaliyyətləri izləyir və potensial hücumları aşkarlayır, lakin bu hücumları avtomatik olaraq dayandırmır. O, yalnız administratora xəbərdarlıq edir.

IPS: IDS-in genişlənmiş formasıdır və aşkar edilmiş hücumları avtomatik olaraq dayandıra bilir. Bu, həm hücumları aşkar edir, həm də onları bloklayır.

Bu sistemlər şəbəkənin təhlükəsizliyini təmin etmək üçün mühüm rol oynayır və həmçinin hücumların qarşısını almağa və ya onların təsirini minimuma endirməyə kömək edir.

11. Təhlükəsizlik Testi (Security testing)

Təhlükəsizlik testi proqram sistemlərinin təhlükəsizliyini və möhkəmliyini təmin etmək üçün mühüm prosesdir. Bu, zərərli aktorlar tərəfindən istifadə edilə bilən zəifliklərin müəyyən edilməsinə və aradan qaldırılmasına yönəlmiş müxtəlif texnikaları əhatə edir. Müntəzəm təhlükəsizlik testi sistemlərin bütövlüyünü, məxfiliyini və mövcudluğunu qorumağa kömək edir. Təhlükəsizlik testinin əsas komponentlərinə nüfuz testi, zəifliyin skan edilməsi və kodun nəzərdən keçirilməsi daxildir.

Əsas Komponentlər

1. **Nüfuz Testi**
2. **Zəifliyin Skanı**
3. **Kod Baxışları**

Təhlükəsizlik testini inkişaf dövrünə inteqrasiya etməklə, təşkilatlar kibertəhlükələrə qarşı etibarlı müdafiəni təmin etməklə təhlükəsizlik məsələlərini fəal şəkildə müəyyən edə və həll edə bilər. Müntəzəm təhlükəsizlik testi təhlükəsiz mühiti qorumağa kömək edir və istifadəçilər və maraqlı tərəflər arasında etibarı artırır.

12. Hadisəyə cavab (Insident response)

Hadisələrə reaksiya təşkilatın kibertəhlükəsizlik strategiyasının kritik elementidir. Bu, təhlükəsizlik pozuntularını effektiv şəkildə aradan qaldırmaq üçün hərtərəfli planın olmasını nəzərdə tutur. İnsidentə cavab planı təşkilatın təhlükəsizlik insidentlərinin təsirini tez bir zamanda azalda bilməsini və gələcəkdə baş verə biləcək hadisələrin qarşısını almaq üçün onlardan öyrənə bilməsini təmin edərək, qarşısının alınması, aradan qaldırılması, bərpası və insidentdən sonrakı təhlil üçün addımları əhatə edir (Sodagudi, S., Kotha, S.K., David Raju,2019).

Hadisələrə Cavab Planının Əsas Komponentləri

1. **Hazırlıq**
2. **İdentifikasiya**
3. **Saxlama**
4. **Silinmə**
5. **Bərpa**
6. **Hadisədən sonrakı təhlil**

Güclü insidentlərə cavab planını həyata keçirməklə təşkilatlar təhlükəsizlik pozuntularını effektiv şəkildə idarə edə, ümumi təhlükəsizlik dayanıqlığını artırarkən sürətli mühafizə və bərpanı təmin edə bilərlər.

13. Xidmətdən imtina hücumu (ing. Distributed Denial of Service, DDoS) hücumu, bir sistemin və ya şəbəkənin normal işləməsinə mane olmaq üçün bir çox mənbədən çox sayda saxta trafik göndərməklə həyata keçirilir. Bu hücumlar, veb-saytları, xidmətləri və ya şəbəkələri yükləyərək və ya hətta tamamilə çökdürərək onların əlçatmaz olmasına səbəb olur. Adətən, zombi kompüterlərdən və ya botnet (ing. botnet) adlanan infeksiyalı cihazlardan ibarət geniş bir şəbəkə vasitəsilə həyata keçirilir. DDoS hücumları, IT infrastrukturuna ciddi zərər verə bilər və iş fəaliyyətini dayandıra bilər. Ən çox rast gəlinən DDoS hücum növləri arasında UDP (ing. User Datagram Protocol) flood, ICMP (ing. Internet Control Message Protocol) flood, SYN (ing. Synchronize) flood və HTTP (ing. Hypertext Transfer Protocol) flood kimi metodlar yer alır.

Veb-saytların yaradılması və saxlanması kodun yazılmasını, serverlərin konfiqurasiyasını və verilənlər bazalarının idarə edilməsini əhatə edir.Bütün bunlar təhlükəsizlik şərtləri daxilində yerinə yetirilmədikdə təhlükəsizlik zəifliyinə səbəb ola bilər. İstifadəçi daxiletməsini sanitarlaşdırmamaq və ya proqram təminatını məlum təhlükəsizlik yamaqları ilə yeniləməyə məhəl qoymamaq kimi etibarsız kodlaşdırma təcrübələri kibercinayətkarların istifadə edə biləcəyi giriş nöqtələri yaradır. Buna görə də proqramçılar veb inkişaf proqramlarının təhlükəsizlik vəziyyətini yaxşılaşdırmaqla, təşkilatlar təhlükəsizlik pozuntusu ehtimalını və potensial riskləri azalda bilər.

İstifadəçilər veb-saytların öz həssas məlumatlarını və məxfiliyini qorumasını gözləyirlər və hər hansı bir təhlükəsizlik çatışmazlığı etibarı sarsıda və nüfuzun zədələnməsinə səbəb ola bilər. Veb inkişafında kibertəhlükəsizliyə üstünlük verməklə təşkilatlar istifadəçi məlumatlarını qorumaq və etibarı artırmaq öhdəliyini nümayiş etdirirlər. Bəzi veb təhlükəsizlik standartları aşağıdakılardır:

Kibertəhlükəsizlik standartı nədir?

Kibertəhlükəsizlik standartı təşkilatların kibertəhlükəsizliyini artırmaq üçün istifadə edə biləcəyi təlimatlar və ya ən yaxşı təcrübələr toplusudur.Təşkilatlar sistemlərini və məlumatlarını kiber təhlükələrdən qorumaq üçün müvafiq tədbirləri müəyyənləşdirmək və həyata keçirmək üçün kiber təhlükəsizlik standartlarından istifadə edə bilərlər. Standartlar həmçinin kibertəhlükəsizlik hadisələrinə cavab vermək və onlardan sonra bərpa etmək üçün bələdçi rolunu oynayır.Kibertəhlükəsizlik sistemləri ümumiyyətlə ölçüsündən, spektrından və sektorundan asılı olmayaraq bütün təşkilatlara aiddir.

Müdafiə üçün federal satınalma qaydalarına əlavə

DFARS, ABŞ Müdafiə Nazirliyinin (ing. Department of Defense, DoD) satınalmaları ilə bağlı tənzimləmələri əhatə edən bir əlavədir. Bu tənzimləmələr, müdafiə sektoru ilə müqavilə bağlayan təşkilatların təhlükəsizlik və məlumatların qorunması tələblərini yerinə yetirmələrini təmin edir. Əsasən DFARS 252.204-7012 maddəsi altında, şirkətlərin NIST SP 800-171 standartına uyğun təhlükəsizlik nəzarətlərini tətbiq etməsi və kibertəhlükəsizlik insidentlərini 72 saat ərzində DoD-a bildirməsi tələb olunur. DFARS uyğunluğu milli təhlükəsizliyi qorumaq, təchizat zəncirinin təhlükəsizliyini artırmaq və müdafiə sektorunda müqavilə bağlayan şirkətlər üçün zəruri tələbləri müəyyənləşdirmək üçün vacibdir.

İnformasiya təhlükəsizliyinin idarə edilməsi haqqında federal qanun

FISMA, ABŞ federal hökumətinin məlumat sistemlərinin təhlükəsizliyini təmin etmək üçün qəbul edilmiş qanundur. Bu qanun, federal agentliklərdən informasiya təhlükəsizliyi proqramlarının yaradılmasını və idarə edilməsini tələb edir. FISMA, federal informasiya sistemlərinin təhlükəsizliyini və məxfiliyini qorumaq üçün milli standartların və ən yaxşı təcrübələrin tətbiqini təmin edir.

Tibbi sığorta daşınabilərlik və hesabatlılıq Qanunu

HIPAA, Amerika Birləşmiş Ştatlarında sağlamlıq sektorunda şəxsi məlumatların gizliliyini, bütövlüyünü və əlçatanlığını təmin etmək məqsədi ilə qəbul edilmiş bir qanundur. HIPAA, sağlamlıq informasiya mübadiləsini, elektron məlumatların saxlanılmasını və informasiya təhlükəsizliyi prosedurlarını dəyişdirərək sağlamlıq sektorunda məlumatların məxfiliyini və bütövlüyünü təmin etmək üçün tədbirlər görməkdədir.

Beynəlxalq standartlaşdırma təşkilatı 22301 (ISO)

ISO 22301, təşkilatların bir işin davamlılığını necə təmin edə biləcəyini və özlərini fövqəladə hallardan qoruya biləcəyini izah edən beynəlxalq bir standartdır. Standart hərtərəfli iş davamlılığı idarəetmə sistemi üçün çərçivə təmin edir. Ölçüsündən, sənayesindən və yerindən asılı olmayaraq hər hansı bir təşkilat tərəfindən istifadə edilə bilər.

ISO/IEC 27001 - məlumat təhlükəsizliyi idarəetmə sistemi standartıdır. Bu standart, məlumat təhlükəsizliyi risklərinin idarə olunması üçün tətbiq edilən bir çərçivə təqdim edir.

ISO/IEC 27002 - məlumat təhlükəsizliyi idarəetmə sistemi üçün praktika qaydasıdır. Bu standart, bir təşkilatda təhlükəsizlik nəzarətlərinin necə tətbiq edilməsi və təkmilləşdirilməsi haqqında məsləhətlər və tövsiyələr təmin edir. ISO/IEC 27002, bir İnformasiya Təhlükəsizliyi İdarəetmə Sistemi (ing. Information Security Management System ,ISMS) üçün tələbləri təyin edən ISO 27001 standartını dəstəkləyir.

ISO/IEC 27032 - "İnternet Təhlükəsizliyi - Təhlükəsizlik Vəzifələrinin Müəyyənləşdirilməsi və Tətbiqi üçün İdarəçilik" standardıdır. Bu standart, internet təhlükəsizliyi məsələləri ilə məşğul olan təşkilatlar üçün təhlükəsizlik vəzifələrinin müəyyənləşdirilməsi və tətbiqinə kömək edir.

ISO/IEC 27701 - "Məlumat Təhlükəsizliyi İdarəetmə Sistemi - Şəxsi Məlumatların Qorunması üçün Tələblər" standardıdır. Bu standart, məlumat təhlükəsizliyi idarəetmə sistemlərinin təhlükəsizlik məlumatlarının idarə olunması üçün şəxsi məlumatların qorunması tələblərini dəstəkləməyə kömək edir.

NIST CSF (Cybersecurity Framework)

ABŞ Milli Standartlar və Texnologiya İnstitutu tərəfindən hazırlanmış kibertəhlükəsizlik çərçivəsidir. Bu çərçivə, bir təşkilatın kibertəhlükəsizlik risklərini idarə etmək üçün bir quraşdırıcı, dinamik və səmərəli təklifat təmin edir. NIST, təhlükəsizlik proqramlarının inkişaf etdirilməsində, təhlükəsizlik proseslərinin təyin edilməsində və kibertəhlükəsizlik risklərinin dəyərləndirilməsində istifadə olunur.

FƏSİL II VEB MÜHİTDƏ MÖVCUD BOŞLUQLARIN VƏ TƏHDİTLƏRİN ANALİZİ.

2.1 Vebdə mövcud boşluqlar və təhdidlər

7 milyon veb-saytın təhlilinə əsaslanaraq, "SiteLock" bildirir ki, veb-saytlar hazırda hər gün orta hesabla 94 hücuma məruz qalır və həftədə təxminən 2608 dəfə botlar tərəfindən avtomatlaşdırılmış rejimdə yoxlanılır. Orta hesabla 4,45 milyon dollara başa gələn məlumat pozuntuları ilə veb-sayt təhlükəsizliyi təhdidlərinin ciddiliyini nəzərə almamaq olmaz.

Bu hücumlar müştəri itkisi, saytların əlçatanlığının pozulması və dayanma müddəti səbəbindən maliyyə itkilərinə səbəb olur və müştərilərin etibarını sarsıdır.Veb-sayt təhlükəsizliyinə təhdidlərin sayının artması, artan miqyası, mürəkkəbliyi və təsiri təhdidlərin proaktiv qarşısının alınması tədbirlərinə ehtiyacı vurğulayır.Bütün sistem müdaxilələrinin 70%-dən çoxu zərərli proqramla (malware) bağlıdır və bütün zərərli proqramların 32%-i internet vasitəsilə yayılır. Zərərli URL-ləri saxlayan saytların əsas kateqoriyaları bunlardır:

- İstehsalat (19,87% zərərli URL ehtiva edir)
- Shareware/torrents (11.84%)
- Sosial şəbəkə (8,71%)
- Əyləncə (8,63%)
- Tibb (7,66%)
- URL keçid dəyişdiricisi (5,81%)
- Digər (28,06%)

Aparılan araşdırmalar nəticəsində belə bir qənaətə gəlmək olar ki, internetdən istifadə edən hər kəs təhlükə altındadır. Və bu elmi iş internet istifadəçilərinin internetdən təhlükəsiz bir şəkildə istifadə edə bilmələri üçün sözü gedən təhdidlərin araşdırılması və qarşısının alınması üsullarının öyrənilməsini özündə ehtiva edir.

Ümumdünya Şəbəkəsi , aşkar edilmiş zəifliklərin və bildirilən təhlükəsizlik insidentlərinin sayında müvafiq artıma, eləcə də boşluqların sayının artmasına səbəb olan, getdikcə daha çox həssas məlumatların təqdim edildiyi veb proqramlar vasitəsilə

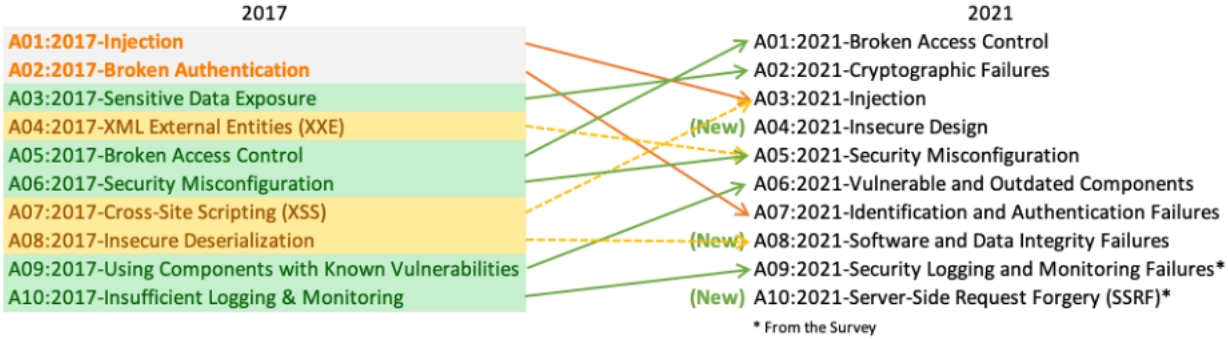
güclü informasiya paylaşma platformasına çevrilmişdir. Veb tətbiqi funksiyalarının genişləndirilməsi proqramların daha effektiv və sürətli cavab vermə qabiliyyətini artırdı. Bu, inkişafın ilkin mərhələlərində və proqram təminatının inkişaf dövrü boyunca təhlükəsizlik yoxlama nöqtələrinin və texnikalarının tətbiqi ilə təhlükəsiz veb proqramların inkişafının təkmilləşdirilməsinin çox güclü səbəbinə çevrilmişdir. Vebin populyarlığının artması və veb tətbiqlərinin genişlənməsi və demək olar ki, hər bir əsas sistemin hazırda veb texnologiyasından asılılığı səbəbindən veb tətbiqlərindəki zəifliklər vebi kiber cinəyatkarların əksəriyyəti üçün əsas diqqət mərkəzinə çevirmiş, buna görə də vebin hədəflənməsi əsas məsələ halına gəlmişdir (Peder Jungck, and Simon S.Y. Shim,2004).

Səhv kodlaşdırma, yanlış konfiqurasiya edilmiş veb serverlər, proqram dizayn qüsurları və ya formaların təsdiq edilməməsi nəticəsində yaranan sistem qüsurları da daxil olmaqla, müxtəlif səbəblərdən veb proqramlar hücuma məruz qala bilər. İstənilən veb tətbiqində hakerlərin daha yüksək səviyyədə istifadə edə biləcəyi ən azı bir boşluq var .

Resursların proqnozlaşdırıla bilən yeri, strukturlaşdırılmış sorğu dilivə kod tətbiqi üç əsas təhlükəsizlik pozuntusu idi və bütün veb tətbiq və tətbiq proqramlaşdırma interfeysi hücumlarının 64%-ni təşkil edirdi. 2023-cü ildə veb tətbiqetmələrə paylanmış xidmətdən imtina hücumu hücumlarının sayı 2022-ci illə müqayisədə 33% azalsa da, veb tətbiqetmələrində düşmən əməliyyatların tezliyi eksponent olaraq artaraq 500% oldu. Hal-hazırda hücumçular onlayn tətbiqetmələrə və onların infrastrukturuna daha çox diqqət yetirirlər və Xidmətdən imtina hücumları hücumları veb tətbiqləri hədəf alan daha mürəkkəb hücumlara keçir. Kibercinayətkarlar sındırılmış saytlardan zərərli proqramların yayılması, məxfi məlumatların oğurlanması kimi məqsədlər üçün istifadə edirlər. Bütün bunlar təşkilatın işini və nüfuzunu təhdid edir. Beləliklə, proqramı qorumaq və veb tətbiqindəki bütün potensial zəifliklərı aradan qaldırmaq yalnız bir seçim deyil, 2024-cü ildə təcili bir zərurətdir.

Açıq mənbə icması olan Açıq Veb Tətbiq Təhlükəsizliyi ən çox yayılmış veb tətbiqi zəifliklərinin icmalını yaratmaq və onları azaltmaq üçün sənayedə ən yaxşı təcrübələri təqdim etməklə interneti istifadəçilər üçün ən təhlükəsiz etmək məqsədi

daşıyır.OWASP Top 10 sadəcə veb proqram zəiflikləri siyahısı deyil. O, OWASP riskin qiymətləndirilməsi (ing.Risk Rating)metodologiyasından istifadə edərək hər bir zəiflik sinfini qiymətləndirir və hər bir risk üçün nümunələr, hücumların qarşısının alınması tövsiyələri və bağlantılar təqdim edir. OWASP-in ən yaxşı 10 veb tətbiqi zəifliyini araşdıraraq,proqram tərtibatçıları zərərli hücumlara gəldikdə istifadəçilərin təhlükəsizliyini qorumağa kömək edəcək daha təhlükəsiz proqram yaratmaq üçün konkret addımlar ata bilər. Şək.2.1 OWASP siyahısındakı 2017-ci ildən 2021-ci ilə qədər olan dəyişiklikləri görə bilərsiniz.



Şək.2.1.1 OWASP 2017-2021 müqayisəsi (https://owasp.org/Top10 , 2021)

Pozulmuş giriş nəzarəti (ing. Broken Access Control)

Pozulmuş giriş nəzarəti, veb təhlükəsizlik üçün vacib olan bir kiber təhlükədir. Bu, bir sayt və ya tətbiq proqramında düzgün şəkildə idarə olunmayan giriş imkanlarının istifadə edilməsi nəticəsində məxfilik və məhdudiyyətlərə əməl edilməyən məlumatların əldə edilə biləcəyi bir təhlükədir. Müəyyən bir sənəd, məlumat və ya funksiyanın ancaq müəyyən istifadəçilər tərəfindən çatdırılması təmin edilmir, bu da potensial istismara və məlumatların qeyri-müvafiq ələ keçirilməsinə gətirib çıxara bilər. Bu, nümunələrə icazəsi olmayan şəxslərə yetki verilməsi, istifadəçi sessiyalarının düzgün şəkildə idarə edilməməsi və ya səhifənin URL parametrlərinin dəyişdirilməsi ilə baş verə bilər (Butler W. Lampson,2004).

Kriptoqrafik Uğursuzluqlar (ing.Cryptographic failures)

Kriptoqrafik uğursuzluqlar, kriptoqrafiya tətbiqlərində görünən boşluq və zəifliklərdir. Bu uğursuzluqların arxasında, məlumatların qorunmasında istifadə olunan kriptoqrafik protokolların və alqoritmlərin düzgün şəkildə tətbiq edilməməsi,

anlaşılmazlıq və ya əksikliklər yatır. Bu uğursuzluqların əsasında bir sıra problemlər ola bilər:

- Müasir hesablama gücü ilə asanlıqla qırıla bilən zəif və ya köhnəlmiş şifrələmə alqoritmlərindən istifadə.
- Hətta güclü şifrələmə alqoritmləri düzgün tətbiq edilmədikdə uğursuz ola bilər. Ümumi səhvlərə defolt və ya sərt kodlu şifrələmə açarlarından istifadə, açarların düzgün saxlanmaması və ya ötürülmə və ya saxlama zamanı məlumatların açıqda qalmasına səbəb olan şifrələmə/deşifrləmə prosesindəki səhvlər daxildir.
- Açarların birdən çox sistemdə təkrar istifadəsi və ya açarların vaxtaşırı yenilənməməsi kimi zəif açar idarəetmə təcrübələri.
- Kriptoqrafik kitabxanalarda zəifliklər.Bir çox veb proqramlar şifrələmə tapşırıqları üçün üçüncü tərəfin kriptoqrafik kitabxanalarına etibar edir. Bu kitabxanalardakı veb tətbiqi zəiflikləri kriptoqrafik nasazlıqlara səbəb ola bilər, xüsusən də məlum problemlərin aradan qaldırılması üçün onlar müntəzəm olaraq yenilənmirsə.

Biz parollar, e-mail ünvanları, xəstənin sağlamlıq qeydləri, mülkiyyət biznes sirləri, kredit kartı məlumatı və s. haqqında danışırıq. Proqram avtomatik verilənlər bazası şifrələməsindən istifadə edərək kredit kartı məlumatlarını səylə şifrələyir. Bura kimi hər şey yaxşıdır, ancaq bu məlumat əldə edildikdə, dərhal şifrəsi açılır. Veb tətbiqlərindəki bu təhlükəsizlik zəifliyi, kredit kartı məlumatlarını açıq mətndən çıxarmaq üçün SQL inyeksiyasının uğursuzluğuna yol açır – biz buna həmçinin gözləyən hər hansı bir hücumçu üçün hazır fürsət də deyə bilərik.

İnyeksiya

İnyeksiya qüsuru veb proqramlardakı boşluqlardan biridir ki, bu da kiber hücumçuya proqram vasitəsilə zərərli kodu başqa bir sistemə ötürməyə imkan verir. Bu inyeksiyalar müxtəlif forma və ölçülərdə olur, o cümlədən SQL, CRLF, LDAP inyeksiyaları və s. həssas proqramlarda olan digər müştəriləri təhlükə altına almaqla geniş təsirə malikdirlər. Əslində, kod inyeksiyası (14%) və SQL inyeksiyası (11%) hücumları birlikdə bütün veb proqram hücumlarının dörddə birini təşkil edir [7].

Təhlükəli Dizayn (ing.Insecure Design)

OWASP Top 10 zəiflik siyahısına yeni daxil edilmiş bu kateqoriya təhlükəsizlik təhdidlərinin artmasına yol açan dizayn və memarlıq qüsurlarına diqqət yetirir. Təsəvvür edin ki, təhlükəsizlik nəzarətinin mükəmməl şəkildə həyata keçirilməsi və risklərin azaldılması üçün sərf olunan zəhmətli səylər yalnız təməl dizayn qüsurları ilə məhv edilir. Əsas struktur qüsurlu olarsa, hətta ən təcrübəli təhlükəsizlik tədbirləri belə hücumlara qarşı tab gətirə bilməz. Şübhəsiz ki, bacarıqlı hücumçular gec-tez bu veb proqram zəifliklərini araşdırıb taparaq istifadə edəcəkdir.

İdentifikasiya və Doğrulama Uğursuzluqları (ing.Identification and Authentification Flaws)

Getdikcə mürəkkəbləşən rəqəmsal dünyada autentifikasiya uğursuzluqları veb tətbiqlərində nisbətən ümumi təhlükəsizlik zəifliyidir. Veb tətbiqinizin istifadəçi identifikasiyası, autentifikasiyası və ya sessiyanın idarə edilməsi funksiyaları dəqiq yerinə yetirilmirsə və ya lazımi şəkildə qorunmursa, bu öz növbəsində böyük təhdidlərlə bizi üz-üzə qoya bilər.

Proqram təminatı və məlumatların tamlığı ilə bağlı nasazlıqlar (ing.Software and Data Integrity Failures)

Proqram təminatı və məlumatların tamlığı ilə bağlı nasazlıqlar, proqramlarda və sistemlərdə məlumatların düzgün şəkildə saxlanması, işlənməsi və ötürülməsi ilə bağlı yaranan problemləri ifadə edir. Bu cür nasazlıqlar, məlumatlarda yaradılan dəyişikliklərin proqram təminatı tərəfindən doğrulanması və ya proqram təminatının təhlükəsizliyinin zəif olduğu halları əhatə edir

Təhlükəsizlik Qeydiyyatı və Monitorinq Uğursuzluqları (ing.Security Logging and Monitoring Flaws)

Veb tətbiqi zəifliklərinizi izləmək üçün düzgün alətlər olmadan, mahiyyətcə statik naviqasiya edirsiniz. Beləliklə, qeydlər və monitorinq əsas hesabatlılığı təmin edir, sizə baş verənlər barədə aydın fikir verir, insident xəbərdarlığını işə salır və məhkəmə-tibbi araşdırmalar üçün mühüm yardım rolunu oynayır. Bu sistemlər uğursuz olarsa, bu, gəminin radarını söndürməyə bənzəyir - pozuntuları aşkar etmək və onlara reaksiya vermək qabiliyyətiniz ciddi şəkildə pozulur.

Server tərəfində sorğu saxtakarlığı (ing.Server Site Request Forgery,SSRF)

Bu, veb tətbiqini aldadan, gözlənilməz yerə saxta sorğu göndərən aldadıcı kiber boşluqdur. SSRF zamanı, hücumçu HTTP istəklərini, adətən serverin daxili və ya təyin edilmiş mövqelərində icra etmək üçün dəyişir. SSRF, hücumçunun şəbəkəyə daxil olmasına, yerli və ya xarici resurslara müraciət etməsinə və ya istifadəçilərə təsir etməsinə imkan verir. Bu, müvafiq qorunma tədbirləri olmadan serverlərdə ciddi təhlükələr yarada bilər. SSRF nümunələri arasında daxili serverlərə nəzarət və məlumatların əldə edilməsi, şəbəkəyə daxil olmaq və daxili servislərə hücum nümunələri yer alır.

Təhlükəsizliyin Yanlış Konfiqurasiyası (ing.Security missconfiguration)

Bu, təhlükəsizlik protokollarınız düzgün qurulmadıqda və ya səhvlər etdikdə baş verir. Bu o qədər də aşkar olmayan səhvlər proqramınızı, onun dəyərli məlumatlarını, bütün təşkilatınızı təhlükəli kiberhücum və ya haker istismarına məruz qoyaraq açıq təhlükəsizlik boşluqlarını ortaya qoyur. Bu veb proqram zəifliklər kibercinayətkarlar üçün asan hədəflər halına çevrilmiş olur.

Zəif və köhnəlmiş komponentlər (ing.Vulnerable and Outdated Conponenets)

Əksər onlayn proqramlar üçüncü tərəf çərçivələrindən istifadə etməklə qurulur. Beləliklə, tətbiqinizdə vurğuya nəzarət pozuntuları, icazəsiz giriş, SQL inyeksiyaları və digər təhlükələr kimi gözlənilməz hadisələrin baş verməsinə səbəb ola biləcək naməlum kodlar ola bilər.

2.2. Veb əsaslı təhdidlərin analizi

Veb əsaslı təhdidlər və ya onlayn təhdidlər internet üzərindən arzuolunmaz hadisə və ya hərəkətə səbəb ola biləcək kibertəhlükəsizlik riskləri kateqoriyasıdır.Veb təhdidləri son istifadəçi zəifliklər, veb-xidmət tərtibatçıları/operatorları və ya veb xidmətlərinin özləri tərəfindən yarana bilər. Məqsəd və səbəbdən asılı olmayaraq, veb təhlükəsinin nəticələri həm fərdlərə, həm də təşkilatlara zərər verə bilər.Veb əsaslı təhdidlər geniş şəkildə bir çox növə bölünür:

Saytlararası Skript (ing.Cross-Site Scripting, XSS)

XSS zəifliyi veb zəifliklər arasında geniş yayılmış bir zəiflikdir. XSS zəifliklərindən istifadə bir çox ciddi problemə səbəb ola bilər.Hücumçu müştəri skriptini veb səhifələrə və ya serverə və veb tətbiq plaginlərinə yerləşdirə bilər. Bu hücumlardan istifadə edərək saytda istifadəçilər üçün əlçatan olacaq zərərli məzmun yerləşdirə bilər. Viral məzmunu tətbiq etməklə hücumçu həssas səhifə məlumatlarına, sessiya məlumatlarına və brauzerin idarə etdiyi digər vacib məlumatlara səlahiyyətli giriş əldə edə bilər. Beləliklə, verilən hücum koddan istifadə edilən hücuma aiddir.Nümunə kimi qeyd etmək olar ki, 2006-cı ildə Beantovn haker Təşkilatı 2 milyon aktiv istifadəçisi olan bir onlayn platforma olan LiveJournal da XSS zəifliklərini aşkar etdilər (Rahul Johari and Pankaj Sharma,2012). Hücumçu zərərli kodu ehtiva edən çox sayda URL yaratdı və istifadəçiləri onlara keçməyə məcbur etdi. Qurbanlar bu URL-lərə daxil olduqları zaman, hücumçu istifadəçilərin kukilərini oğurlayıb qurbanların hesablarına daxil olmaq üçün istifadə edə bilirdi.

XSS Zəifliklərinin Təsnifatı

Əvvəlcə iki əsas XSS növü müəyyən edilmişdir: Saxlanılan XSS (ing.Stored XSS) və Qalıcı olmayan XSS (ing.Reflected XSS).Stored XSS, məlumatların serverdə saxlanılması zamanı hücum etdiyi XSS növüdür. Burada, hücumçu serverə pis niyyətlə işlədiləcək kod yerləşdirir və istifadəçilər o məlumatı oxuduğu zaman hücum edilir.Reflected XSS, URL-dəki parametrlər vasitəsilə hücum etdiyi XSS növüdür.Hücumçu, pis niyyətlə hazırlanmış bir URL vasitəsilə məlumatı göndərir və server tərəfindən qaytarılan cavabda bu məlumatlar göstərildiyi zaman hücum edilir.2005-ci ildə Amit Klein üçüncü növ XSS-növünü təyin etdi və bu yeni hücum növü Sənəd obyekti modeli (Document Object Model, DOM) əsaslı XSS olaraq adlandırıldı. DOM əsaslı XSS həmçinin tip-0 XSS kimi də tanınır. DOM əsaslı XSS, JavaScript kodunun istifadəçi tərəfindən dəyişdirilmiş məlumatlarla manipulyasiya edilməsi zamanı aktivləşir. Burada, hücumçu, səhifədə olan JavaScript kodunu pis niyyətlə hazırlanmış məlumatlarla dəyişdirir, bu da brauzerdə pis niyyətlə işlənə biləcək kodların işləməsinə səbəb olur. XSS boşluqları kuki məlumatlarının oğurlanmasına, DOS, DDOS, fişinq hücumlarına səbəb ola bilər.

Saytlararası Sorğu Saxtakarlığı

CSRF, istifadəçinin istifadə etdiyi bir veb səhifəsindən yararlanan hücumçunun istifadəçinin adına avtomatik olaraq HTTP istəkləri göndərməsinə imkan verən bir təhlükədir. Bu istəklər onun adı ilə serverə göndərilir. Bu, həm istifadəçi hesabları, həm də müvafiq brauzer istifadə olunaraq edilə bilər. CSRF əsasən o zaman istifadə olunur ki, "cinayətkar" öz qurbanının adından veb-sayt üzərindən şifrəsinin dəyişdirsin, şifrənin bərpası üçün istifadə olunan məxfi sözü əldə etsin, saytda istifadəçi hüquqlarını dəyişsin və s. Həmçinin CSRF-in köməyi ilə müxtəlif refleksiv (reflected) XSS hücümları həyata keçirə bilər.Uğurlu bir CSRF hücumu üçün qurbanın veb tətbiqində yaxşı bir sessiyaya sahib olması lazımdır. CSRF hücumunda, hücumçu, həssas veb-sayt GET metodundan istifadə edərsə, tələb olunan URL ilə HTML etiketindən istifadə edə bilər. Post metodundan istifadə edən sorğular üçün hücumçu JavaScript XML,HttpRequest və ya əvvəlcədən təyin edilmiş giriş formasını payload kimi istifadə edə bilər. Qurban daha sonra CSRF məlumatlarını ehtiva edən zərərli bir veb-saytına cəlb olunur. Qurban sayta daxil olduqda, qurbanın sessiyası haqqında məlumat olan əvvəlcədən təyin edilmiş sorğular avtomatik olaraq veb-sayta göndərilir və sorğular müvafiq olaraq işlənir. Qurban, özü də bilmədən, bütün bu sorğulara hücumçunun saytında cavab verir,nəticədə özünü təhlükəyə atmış olur.

Bugcrowd kiber təhlükəsizlik platformasının 2021-ci ildə apardığı bir araşdırmaya görə, CSRF zəifliyi platformanın ən çox yayılmış səhvləri siyahısında 8-ci yerdədir.Bununla birlikdə, bu hücum hələ də bir çox veb tətbiq developeri tərəfindən tez-tez nəzərə alınmır və elmi ədəbiyyatda nadir hallarda müzakirə olunur.Bu hücum, eyni zamanda qurbana pul köçürmək, parol dəyişdirmək və həssas məlumatları dəyişdirmək kimi bir çox zərərlər verə bilər.

Bu müdafiələri veb tətbiqlərə tətbiq etməzdən əvvəl hücumları təhlil etmək və müəyyənləşdirmək çox vacibdir. CSRF-nin aşkarlanması və istifadəsi digər böyük hücumlarla müqayisədə nisbətən asandır. İstifadəçi bu hücumun harada və necə edildiyini bilirsə, qarşısını almaq da nisbətən asanlaşır.

SQL inyeksiyası

Müasir veb-saytların və tətbiqlərin əksəriyyəti Strukturlaşdırılmış Sorğu dili (SQL) istifadə edərək proqramlaşdırılmış verilənlər bazalarına qoşulur. SQL

inyeksiyası, tətbiqlərin verilənlər bazasına sorğular gedən zaman soğunun pozulması ilə hücumçuın istifadə etdiyi bir üsuldur. Bu hücum hücumçuın veb məlumatlarını icazəsiz oxumaq və ya yazmaq imkanı verir. Bu hücumla hücumçu şəxsiyyəti dəyişdirə, verilənlər bazasındakı mövcud məlumatları dəyişdirə, etibarlılıq problemlərini aradan qaldıra, bütün məlumatların açıqlanmasına, məlumatlara zərər verə, ziyarətçilər üçün əlçatmaz edə və server zərərli hala gətirə bilər. SQL sorğularının tətbiqi ilə əlaqəli zəifliklər veb-saytdakı sorğulara qeyri-adekvat baxdıqda, filtrlədikdə, nəzarət edilmədikdə baş verir, bu da hücumçuların məlumat almaq üçün verilənlər bazası sorğularına SQL kod parçalarını daxil etməyə imkan verir. SQL inyeksiyasının bəzi növləri vardır:

Daxili SQLi (ing.İn-band SQLi): Bu, hücumçuların SQL Injection hücumlarını eyni kanal vasitəsi ilə yerinə yetirdikləri ən geniş yayılmış SQL Injection növüdür. Hücumçular, məlumat bazasına hücum etmək üçün istifadəçi daxil sahələrinə zərərlı SQL kodlarını yerləşdirirlər və nəticələri əldə etmək üçün eyni HTTP responsundan istifadə edirlər.

Səhv əsaslı SQLI (ing.Error-based SQLI): Bu növ SQL Injection, hücumçuların məlumat bazasından xəbərdarlıq xəbərləri əldə etmək üçün səhv mesajlarından istifadə etməsinə əsaslanır. Səhv mesajlarının detallarından yararlanan hücumçular, məlumat bazasının strukturunu və informasiyanın nəticələrini öyrənməyə çalışırlar.

Birləşmə əsaslı SQLI (ing.UNION-based SQLi): Bu, hücumçuların məlumat bazasından bir HTTP responsunu geri qaytarmaq üçün UNION SQL operatorundan istifadə etdikləri bir SQL Injection növüdür. Hücumçular, responsu qiymətləndirərək məlumat bazasının məzmunu barədə ipuclarını qiymətləndirə bilərlər.

Məntiqi (kor) SQLI (ing. Inferential (Blind) SQLI): Bu növ SQL Injection, hücumçuların məlumat bazasını sorğulamaq və serverin davranışını izləyərək məlumat bazasının strukturunu öyrənmək üçün istifadə olunur. Bu tip hücumlar daha yavaş olsa da, digər SQL Injection növləri kimi məlum informasiya aşkarlamaqda istifadə olunur.

Məntiqi (ing. Boolean): Bu, Blind SQL Injection üçün bir alt növ olaraq həyata keçirilir. Hücumçular, məlumat bazasına istədikləri sorğuları yerinə yetirmək üçün boolean (true/false) cavablarını qiymətləndirirlər. HTTP responsunun dəyişdirilməsi

və ya dəyişilməməsi ilə nəticənin doğruluğunu qiymətləndirərək məlumatlar əldə edirlər.

Zaman əsaslı (ing. Time-based): Bu, digər bir Blind SQL Injection alt növüdür. Hücumçular, məlumat bazasına göndərilən sorğuların nəticələrinin müəyyən vaxtda (saniyələr şəklində) cavablanmasını gözləyərək məlumatlar əldə edirlər.

Xarici interfeysli SQLI (ing. Out-of-band SQLI): Bu növ SQL Injection, eyni HTTP kanalını istifadə etmədən məlumat bazasına hücum etməyə imkan verir. Hücumçular, ayrı bir kanal vasitəsilə məlumat bazasına sorğular göndərərək informasiya əldə edirlər.

Spam hücumu.

Spam istənməyən kütləvi elektron mesajlar üçün istifadə olunan termindir. Elektron poçt spamın yayılmasının ənənəvi üsulu olsa da, sosial şəbəkə platforması spamın yayılmasında daha uğurludur (Xiaowei Li and Yuan Xue, 2011). Qanuni istifadəçilərin ünsiyyət detallarını asanlıqla şirkət saytlarından, bloqlardan və xəbər qrupundan əldə etmək olar. Hədəfə alınmış müştərini spam mesajlarını oxumağa və bu mesajların təhlükəsiz olduğuna inandırmaq çətin deyil. Spamların əksəriyyəti kommersiya reklamlarıdır, lakin istifadəçilərdən həssas məlumatlar toplamaq üçün də istifadə edilə bilər və ya viruslar, zərərli proqramlar və ya saxta fəaliyyətlər kimidə qarşımıza çıxa bilər.

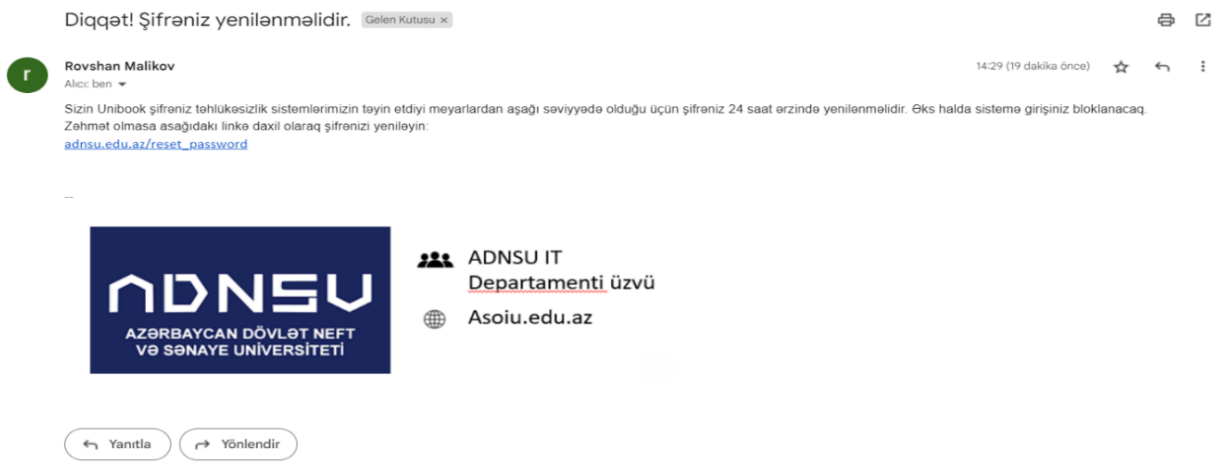
Fişinq hücumu (ing.Phising attack)

Fişinq hücumları onlayn əməliyyatlarda və xidmətlərdə iştirak edən çoxlu sayda təşkilatlara görə ən çətin sosial mühəndislik kiberhücumlarından biridir. Bu hücumlarda cinayətkarlar orijinal veb-saytın surətini çıxaran və məlumatları zərərli serverə göndərən giriş forması vasitəsilə istifadəçiləri etimadnamələrini və ya həssas məlumatlarını çıxarmaq üçün aldadırlar. Fişinq hücumu, hücumçunun istifadəçi adı, şifrə və istifadəçinin kredit kartı məlumatları kimi həssas məlumatları saxta veb-saytlar və real görünən e-poçtlar vasitəsilə əldə edə biləcəyi bir növ sosial mühəndislik hücumudur.

Bir çox fişinq hücum vektorlarında veb-sayta işarə edən URL olduğundan, biz veb-saytları hücumların son nöqtəsi kimi müəyyən edə bilərik. Anti-Fişinq İşçi Qrupu

(ing. Anti-Phishing Working Group , APWG) 2020-ci ilin son rübündə 611 877 unikal fişinq saytı aşkar edib. Bu hücumların əsas hədəfləri maliyyə institutları (24,9%), sonra sosial media (23,6%), Xidmət kimi proqram (ing.Software as a Service, SAAS) və veb-email xidmətləri (19,6%) və ödəniş platformaları (8,5%) olmuşdur(Steve Petite,2001). Fişinq kampaniyaları nəzərəçarpacaq təsirə malikdir, çünki açıqlanan şəxsi məlumatlar şirkətlərə 411 milyon ABŞ dollarından çox və istifadəçilərə milyonlarla ABŞ dolları dəyərində olan iqtisadi itkilərinə səbəb olmuşdur.

Bəzi nümunələr nəzər salsaq görərik ki,məsələn, adnsu.edu.az saytından saxta e-poçt mümkün qədər çox fakültə üzvünə kütləvi şəkildə paylanır. E-poçt istifadəçinin parolunun bitmək üzrə olduğunu iddia edir. Şifrəni 24 saat ərzində yeniləmək üçün adnsu.edu.az/reset_password saytına daxil olmaq üçün göstərişlər verilir. Şək.2.2.2 ümumi fişinq fırıldaqçılıq cəhdini göstərir:

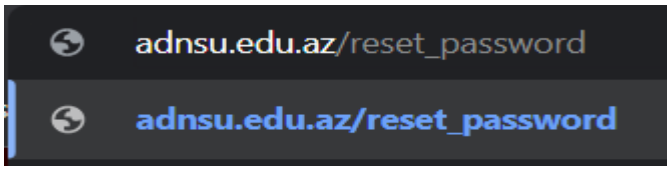


Şək.2.2.2 Fişinq nümunəsi (Rovshan Məlikov, 2022)

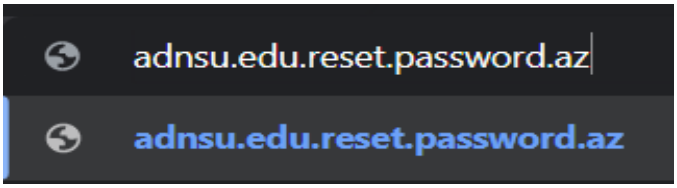
Linkə klikləməklə bir neçə şey baş verə bilər.Məsələn,istifadəçi myuniversity.edurenewal.com-a yönləndirilir,amma bu səhifə həm yeni, həm də mövcud parolların tələb olunduğu əsl yeniləmə səhifəsi kimi görünən saxta səhifədir. Səhifəni izləyən hücumçu universitet şəbəkəsindəki təhlükəsiz ərazilərə daxil olmaq üçün orijinal parolu oğurlayır.İstifadəçi faktiki parol yeniləmə səhifəsinə göndərilir. Bununla belə, yönləndirilərkən zərərli skript istifadəçinin sessiya kukisini oğurlamaq üçün arxa planda aktivləşir. Bu, cinayətkarın universitet şəbəkəsinə imtiyazlı giriş imkanı verən əks olunan XSS hücumu ilə nəticələnir.

E-poçt fişinqi

E-poçt fişinqi söz oyunudur. Minlərlə saxta mesaj göndərən bədiyyətli şəxslər, alıcıların yalnız kiçik bir faizi tələyə düşsə belə, əhəmiyyətli məlumat və külli miqdarda pul əldə edə bilər. Yuxarıda göründüyü kimi, bədniyyətli şəxslərin müvəffəqiyyət nisbətlərini artırmaq üçün istifadə etdiyi bəzi üsullar var.Birincisi, onlar saxta təşkilatdan gələn faktiki e-poçtları təqlid etmək üçün fişinq mesajlarının hazırlanmasında çox səy göstərirlər. Eyni ifadələrdən, şriftlərdən, loqolardan və imzalardan istifadə mesajların qanuni görünməsinə səbəb olur.Şək.2.2.3 və şək.2.2.4-dəki nümunədə adnsu.edu.az/reset_password URL-si adnsu.edu.reset.password.az olaraq dəyişdirildi. İki ünvan arasındakı oxşarlıqlar təhlükəsiz bir əlaqə təəssüratı yaradır, bu da alıcının hücumun baş verdiyindən xəbərdar olması ehtimalını azaldır.



Şək.2.2.3 (Rovshan Məlikov, 2022)



Şək.2.2.4 (Rovshan Məlikov, 2022)

Spear fişinqi (ing. Spear phishing)

Spear phishing, təsadüfi tətbiq istifadəçilərindən fərqli olaraq, müəyyən bir şəxsi və ya müəssisəni hədəf alır.

Bu, təşkilat, o cümlədən onun güc strukturu haqqında xüsusi bilik tələb edən fişinqin daha dərin versiyasıdır.

Asanlıqla oğurlana bilən şəxsi məlumatlara aşağıdakılar daxildir:

1. Sosial təminat nömrəsi
2. Bank hesab nömrəsi
3. Kredit kartı məlumatları
4. E-poçt ünvanı

5. Tibbi qeydlər
6. Telefon nömrəsi

XML yol inyeksiyası (ing. XPath injection)

XPath inyeksiyası bir hücum növüdür. Bu, XML path (XML path) sorğularından istifadə edərək hazırlanmış bir tətbiqə zərər verir. Bu dil XML sənədlərindən qovşaqları seçə bilər. Bu tip hücum, məlumatların alınması üçün XPath sorğusu istifadəçinin veb-saytında verdiyi məlumatlardan istifadə edərək hazırlandıqda baş verir. Hücumçu sadəcə veb-sayta pozulmuş məlumatları asanlıqla əlavə edə və XML məlumatlarının quruluşunu əldə edə və onlara daxil ola bilər.

XML sorğu inyeksiyası (ing.XQuery injection)

XQuery funksional proqramlaşdırma dilidir. Toplanmış məlumatları XML formatına çevirir. Bu hücum məlumat zərərli mənbə tərəfindən daxil edildikdə baş verir. XQuery Injection XML XQuery Dilinə qarşı klassik SQL inyeksiya hücumunun variantıdır. XQuery Injection, XQuery əmrlərinə ötürülən düzgün olmayan təsdiqlənmiş məlumatlardan istifadə edir. Bu qayıdış, hücumçu adından XQuery rutinlərinin daxil ola biləcəyi əmrləri yerinə yetirəcək. XQuery inyeksiyası qurbanın mühitindəki elementləri sadalamaq, yerli hosta əmrlər yeritmək və ya uzaq fayllar və məlumat mənbələrinə sorğuları yerinə yetirmək üçün istifadə edilə bilər. SQL inyeksiya hücumları kimi, hücumçu resurs giriş qatını hədəfləmək üçün proqram giriş nöqtəsi üzərindən keçir.

Link İzləmə (ing. Link Traversal)

Hücumçular müəyyən veb-saytlarının URL-larını izləyərək artıq mövcud olmayan və ya mövcud olan bəzi linkləri və URL-ləri öyrənirlər. Bu linklər hələ də veb tətbiqdən silinməmiş dəyərli məlumatlara çatmağa imkan verə bilər.Link Traversal hücumçuların veb-sayt serverindəki məhdud fayllara və qovluqlara icazəsiz giriş əldə etməsinə imkan verən bir kiberhücum növüdür. Bu, Şəxsi məlumatlar, Giriş etimadnaməsi və maliyyə məlumatları kimi həssas məlumatlara icazəsiz girişə və e-mail və sosial media kimi onlayn hesabların güzəştə getməsinə səbəb ola bilər.

Yanlış yönləndirmə (ing.Path Truncation)

Yanlış yönləndirmə hücumu veb proqram və ya xidmətdə URL-lərin (Uniform Resource Locator) yollarını manipulyasiya etməklə həyata keçirilən hücum növüdür. Bu hücumda təcavüzkar URL-in yol hissəsini dəyişdirərək tətbiqdə tələb olunanlardan başqa müxtəlif fayl və ya səhifələrə daxil olmağa çalışır.

Bu cür hücumlar tez-tez server tərəfindəki zəifliklərdən, məsələn, qeyri-adekvat giriş nəzarəti və ya düzgün yolun təsdiq edilməməsi nəticəsində yaranır. Yolun kəsilməsi hücumları təcavüzkarın həssas məlumatlara və ya sistemə giriş əldə etməsinə və vacib məlumatlara zərər verməsinə imkan yarada bilər.

Kobud güc hücumu (ing.Brute force)

Bu, əsasən veb-sayt və ya hədəf istifadəçi, hücumçuın onları təxmin etməsi və hücumu həyata keçirməsi lazım olduqda proqnozlaşdırılan sessiya identifikatorlarından istifadə edərsə işləyir. Başqa bir ssenari, hücumçuın zəif təhlükəsizlik tədbirləri olan bir veb-saytdan sessiya identifikatorlarının siyahısına daxil olmasıdır.

FƏSİL III VEB-SAYTLARDA MÖVCUD OLAN BOŞLUQLARIN VƏ TƏHDİTLƏRİN AŞKARLANMASI VASİTƏLƏRİ VƏ ÜSULLARI

3.1 Aşkarlama metodlarının analizi

Bu fəsil, veb-saytlarda və platformalarda mövcud olan boşluqların və təhdidlərin aşkarlanması üsullarının metodologiyasını təqdim edir. Veb-saytlarının və platformaların artan kompleksliyi, onların məxfilik, təhlükəsizlik və funksional keyfiyyətinin əsas məqamlarından biri halına gəlmişdir. Bu səbəblə, bu iş, veb-saytlarının və platformaların təhlükəsizliyini təmin etmək və onları potensial təhlükələrə qarşı qorumaq üçün vacibdir.

Bu fəsilin məqsədi, veb-saytlarda və platformalarda mövcud olan boşluqların və təhdidlərin aşkarlanması prosesinə geniş bir baxış verməkdir. Bu, mövcud metodologiyaların və texnologiyaların təhlükəsizliyin təmin edilməsi üçün nə qədər effektiv olduğunu və necə tətbiq edilə biləcəyini araşdırır. Fəsil, əsasən aşkarlama metodlarının analizini hədəfləyir və bu metodlar veb-saytlarının və platformalarının müdafiəsinin mühüm hissələrindən birini təşkil edir.

Hücumların aşkar olunması üçün klassik yanaşmalar.

1. İmza əsaslı aşkar edilmə:Bu cür aşkarlama üsulları artıq aşkar edilmiş hücumları aşkar etmək üçün effektivdir. Bu üsullar hər yeni gələn paketi artıq aşkarlanmış məlum hücumların siyahısı ilə təsdiqləyir. Bu üsul bir çox hücum növünə qarşı effektiv təsir göstərsə də 0-gün hücumlarını (ing. zero-day attacks) aşkar edə bilmir. O, proqram səhvlərini yəni “false positive”–ləri müəyyən edə bilər. Bu aşkarlama üsulu virus proqram təminatı satıcıları tərəfindən istifadə edilir.

2. Bilik əsaslı aşkarlama:Bu tip hücum aşkarlama sistemi sistem zəifliklərı və əvvəlki hücumların təsviri haqqında məlumatları özündə saxlayır və şübhəli istifadəçi davranışlarını aşkar edə bilir. İstifadəçi davranışları normal və anormal olmaqla iki sinifdən ibarətdir. Normal davranış istifadəçi profili kimi müəyyən edilir, digər sinif isə kibercinəyətkarın anormal davranışını ehtiva edir.

3. Statistikaya əsaslanan aşkarlama:Bu texnika şəbəkənin normal fəaliyyətini müəyyənləşdirir. Əgər bəzi fəaliyyətlər normal fəaliyyətlərin əhatə dairəsini keçərsə, bu, zərərli fəaliyyət kimi qiymətləndiriləcəkdir. Bu sistem daha dəqiq nəticələr əldə etmək üçün şəbəkədəki trafik sxemlərinə davamlı olaraq nəzarət edir. Sonra bu sistemlər mürəkkəb statistik alqoritmdən istifadə edərək trafiki təhlil edir və sonra trafik nümunələrində hücumları müəyyənləşdirir. Bu texnika bir hədd dəyərindən istifadə edir və hər paket üçün anomaliya hesabını yaradır. Paketin anomaliya xalı həddən artıq böyükdürsə, paket zərərli hadisə kimi qəbul edilir və xəbərdarlıq mesajı verir.

4. Davranış əsaslı aşkarlama:Həm adi, həm də zərərli proqramların davranışı kod tələblərindən asılıdır. Bu, bayt ardıcıllığının yoxlanılmasını tələb etməyən hücumların vacib xüsusiyyətlərini müəyyən etməyə imkan verir. Bu davranışa əsaslanan hücum aşkarlama metodunun əsas məqsədi veb tətbiq serverinin gələcək davranışını müəyyənləşdirməkdir. Bu metod şəbəkə trafik axınının proqnozlaşdırma qabiliyyətindən asılıdır.

5. Hibrid əsaslı aşkarlama:Yuxarıda göstərilən bütün metodların üstünlükləri və mənfi cəhətləri var. Hibrid metodlar statistika, bilik, imza və davranışa əsaslanan metodları birləşdirir. Bütün metodların üstünlüklərini birləşdirir, çatışmazlıqları aradan qaldırır və daha yaxşı nəticələr verir. Bu hibrid metod veb tətbiqləri sıfır gün hücumlarından uğurla qorumağa nail olur.

Hücumların aşkarlanması üçün hazırlanmış üsullar:

Etibarsız yönləndirmə və aşkarlama sistemi metodu

Ashish Kumar altı maşın öyrənmə təsnifat alqoritmlərini, yəni qərar ağacı (ing. decision tree), təsadüfi meşə (ing. random forest), ADA gücləndirmə (ing. Adaptive Boosting), dəstək vektor maşını (ing. support vector machine), xətti reqressiya (ing. linear regression) və neyron şəbəkəsini tədqiq etmişdir (Kumar, D. Garg and P. S. Rana, 2015). Performansa əsasən, ansambl modelini təkmilləşdirmək üçün üç alqoritm seçilir. Bu ansambl modeli təklif olunan sistemlərdə profil hücumlarını aşkar etmək

üçün istifadə olunan neyron şəbəkəsi, SVM və təsadüfi meşə alqoritmindən ibarətdir. Model 10 oK film verilənlər bazası[1] ilə sınaqdan keçirilib.

Etibarsız yönləndirmə aşkarlama sistemi qara qutu (black box) skan etmə texnikasından istifadə etməklə Linux-da həyata keçirilən ilk təhlükəsizlik texnikasıdır. Etibarlı olmayan yönləndirmə və irəliyönləndirmələri aşkar etmək üçün bir sistemdir. Bu, tipik olaraq veb tətbiqlərində mövcud olan və saytların mənimsədiyi potensial təhlükələri azaldan bir təhlükəsizlik mənbəyidir. URFDS, hücumların növünü, tipini və mənbəyini aşkar etmək üçün müxtəlif alqoritmlər və texnologiyalar istifadə edir.

URFDS-in arxitekturu aşağıdakı əsas komponentlərdən ibarətdir:

Log məlumatları toplama: Sistem, hücumları aşkar etmək üçün əvvəlcədən müəyyən edilmiş alqoritmlərə əsaslanan log məlumatları toplayır. Bu loglar, hücumların müəyyən edilməsində kritik önəmə malikdir.

Verilənlərin analiz edilməsi: Toplanan log məlumatları, alqoritmlər tərəfindən müvafiq formata çevrilir və analiz edilir. Bu analizlər, etibarlı olmayan yönləndirmə və irəliyönləndirmə hallarını təyin etməyə kömək edir.

Hücumların aşkar edilməsi: URFDS, verilənlərin əsasında etibarlı olmayan yönləndirmə və irəliyönləndirmə hallarını aşkar etmək üçün fərqli alqoritmlər və metodologiyalar istifadə edir. Bu alqoritmlər, hücumların növünə və mənbəsinə görə müxtəlif təhlillər aparır.

Nəticələrin qiymətləndirilməsi: Alqoritmlərin işləməsindən sonra əldə edilən nəticələr, hücumların növünü və şiddətini qiymətləndirmək üçün nəzarət edilir və dəyərləndirilir.

Zərərli yönləndirmə hallarının bloklandırılması: Nəticələrə əsasən, sistem etibarlı olmayan yönləndirmə və irəliyönləndirmə hallarını bloklamaq üçün müvafiq tədbirlər götürür.

URFDS adlı sistemimiz, web tətbiqlərində URF təhlükəsizliyini aşkar etmək üçün dörd əsas komponentdən ibarətdir: bir spider, bir analizator, bir modifikator və bir filter. Sistemin ümumi arxitekturu Şək.3.1.1-də verilmişdir.

[1] https://movielens.org/movies/2959

Sistem, məntiqi düzgünlüyünü test edərək və 142,522,691 unikal linkdə hücumları taparaq doğruluğunu sübut etmişdir. Bu sistem, əvvəlki sistemlər tərəfindən tanımlanmayan bəzi hücumları da tapmışdır (Jing Wang , Hongjun Wu "URFDS" 2015).

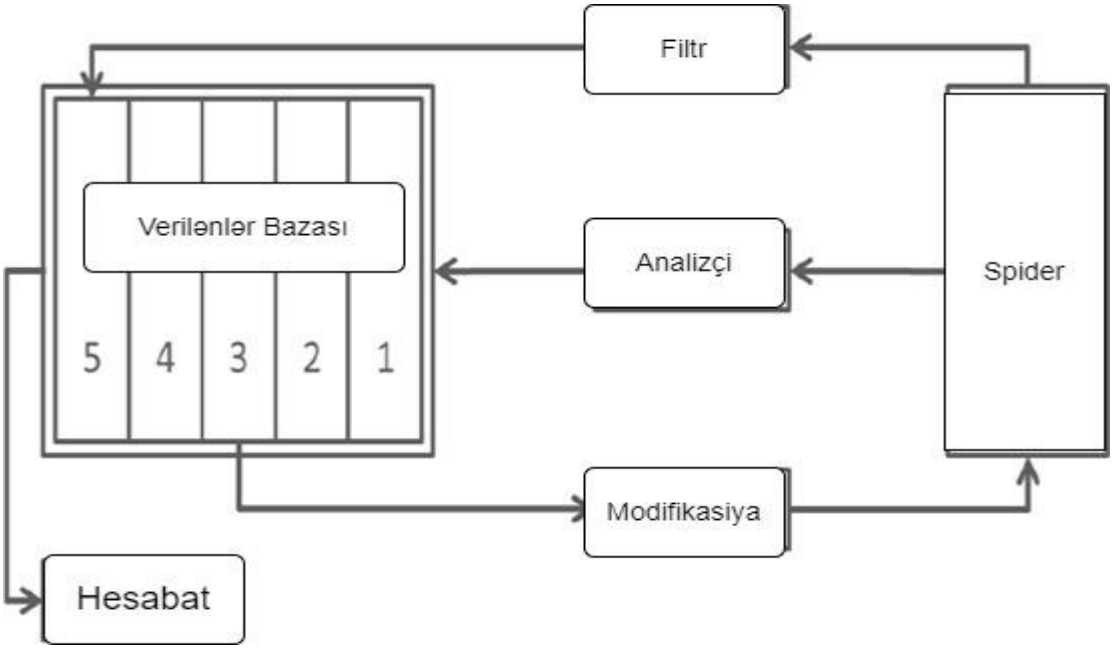
"Spider" komponenti, URFDS sisteminin bir hissəsidir və veb səhifələrindən məlumat toplamaq üçün istifadə olunur. Bu komponentin iş prinsipi aşağıdakı kimi işləyir:

1. Veb səhifələrinin toplanması: Spider, əsasən, bir axtarış motoru kimi davranır və verilmiş URL-ləri istifadə edərək veb səhifələrini toplayır.
2. Linklərin çıxarılması: Spider, alınan veb səhifələrindən linkləri tapır və onları ayrıca yaddaşa alır.
3. Yeniləmələr: Spider, əvvəlcədən yaddaşa alınmış linkləri də yeniləyə bilər. Yeniləmə prosesi, yeni məlumatların əldə edilməsi və mövcud olan linklərin dəyişdirilməsi ilə bağlı olaraq fərqli olabilir.
4. Yaddaş: Spider, alınan veb səhifələrindən əldə edilmiş məlumatları yaddaşda saxlayır. Bu, digər komponentlər üçün linklərin və səhifə məlumatlarının əlçatanlığına imkan verir.

Bu prinsip əsasında, spider, URFDS sistemi üçün əsas məlumat toplama və işləmə proseslərində mühüm bir rol oynayır.

Analizator, URFDS sisteminin bir hissəsidir və linklərin strukturunu təyin etmək üçün istifadə olunur. İş prinsipi aşağıdakı kimi işləyir:

1. Parametrlərin və HTTP prefixlərin yoxlanılması
2. Linklərin strukturunun təyini
3. Məlumatların bazada saxlanılması
4. Təhlükəli linklərin aşkar edilməsi



Şək.3.1.1 URFDS sistem arxitekturası (Jing Wang, 2015)

Analizator, URFDS sisteminin təhlükəli linkləri aşkar etmək üçün əsas mexanizmlərindən biridir.

Modifier, URFDS sisteminin bir hissəsidir və linkləri dəyişdirərək yeni testlər üçün yeni linklər yaradır. İş prinsipi aşağıdakı kimi işləyir:

1. Yaddaşdakı linklərin dəyişdirilməsi
2. Yeni linklərin yaradılması
3. Təhlükəli linklərin aşkar edilməsi

Modifier, URFDS sisteminin linkləri dəyişdirərək yeni testlər və yeni linklər yaratmaq üçün əsas funksionallığı icra edir.

Filter, Unvalidated Redirects and Forwards Detection System (URFDS) sisteminin bir hissəsidir və yönləndirmə URL-inin təsdiqlənib-təsdiqlənmədiyini yoxlayır. İş prinsipi aşağıdakı kimi işləyir:

1) Yönləndirmə URL-lərinin yoxlanılması
2) Təhlükəsizlik təsdiqləməsi
3) Məlumatın təsdiqlənməsi

Filter, URFDS sisteminin təhlükəli linkləri filtrləmək və təhlükəsiz linkləri təsdiqləmək üçün əsas funksionallığı icra edir. URFDS, veb tətbiqlərinə hücumların qarşısını almaq üçün vacib sayılan alətlər sırasındadır və bu sistem hücumların aşkar edilməsi və məhdudiyyətlənməsi üçün təhlükəsizlik həllərini özündə ehtiva edir.

Şək.3.1.2 də URFDS üçün kod nümunəsi nəzərdən keçirərək sistemin işləmə prinsipi yaxından analiz etmək olar.

```python
import urllib.parse

def is_valid_url(url):
    # Yönləndirmə URL-lərinin təhlükəsizliyini yoxlamaq üçün əlavə təhlükəsizlik yoxlamaları edilə bilər
    # Bu nümunədə, sadə bir yoxlama üçün URL-də "http" və "https" prefikslərinin olub-olmadığı yoxlanılır
    if url.startswith("http://") or url.startswith("https://"):
        return True
    return False

# Nümunə üçün, URL-lərin siyahısını göstərir
urls = [
    "http://www.example.com",
    "https://www.example.com",
    "ftp://www.example.com",
    "http://www.example.com/redirect?url=https://www.example.com/redirected",
    "https://www.example.com/redirect?url=https://www.example.com/redirected"
]

for url in urls:
    if is_valid_url(url):
        print(f"{url} - Təhlükəsiz")
    else:
        print(f"{url} - Təhlükəsiz deyil")
```

Şək.3.1.2 URFDS üçün kod nümunəsi (Sevda Xıdırova, 2024)

FAR IDP metodu

Qeyri-səlis assosiasiya qaydasına əsaslanan müdaxilənin aşkarlanması və qarşısının alınması sistemi, e-ticarət veb aplikasiyalarında müdaxilə üçün assosiasiya qaydalarının təyin edilməsi və istifadə edilməsi ilə əlaqədardir. Bu sistem, müxtəlif məhsulların satın alınması ilə bağlı məlumatları təhlil edir və bu məlumatlar əsasında assosiasiya qaydaları yaradır. Məsələn, müştərilərin birgə alıb-satmağa meyilli olduğu məhsullar təyin edilir və bununla bağlı qaydalar qurulur (Gaik-Yee Chana, Fang-Fang Chuaa and Chien-Sing Leeb, 2015).

Bu qaydalar vasitəsilə, sistemin normal fəaliyyətlərə uyğunluğu qiymətləndirilir və normadan fərqli olan zərərli fəaliyyətlər aşkar edilir. Bu təhlil prosesi, sistemin qaydaların ətraflı təhlilinə əsaslanmasını təmin edir və zərərli fəaliyyətlərin müəyyən edilməsində kömək edir.

Müəyyən edilmiş zərərli fəaliyyətlərə cavab olaraq, sistemin müdaxilə prosesi işə salınır. Bu proses, müştərilərlə əlaqə saxlanılması, şübhəli fəaliyyətlərin səbəblərinin təyin edilməsi və qarşının alınması kimi addımları özündə saxlayır.

FAR IDP sistemi, e-ticarət veb aplikasiyalarında istifadə olunan və assosiasiya qaydalarına əsaslanan bir müdaxilə sistemi və alqoritmidir Şək.3.1.4. Bu sistem,

müəyyən qaydalara əsaslanan bir alqoritm ilə təhlükəli fəaliyyətləri aşkar etməyə və qarşısını almağa kömək edir. İş prinsipi aşağıdakı kimi işləyir:

1.Assosiasiya qaydalarının təyin edilməsi

2. Müdaxilənin aşkar edilməsi

3. Fəaliyyətin qarşısının alınması

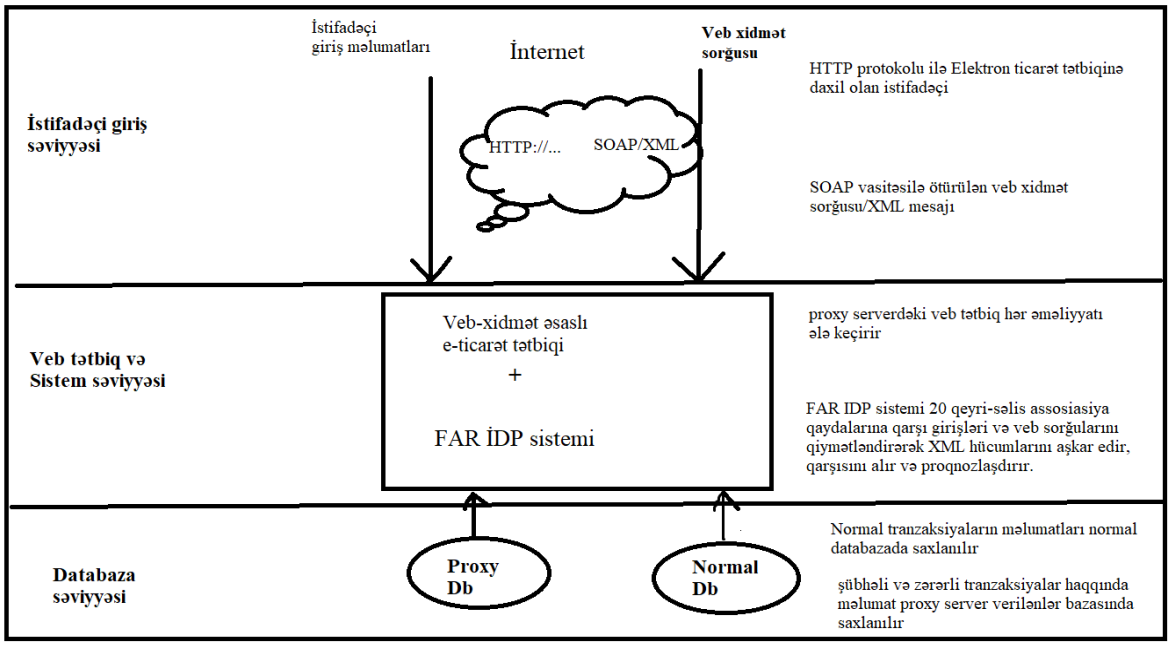
4.Yenilənə bilən sistem

Şək.3.1.3 də, "mlxtnd" kitabxana funksiyası ilə assosiasiya qaydalarının təyin edilməsi və təhlili üçün tətbiq edilən bir python kodu var. Bu kod, məlumat setindən assosiasiya qaydalarını təyin etmək üçün Apriori alqoritmini istifadə edir və sonra zərərli fəaliyyətlərin aşkarlanması, qarşısının alınması və müdaxilə etmək üçün nəzərdə tutulmuş bir hissədən ibarətdir.

```python
# Məlumatların yaradılması
data = [
    {'mehsul': 'X', 'musteri': 'A'},
    {'mehsul': 'Y', 'musteri': 'A'},
    {'mehsul': 'X', 'musteri': 'B'},
    {'mehsul': 'Z', 'musteri': 'B'},
    # Digər məlumatlar ...
]

# Assosiasiya qaydalarının təyin edilməsi
from mlxtend.frequent_patterns import apriori
from mlxtend.frequent_patterns import association_rules

df = pd.DataFrame(data)
hot_encoded_df = df.groupby(['musteri', 'mehsul']).size().unstack().fillna(0)
frequent_itemsets = apriori(hot_encoded_df, min_support=0.2, use_colnames=True)

# Assosiasiya qaydalarının təhlili
rules = association_rules(frequent_itemsets, metric="lift", min_threshold=1)

# Zərərli fəaliyyətlərin aşkarlanması və qarşısının alınması
for index, row in rules.iterrows():
    if row['lift'] > 1:  # Təhlükəli qaydaları təyin etmək üçün müəyyən bir metrik istifadə edilə bilər
        print("Təhlükəli assosiasiya:", row['antecedents'], "->", row['consequents'])
        # Zərərli fəaliyyətə qarşı addımlar atılması

```

Şək.3.1.3 (İbrahim Seyfullayev, 2024)

FAR IDP sistemi, süni intellekt alqoritmlərindən və assosiasiya qaydalarının tətbiqindən istifadə edir. Bu, e-ticarət veb aplikasiyalarında zərərli fəaliyyətlərin aşkarlanması və qarşısının alınması üçün effektiv bir yanaşmadır. Honeypot sistemi ilə FP-growth və Hidden Markov Modellərindən istifadə etməklə təklif olunan veb tətbiqlərində zərərli fəaliyyətin aşkarlanması həyata keçirir. Veb server tərəfində təcavüzkarın davranışını aşkar edir və proqnozlaşdırır. Bu, server və müştərilər arasında keçmiş qarşılıqlı əlaqə davranışına əsaslanır.



Şək.3.1.4 FAR IDP sistem arxitekturası (Gaik-Yee Chana, Fang-Fang Chuaa and Chien-Sing Leeb , 2015)

Joza metodu

Hiper-mətnli preprosessor (Hipertext preprocessor ,PHP) əsaslı proqramlarda SQL inyeksiya hücumlarını aşkar etmək üçün *Joza* metodu həyata keçirilir. Joza, mənfi və müsbət nəticə çıxarmağın üstünlüklərini birləşdirən hibrid yanaşmadır. Joza-nın təhlükəsizliyi WP-SQLI-LAB test üsulundan istifadə etməklə qiymətləndirilir. Bu metod SQL inyeksiya hücumlarının aşkarlanması üçün dəqiqdir. Joza metodikası, SQL inyeksiyası kimi yayılmış veb tətbiqləri üzərindəki zərərli fəaliyyətləri aşkar etmək və müdafiə etmək üçün inkişaf etdirilmiş bir təsir müəyyən etmə metodikasıdır. Bu metodika, hibrid bir təsir müəyyən etmə metodikasıdır və təhlükəli girişləri aşkar etmək üçün müxtəlif məlumatlardan istifadə edir (Naderi-Afooshteh, Anh Nguyen-Tuong, M. Bagheri-Marzijarani, J. D. Hiser and J. W. Davidson, 2015).

Joza metodikasının əsas mərhələləri aşağıdakılardır:

1. Verilənlərin izlənməsi: Joza, veb tətbiqinin girişlərini izləyərək bu girişləri təhlil edir. Bu, təhlükəli girişləri aşkar etməyə kömək edir.

2. Təsirli təhlil: Joza, izlədiyi girişləri hibrid təsir müəyyən etmə ilə təhlil edir. Bu metodika, məlumatın nəzarət dövrünü izləmək və məlumatların necə dəyişdirildiyini anlamaq üçün zərərli girişlərin təhlilindən istifadə edir.

3. Nəticələrin təhlili: Joza, təhlükəli girişlərin nəticələrini təhlil edir və hücumun məqsədini və potensial ziyanını qiymətləndirir.

4. Mühafizə tədbirlərinin tətbiqi: Joza, təhlükəli girişlərin aşkar edilməsindən sonra mövcud olan təhlükəni aşmaq üçün mühafizə tədbirləri tətbiq edir.

Joza metodikası, veb tətbiqlərinin mühafizəsini artırmaq və SQL injection kimi yayılmış təhlükələrə qarşı mübarizədə müvəffəqiyyətlə tətbiq edilmiş bir təsir müəyyən etmə metodikasıdır.

Onlayn sosial şəbəkələrdə XSS, SQL kimi hücumları aşkarlaya bilən yeni sistem təklif edilmişdir. Bu sistem Alternativ qərar ağacı (Alternating Decision, AD) təsnifatı və təkmilləşdirilmiş n-qram modelinin hibrid formada birləşdirilməsi ilə həyata keçirilir. Təsnifatdan istifadə edərək sistem veb-səhifələrin xüsusiyyətlərinin sayını müəyyən edir və hücumların aşkarlanması üçün təsnifatlandırıcı yaradır. Sonra veb-səhifələri təsnif etmək üçün artıq çıxarılan xüsusiyyətlərdən n-qram modeli hazırlanır. N-gram modeli, bir mətnin ardıcıl sözlər, hərflər və ya simvollar dəsti arasında müəyyən bir sıxılığın müşahidə edilməsində istifadə olunan bir təhlil metodikasıdır. N-gram modeli, bir mətni n sayda ardıcıl hissəyə (n-grama) bölərək hər bir hissənin neçə dəfə təkrarlandığını və bu hissələrin növünü müəyyənləşdirir. Əsasən, 2-gram (bi-gram), 3-gram (tri-gram) və s. olmaqla istifadə olunur.

N-gram modelinin əsas prinsipi, bir mətnin ardıcıl hissələrindəki çoxluğu və sıxlığı analiz etməkdən ibarətdir. Bu, mətnin strukturunu, dil xüsusiyyətlərini və məzmununu anlamağa kömək edir. N-gram modelləri dil modelləşdirmə və mətn sinifləndirmə kimi mətn işləmə tətbiqlərində geniş miqyasda istifadə olunur. Şək.3.1.5-dəki sadə nümunə də SQL inyeksiyasının qarşısının alınması üçün Python-da n-qram və AD ağac modelinin işləmə prinsipi öz əksini tapır, lakin real dünya tətbiqlərində istifadə olunan üsullar daha mürəkkəbdir.

```python
from flask import Flask, request

app = Flask(__name__)

# SQL inyeksiyasının yoxlama funksiyası
def process_query(query):
    # Gelen sorguda təhlükəli ola biləcək ifadələrin yoxlanılması
    if "DROP" in query.upper() or "DELETE" in query.upper() or "UPDATE" in query.upper():
        return "Təhlükəli sorgu"
    # Təhlükəli ifadə yoxdursa sorgu işlənir
    # Burada verilənlər bazasına qoşularaq sorgu işlədilə bilər
    return "Sorgu uğurla işləndi"

@app.route('/')
def home():
    return 'SQL inyeksiyasının yoxlanması Nümunəsi'

@app.route('/query', methods=['POST'])
def query():
    # POST istəyindən gələn SQL sorgusu alınır
    query = request.form['query']
    # SQL sorgusu işlənir
    result = process_query(query)
    return result

if __name__ == '__main__':
    app.run(debug=True)
```

Şək.3.1.5 N-gram ilə SQL sorğularının yoxlanılması (Kənan Həsənov, 2024)

N-gram modelləri hər bir n-gramın çoxluğuna və ardıcıl hissələrin sıxlığına əsaslanaraq mətnin xarakteristikalarını qiymətləndirir. Bu, mətnlərdəki hər hansı bir üstünlükləri, tipik olmayan strukturları müəyyən etməyə və hücumları aşkar etməyə kömək edə bilər. Nəhayət, onlayn sosial şəbəkələrdə XSS hücumlarını müəyyən etmək üçün hər iki yanaşmanı birləşdirildi. Sistem sübut edir ki, klassifikatorun və n-gram modelinin birləşdirilməsi bu iki metodun birlikdə işləyərək daha effektiv bir nəticə verməsinə səbəb oldu.

Honey cyber metodu

Honey cyber metodologiyası, kiber təhlükəsizlik sahəsində istifadə olunan bir taktikadır. Bu metod, potensial hücumçuları cəlb etmək və onların hücum niyyətlərini müəyyən etmək üçün əlverişli bir mühit yaradır. Həqiqi sistemlərdə yerləşdirilmiş, lakin həqiqi istifadəçilər tərəfindən işlədilməyən "bal" və ya "honey pot" adlanan mənbələri istifadə edirlər. Bu mənbələr, normal şəbəkə cihazlarına oxşar görünən hədəfləri təmsil edir, lakin əslində onlar yalnız hücumçuların marağına səbəb olmaq məqsədi daşıyır. Hücumçular bu honey pot sistemlərinə cəlb olunur və onlarla interaksiya etdikcə, təhlükəli niyyətlərini ortaya qoyurlar. Böyük şirkətlər və orqanizasiyalar, bu metod vasitəsilə mövcud olan təhlükələri müəyyən etməyə, nail

olur və lazımı tədbirləri həyata keçirmək fürsətləri yaranır.Məsələn, bir şirkət, bir honey potqura bilər ki, bu server şirkətin mövcud web serverinə oxşar görünə, lakin aslında yalnız hücumçulara məxsus olan bir web server olsun. Bu honey pot serverinə giriş etməyə çalışan hücumçuların IP ünvanları və hücum metodları qeydə alınaraq, şirkətin təhlükəsizlik tədbirləri daha da gücləndirilə bilər. Başqa bir nümunə kimi, şirkət, hücumçuları cəlb etmək üçün bir honey pot e-poçt adresi yarada bilər. Bu e-poçt adresi, yalnız hücumçuların əlaqə saxladığı və hücum niyyətlərini açıq şəkildə ortaya qoyduğu bir e-poçt adresi ola bilər. Bu yolla, şirkətin təhlükəsizlik ekspertləri cari hücumların qarşısını almaq üçün uyğun tədbirləri hazırlaya bilərlər (R. Shukla and M. Singh,2014).

Honey Monkey metodu

Honey Monkey metodologiyası, potensial təhlükəsizlik boşluqlarını aşkarlamaq üçün internetdə avtomatik axtarış aparır və fərqli veb səhifələrindən saytları, faylları və digər resursları yükləyən köməkli bir avtomatlaşdırılmış fəaliyyət qurğusunu (honeyclient) istifadə edir. Microsoft tərəfindən təklif edilmiş bu metodun əsas məqsədi, internetdə mövcud olan potensial təhlükəsizlik boşluqlarını aşkarlamaqdır. Bu, saytları və faylları yükləmək, onların davranışını müşahidə etmək və potensial təhlükəsizlik boşluqlarını təyin etmək üçün avtomatik bir təhlükəsizlik yoxlama sistemi təşkil edir.Bu metod, avtomatik cədvələrin yaradılmasını, saytların avtomatik yüklənməsini və davranışlarının izlənməsini tələb edir. Əgər bir saytda və ya faylda təhlükəsizlik boşluğu müşahidə edilsə, bu boşluq qeydə alınır və təhlükəsizlik tədbirlərinin artırılması üçün qabaqcıl addımlar atılır.Bu metod, internetdəki potensial təhlükəsizlik açıqlarını müəyyən etmək və qarşısını almaq üçün effektiv bir yoldur (R. Shukla and M. Singh, 2014).

Cədvəl.3.1.1 araşdırılan metodların müqayisəli təhlili özündə saxlayır və bu təhlil metodların arasındakı fərqləri daha aydın şəkildə əks etdirir.

Aşkar edilmiş hücum	İstifadə edilən məlumat	Istifadə edilən yanaşma	Dəqiqlik/əticə
Profil inyeksiyası Hücum	**Film obyektiv məlumat toplusu**	Ansambl yanaşması SVM, NN ilə, Təsadüfi meşə təsnifatçı.	Dəqiqlik 90%-dən çoxdur
URF zəifliklər	Sistem 142,522,691 unikal link ilə sınaqdan keçirildi	URFDS	0-gün hücumu və “false positive” kimi boşluqları müəyyən edir
SQL enjeksiyonu, XML inyeksiyası, SOAP, XML, DoS hücumları	366 qeyri-səlis assosiativ nümunələr (FAP)	FAR IDP Sistemi	Bilinən mövcud hücumların aşkarlanması və qarşısının alınması və yeni hücumların proqnozlaşdırılması. Dəqiqlik 99%. Əməliyyat müddəti 0,25 ms daha azdır.
Müştəri tərəfdə zərərli aktivlik aşkar edildi.	116 ümumi saytsa Capture-HPC log fayllar	HMM, FP artımı və Honeypot əsasında Proqnozlaşdırma sistemi	90% dəqiqlik
SQL inyeksiyası hücumları	WP-SQLI-LAB, və açıq mənbə təhlükəsizliyi	Joza- hibrid problem çıxarış yanaşması müsbət və mənfi nəticə çıxarma alqoritmi	PHP-yə əsaslanan tətbiqləri avtomatik qoruyur. ”false positive” nəticə vermir, aşağı performanslıdır (4%), və quraşdırmaq asandır.
Saytlararası script (XSS)	33,843 veb səhifə kimi Yaxşı xasiyyətli nümunələr DMOZ-dan əldə edilmişdir verilənlər bazası və 18,700 veb-səhifələri zərərli	ADTree klassifikasiyası ilə N-gram modelinin təkmilləşdirilməsi	Effektiv XSS aşkarlanması. Yaxşı performans dəqiqlik və geri çağırma

	hesab edir -dən alınan nümunələr XSSed verilənlər bazasından və Real saytlardan 3300 veb səhifə.		
Sıfır gün, polimorfik **qurdlar**	Honeynet arxitekturasından asılı olan sınaq mühiti	İkiqat honeynet sistemi – avtomatik imza generasiyası	Yanlış həyəcan siqnalının azaldılması və polimorf qurdlar üçün yüksək keyfiyyətli imzalar yaratmaq
Zərərli veb URL-ləri	Veb URL **crawler** üçün istifadə ediləm veb səhifələrin URL-ləri (100 url üçün veb səhifə)	Python Honey Monkey sistemi	Müxtəlif əməliyyat sistemlərinin zəifliklərini və onların standart veb-sörf proqram təminatını işə salan IP ünvanlarının siyahısını yönləndirən URL siyahısı olan qara siyahı faylı.
XSS, SQL inyeksiyası hücumları	Simvolik soket	CRAXweb	Geniş miqyaslı açıq mənbəli veb proqramlardakı zəiflikləri uğurla müəyyən edir və hücum xəttini yaradır.

Cədvəl.3.1.1 Veb tətbiqlərindəki müxtəlif hücum aşkarlama sistemlərinin müqayisəli təhlili (İbrahim Seyfullayev, Sevda Xıdırova, 2024)

3.2 Aşkarlama alətlərinin analizi ,müqayisəli təhlili və qiymətləndirilməsi

Nüfuzetmə testi ilə veb tətbiq skan edilir və zəifliklər aşkar edilir. Veb zəifliyi skanerlərinin yayılmasını nəzərə alaraq, onların effektivliyini qiymətləndirmək lazımdır. Bunun üçün istifadə olunan üsullardan biri də müqayisəli təhlildir. Veb zəifliyi skanerləri müxtəlif meyarlardan istifadə etməklə qiymətləndirilmişdir. Biz ilk növbədə OWASP etalonundan istifadə edərək dörd tanınmış veb skaneri (Nessus Vulnerability Scanner, OpenVAS, Wapiti və Burp Suite) qiymətləndirir və müqayisə edirik. Biz həmçinin OWASP etalonunda bu dörd proqramın performans nəticələrini onların WAVSEP etalonunda əvvəlki nəticələri ilə müqayisə edərək, bu üç etalonun imkanları arasındakı fərqləri əldə edirik. İnformasiya texnologiyaları sahəsində ən populyar sektorlardan biri öyrənmənin idarə edilməsidir. Veb tətbiqlərin nüfuz sınağı üçün vebsayta baxılır (Shebli, H.M.Z.A.; Beheshti, B.D. 2018).

Məqsəd:

1) Qüsurların müəyyən edilməsi

2) Təhlükəsizlik vəziyyətini müəyyən edin

3) Risk Prioritetlərinin Müəyyən edilməsi

4) Təhlükəsizlik Risklərini Azaldılması

5) Məlumatların pozulmasının qarşısının alınması

Mburano, veb tətbiqi təhlükəsizlik alətlərinin işini qiymətləndirmək üçün standartlaşdırılmış və hərtərəfli test nümunələri dəsti olan Açıq Veb Tətbiqi Təhlükəsizliyi Layihəsindən (OWASP Benchmark) istifadə edərək veb zəifliyi skanerlərinin effektivliyini qiymətləndirdi. Müəlliflər OWASP Benchmark-dan istifadə edərək veb zəiflik skanerlərini, Acunetix, AppScan, Burp Suite və Netsparker-i qiymətləndiriblər. Qiymətləndirmə ölçülərinə əhatə dairəsi, aşkarlama dəqiqliyi və yanlış müsbət dərəcələr daxildir. Nəticələr göstərir ki, hər bir brauzerin performans baxımından özünəməxsus güclü və zəif tərəfləri var. OWASP belə nəticəyə gəldi ki, Benchmark müxtəlif veb zəiflik skanerlərinin performansını qiymətləndirmək və müqayisə etmək üçün faydalı alət ola bilər və istifadəçilərə xüsusi ehtiyac və

tələblərinə əsaslanaraq ən uyğun aləti seçməkdə kömək edə bilər (Mburano, B.; Si, W. 2018) .

Qutam, A. Tiwari, V. yanaşmanın effektivliyini nümayiş etdirmək üçün veb proqramında yerinə yetirilən VAPT - ın ətraflı nümunəsini təqdim etdi. Müəlliflər VAPT prosesində iştirak edən müxtəlif addımları, o cümlədən kəşf, zəifliyin müəyyən edilməsi, istismar və hesabat verməyi təsvir edirlər. Onlar həmçinin Nmap, Burp Suite, Metasploit və SQL Map kimi test zamanı istifadə olunan alətlər və texnikaları müzakirə edirlər. Məqalə veb proqramların təhlükəsizliyinin təmin edilməsində VAPT-nin əhəmiyyətini və inkişaf edən təhlükə mənzərəsi ilə ayaqlaşmaq üçün müntəzəm sınaqlara ehtiyacı vurğulamaqla yekunlaşır. Müəlliflər təşkilatlara VAPT-ni kibertəhlükəsizlik strategiyasının bir hissəsi kimi daxil etməyi və ondan veb proqramlardakı zəiflikləri müəyyən etmək və azaltmaq üçün istifadə etməyi tövsiyə edirlər (Arvind Goutam , Vijay Tiwari, 2020).

S., Kotha, S.K., David Raju veb proqramlarda kiberhücumları aşkar etmək və qarşısını almaq üçün yeni üsullar təqdim etdilər. Birinci mərhələdə, istifadəçi davranışı, şəbəkə trafiki və sistem qeydləri kimi xüsusiyyətlərə əsasən mümkün hücumların aşkarlanması. İkinci mərhələdə, aşkar edilmiş hücumların baş verməsinin qarşısının alınması. Bu qaydalar tətbiqin xüsusi ehtiyaclarına uyğunlaşdırıla və yeni təhlükələr üçün yenilənə bilər. Onlar tapdılar ki, onların metodu geniş spektrli hücumları, o cümlədən SQL inyeksiyası, saytlararası skriptlər və kataloqlar arası hücumları müəyyən edib qarşısını ala bilər. Ümumilikdə, məqalə maşın öyrənməsi və qaydalara əsaslanan metodlardan istifadə edərək veb tətbiqlərində kiberhücumların müəyyən edilməsi və qarşısının alınması üçün perspektivli yanaşma təqdim edir. Bu, veb tətbiqlərinin təhlükəsizliyini artırmaq və məlumat pozuntularının qarşısını almaq istəyən təşkilatlar üçün faydalı ola bilər (S., Kotha, S.K., David Raju 2019).

Boşluqların aşkarlanması

1)HTTP cavabı daxilində brauzer tərəfindən icra edilə bilən kod daxil edildikdəbu kodun nəticəsi brauzerdə əks olunursa bu boşluq XSS boşluğu sayılır. Əlavə edilmiş hücum daimi deyil və yalnız zərərli şəkildə hazırlanmış linki klikləyən və ya üçüncü tərəfin veb saytına daxil olan istifadəçilərə təsir edir; Tətbiqin özündə

saxlanmır. Hücum sətri, tətbiqin səhv emal etdiyi və qurbana geri göndərdiyi hazırlanmış URI və ya HTTP parametrlərinin bir hissəsidir. Bu tip hücumlara qarşı həssas olan veb tətbiqi sorğular vasitəsilə qəbul edilən təsdiqlənməmiş girişi müştəriyə geri göndərəcək. Hücum adətən üç addımı izləyir: Dizayn, burada təcavüzkar zərərli URL yaradır və sınaqdan keçirir; qurbanlarını URL-ni brauzerlərinə yükləməyə inandırdığı sosial mühəndislik; icra isə qurbanın brauzeri vasitəsilə zərərli kodun icrasıdır. Hər Giriş Sahəsində XSS-in yoxlanılması üçün addımlar

1. Giriş vektorlarını izləyin.
2. Giriş vektorlarını yoxlayın

2)Nəticənin veb tətbiqinin təhlükəsizliyinə zərər gətirə biləcək zəifliyi göstərib-göstərmədiyini görmək üçün əvvəlki turda cəhd edilmiş hər bir test girişini araşdırdıq. Bunu etmək üçün yaradılan veb-səhifənin HTML-ni nəzərdən keçirməli və test girişini axtarmalısınız. Xüsusi simvol aşkar edildikdə, tester düzgün kodlaşdırılmamış, dəyişdirilmiş və ya süzülmüş simvolları tapır. Məqsəd bütün HTML xüsusi simvollarını HTML obyektləri ilə əvəz etməkdir. Tanımaq üçün vacib HTML obyektləri bunlardır

1) >(böyükdür)

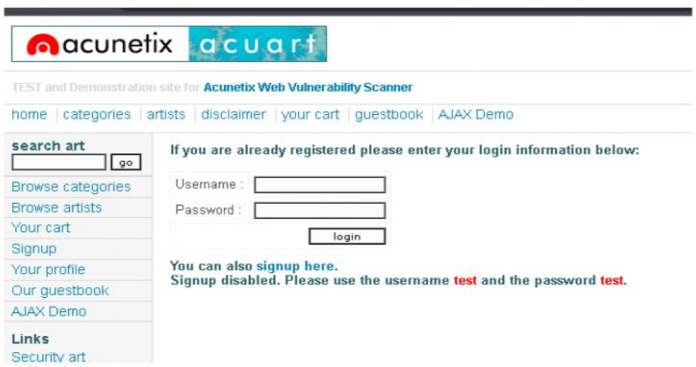
2) <(kiçikdir)

3) & (ampersand)

4)' (apostrof və ya tək dırnaq)

5)"(cüt dırnaq)

XSS-in testi məqsədi ilə istifadə olunan bu veb-saytı nəzərdən keçirək

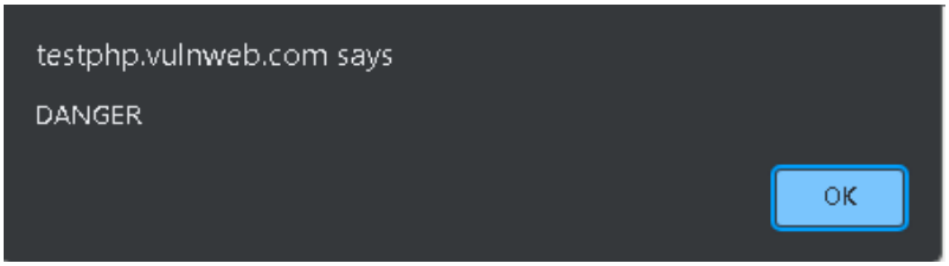


Şək.3.1.6 Acunetix veb zəiflik skaneri (Deekshitha Valluri, 2023)

Acunetix Veb Zəiflik Skaneri Şək.3.1.6-da göstərilmişdir. Testerin fikrincə, hər bir məlumat giriş nöqtəsi XSS hücumu ehtimalını artırmalıdır. Tester istifadəçi dəyişənini sınayacaq və onu təhlil etmək üçün zəiflikdən istifadə etməyə çalışacaq.

http://example.com/index.php?user=<script>alert("Danger")</script>

XSS Nəticəsi Şək.3.1.7-də göstərilmişdir. Bu, XSS zəifliyinin mövcud olduğunu göstərir və əgər kimsə testerin linkinə klik edərsə, tester potensial olaraq istənilən brauzerdə istənilən kodu işlədə bilər.



Şək.3.1.7 XSS-in nəticəsi (Deekshitha Valluri, 2023)

2) Sessiyanın fiksasiyası zəifliyi

Sessiyanın fiksasiyası hücumçuya etibarlı istifadəçi sessiyasını oğurlamağa imkan verən hücumdur. Hücum veb tətbiqinin sessiya ID-sini, xüsusən də həssas veb tətbiqini idarə etməsinə imkan yardacaq məhdudiyyəti araşdırır. O, istifadəçinin autentifikasiyası zamanı yeni sessiya identifikatoru təyin etmir və mövcud sessiya ID-dən istifadə etməyə imkan verir. Hücum etibarlı sessiya identifikatorunun əldə edilməsindən (məsələn, proqrama qoşulmaqla), istifadəçini həmin sessiya ID-si ilə autentifikasiya etməyə sövq etməkdən və sonra istifadə edilən sessiya ID-si haqqında məlumatı olan istifadəçi tərəfindən autentifikasiya edilmiş sessiyanı qaçırmaqdan ibarətdir.

3) Veb Server Parolun Avtomatik Tamamlanmasına İcazə Verməsi

4) Veb proqram kukiləri HTTPOnly kimi qeyd olunmaması

5) Veb əks etdirmə zəifliyi

OWASP onlayn proqram təhlükəsizliyi sahəsində tanınmış və hörmətli bir təşkilatdır. O, inkişaf etdiricilərə və təşkilatlara zəiflikləri müəyyən etmək və azaltmaqda kömək etmək üçün resurslar, alətlər və tövsiyələr təqdim etməklə proqram təminatı və veb tətbiqlərini daha təhlükəsiz etmək məqsədi daşıyır. Tövsiyə olunan

üsul sızma testi üçün istifadə edilən standart üsuldur. Bu metodologiya Zəifliyin növünü və Baqların təsir gücünü təsnif etməyə kömək edir. Metod zəifliklərin müəyyən edilməsində dəqiq və düzgün tətbiq axınını təmin edən bir neçə addımdan ibarətdir.

1) Kəşfiyyat: Hədəf sistemin potensial zəifliklərini və hücum səthini anlamaq üçün kəşfiyyat lazımdır. Bu, uğurlu bir zəiflik qiymətləndirməsinin əsasını təşkil edir.

2) Skan etmə: Skan etmə, açıq portları, xidmətləri və bilinən zəifliklər təyin edərək sistemin potensial zəif sahələrini başlanğıc üçün anlamağı təmin edir.

3) Qiymətləndirmə: Qiymətləndirmə, zəifliklər ciddilik və potensial təsirlərinə görə sinifləndirmək, onları prioritetləndirmək və məqsədəuyğun tövsiyələri təmin etmək üçün əhəmiyyətlidir.

4) Açıqlanma və Analiz: Qiymətləndirmə, zəifliklər ciddilik və potensial təsirlərinə görə sinifləndirmək, onları prioritetləndirmək və məqsədəuyğun tövsiyələri təmin etmək üçün əhəmiyyətlidir.

5) Hesabat və Yamaq: Qiymətləndirmənin nəticələrinə əsaslanaraq sistemi təmir etmək və qorumaq üçün son mərhələ, aşkar olunan məlumatları dokumentləşdirmək və zəifliklər yamamaqdan ibarətdir.

Metodologiya

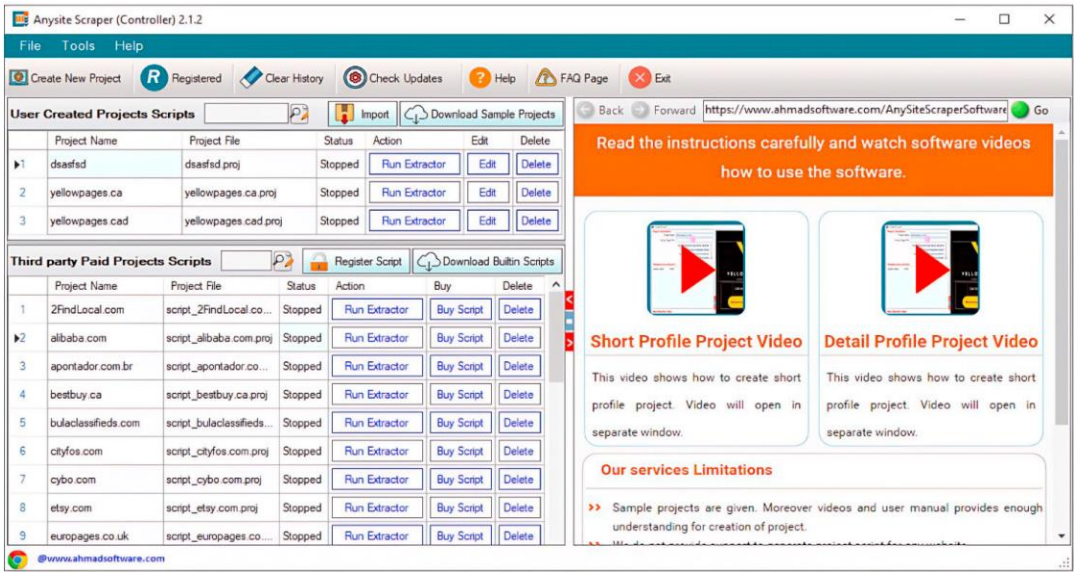
Veb Tətbiqinin Təhlükəsizliyi Testi üçün Test Metodologiyası beş mərhələyə bölünür:

1. Kəşfiyyat
2. Skanlama
3. Qiymətləndirmə
4. Kəşf və Təhlil
5. Hesabat və yamaq

Kəşfiyyat Bu mərhələ hədəf vebsayt, sistem, proqram və s. haqqında məlumatların toplandığı zəifliklərin qiymətləndirilməsi və nüfuzetmə testində məlumat toplama mərhələsidir. id's,.kəşfiyyatın məqsədi mümkün qədər çox potensial təhlükəni, yəni hədəflər Veb Tətbiqində mövcud olan zəifliklər müəyyən etməkdir. Google Dorking: Google Dorks, adətən axtarış motorları tərəfindən indeksləşdirilməyən

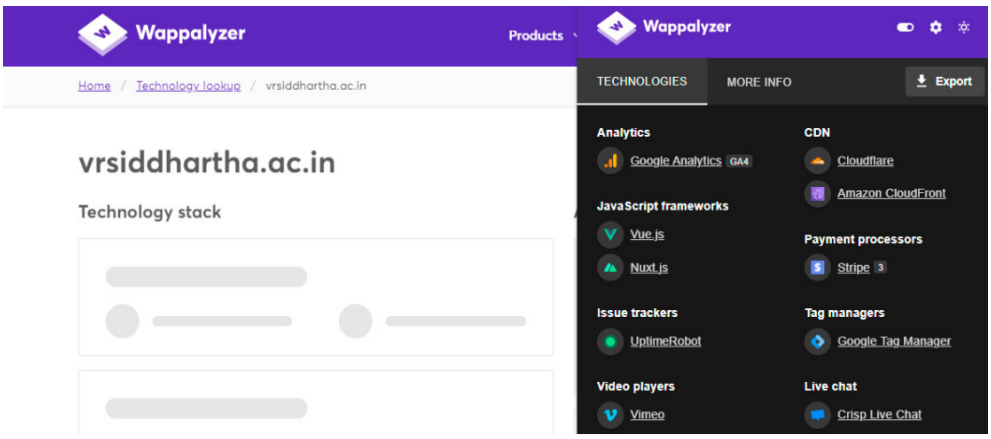
məlumatları axtarmaq üçün qabaqcıl operatorlardan istifadə edən axtarış texnikasıdır. Bu yazıda Google Dorking Hədəf Veb Tətbiqinin Məlumat Toplama Texnikası (Kəşfiyyat) üçün istifadə olunur.

Bu elmi-işdə biz veb-proqramın ayaq izlərini (foot printing) üçün istifadə olunan Vebdata Extractor alətindən istifadə etdik. Tətbiq veb-saytın IP ünvanının bütün statik və dinamik səhifələri haqqında bütün məlumatları verir. Webdata Extractor Şək. 3.1.8-də göstərilmişdir.



Şək.3.1.8 Vebdata Extractor (Deekshitha Valluri, 2023)

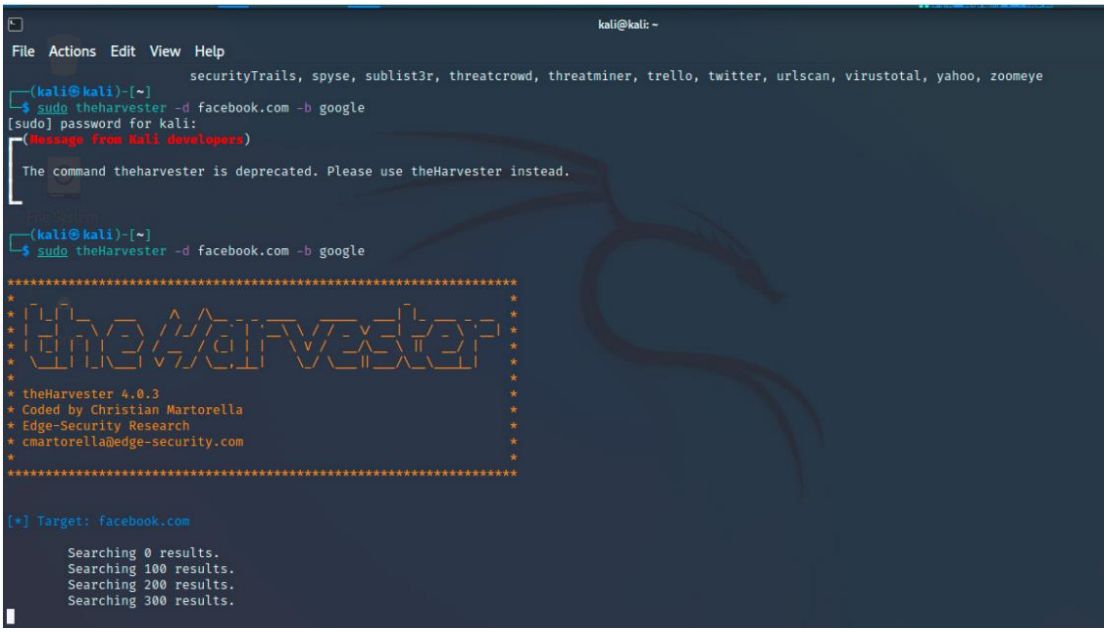
Həmçinin proqramın hazırlanması üçün istifadə olunan Texnologiyaları (Server tərəfi ƏS, FrontEnd, BackEnd, DataBase, IPAddress, UI Frame işləri, Veb serverləri) müəyyən etmək üçün istifadə edilən Wappalyzer Genişlənməsindən istifadə edilir. Wappalyzer Şək.3.1.9-da göstərilmişdir.



Şək.3.1.9 Wappalyzer (Deekshitha Valluri, 2023)

Araşdırma zamanı alt domen adlarını və qeydiyyatdan keçmiş e-poçt ünvanlarını müəyyənləşdirmək üçün Harvester alətindən istifadə edilib.

Harvester Aləti yuxarıdakı şək.3.1.10-da göstərilmişdir. Və enumeration prosesi üçün biz hədəf veb tətbiqinin bütün giriş səhifələrini və Admin giriş səhifələrini toplamaq üçün foot printing çapında əsas addım olan GOOGLE DORKING-dən istifadə etdik.



Şək.3.1.10 Harvester Tool (Deekshitha Valluri, 2023)

Skanlama

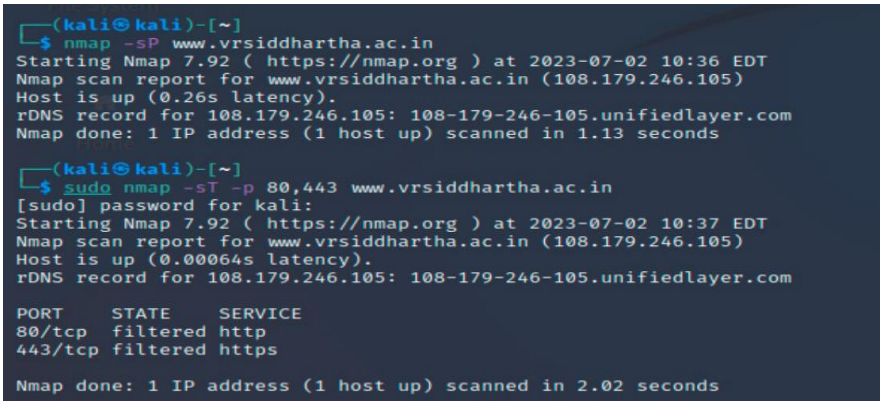
Skanlama Veb Tətbiqinin Zəifliyin Qiymətləndirilməsi və Penetrasiya Texnikasının ən mühüm mərhələsidir. Bu mərhələdə biz istənilən Tətbiqin son nöqtələri adlanan potensial giriş nöqtələrini və portları və zəiflikləri müəyyən etmək üçün hədəf Veb Tətbiqini skan edirik. Bu o deməkdir ki, bura Port daxildir. Veb

Nmap (Network Mapper) şəbəkənin skan edilməsi və xəritələşdirilməsi üçün istifadə edilən məşhur və güclü açıq mənbə alətidir. O, təhlükəsizlik mütəxəssislərinə hostları kəşf etməyə, açıq portları müəyyən etməyə və şəbəkə xidmətləri və əməliyyat sistemləri haqqında məlumat toplamağa imkan verir.

1) Host kəşfi

2) Port Skanı

3) Xidmət və versiyanın aşkarlanması



Şək.3.1.11 Nmap skanlama (Deekshitha Valluri, 2023)

• AngryIP Scanner: Angry IP Scanner və o, həmçinin IPScan kimi tanınır, şəbəkədəki IP ünvanlarını və əlaqəli portları aşkar etmək və skan etmək üçün istifadə edilən məşhur açıq mənbəli şəbəkə skan alətidir. O, istifadəçilərə şəbəkədəki hostlar haqqında məlumatları tez bir zamanda skan etməyə və toplamağa imkan verən sadə və intuitiv interfeys təqdim edir.

1) IP Ünvanı və Port Skanı
2) Host Məlumatı
3) Qiymətləndirmə
4) Kəşf və Təhlil
5) Hesabat və Yamaq

Wapiti

Wapiti, defolt olaraq kali linux-da əvvəlcədən quraşdırılmış zəifliklərin qiymətləndirilməsi üçün ən yaxşı açıq mənbə alətlərindən biridir. Hədəflənmiş veb Tətbiqinin nüfuz sınağı üçün istifadə olunur. Wapiti, açıq Veb Tətbiqi Təhlükəsizliyi Layihəsi (OWASP) boşluqlarını müəyyən edə biləcəyimiz wapiti alətindən istifadə edərək veb tətbiqi ilə qarşılıqlı əlaqə qurmağın ən yaxşı və sürətli yolu olan komanda xətti interfeysidir.

• Backup faylı
• Blind SQL Injection
• Zəif etimadnamələr
• CRLF inyeksiaysı
• Məzmun Təhlükəsizlik Siyasəti Konfiqurasiyası

• Saytlararası Sorğu Saxtakarlığı

• Potensial təhlükəli fayl

• Komandanın icrası

• Path Traversal

• Htaccess Bypass və.s

OpenVAS

OpenVAS zəifliyin hərtərəfli qiymətləndirilməsi və idarə edilməsi üçün güclü açıq mənbəli vasitədir. O, kompüter sistemləri və şəbəkələrində zəiflikləri aşkar etmək və idarə etmək üçün geniş imkanlar təqdim edir. OpenVAS və onun imkanlarının icmalı budur: OpenVAS zəifliyin qiymətləndirilməsini və idarə olunmasını asanlaşdıran məşhur açıq mənbə alətidir. O, təhlükəsizlik zəifliklərini müəyyən etmək və azaltmaq üçün möhkəm funksiyalar dəsti təklif edir. Bu yazıda biz OpenVAS və onun imkanlarını araşdırırıq. onun təhlükəsizlik ekosistemindəki rolu. OpenVAS skaner, menecer və müxtəlif plaginlər daxil olmaqla bir neçə əsas komponentdən ibarətdir. Arxitektura zəifliklərin səmərəli və dəqiq skan edilməsinə və idarə edilməsi proseslərinə imkan verir. Digər təhlükəsizlik alətləri və çərçivələri ilə inteqrasiya OpenVAS-ın imkanlarını artırır.OpenVAS aktivlərin aşkarlanması və hədəf seçimindən başlayaraq zəifliyin skan edilməsinə sistematik yanaşma tətbiq edir. Skanlar xüsusi tələblərə uyğun olaraq konfiqurasiya edilə və planlaşdırıla bilər. Alət hədəf mühitdə zəiflikləri aşkar etmək üçün müxtəlif skan üsullarından istifadə edir.

Zəifliyin aşkarlanması və qiymətləndirilməsi: OpenVAS geniş spektrli zəiflikləri əhatə edir, o cümlədən, lakin bunlarla məhdudlaşmır:

• Ehtiyat fayl boşluqları

• Blind SQL Injection zəifliklər

• Zəif etimadnamə zəifliklər

• CRLF Injection zəifliklər

• Məzmun Təhlükəsizlik Siyasəti Konfiqurasiya zəifliklər

• Saytlararası Tələb Saxtalanma zəifliklər

• Potensial təhlükəli fayl zəifliklər

• Komandanın icrası ilə bağlı zəifliklər

• Path Traversal zəifliklər
• HTTP Secure Headers zəifliklər
• SQL Injection zəifliklər
• Server Side Request Forgery zəifliklər
• Saytlararası Skriptləmə zəifliklər

Bu işdə OpenVas açıq mənbə aləti olan zəifliklərin qiymətləndirilməsi üçün istifadə edilən ikinci alətdir. Aləti istifadə etdikdən sonra şəxsi skan edilmiş hesabatlar üçün giriş etimadnamələri yaradılacaq, biz Veb Tətbiqin Domen adı və ya IP ünvanından istifadə edə bilərik. Openvas aləti skan edildikdən sonra, zəifliklərin şiddətinə görə təsnifatlara görə avtomatik hesabat verir. Və iş performansını verir, veb tətbiqinin tam statistikası yalnız openvas aləti tərəfindən yaradılacaqdır.

Nessus Zəiflik Skaneri: Kompleks Şəbəkə Təhlükəsizliyinin

qiymətləndirilməsi aləti şəbəkə təhlükəsizliyinin qiymətləndirilməsi kompleks İT mühitlərində zəifliklərin müəyyən edilməsində və risklərin azaldılmasında mühüm rol oynayır. Geniş istifadə olunan zəiflik skaneri olan Nessus şəbəkə təhlükəsizliyinin hərtərəfli qiymətləndirilməsi üçün geniş funksiyalar dəsti təklif edir. Bu sənəddə Nessusun arxitekturası, skan etmə metodologiyaları və şəbəkə zəifliklərini aşkar etmək və qiymətləndirmək qabiliyyəti daxil olmaqla, onun dərin tədqiqi təqdim olunur. Bundan əlavə, biz Nessusun təhlükəsizlik zəifliklərinin müəyyən edilməsi və aradan qaldırılmasında praktik tətbiqlərini müzakirə edirik.

1)Giriş:

• Şəbəkə təhlükəsizliyinin qiymətləndirilməsinin əhəmiyyəti
• Nessusun icmalı və onun şəbəkə təhlükəsizliyi mənzərəsindəki əhəmiyyəti
• Digər zəifliklərin skan edilməsi alətləri ilə müqayisə
• Digər təhlükəsizlik alətləri və çərçivələri ilə inteqrasiya

2) Skanlama Metodologiyaları:

• Aktiv və passiv skanlama yanaşmaları
• Şəbəkə skanları üçün fərdiləşdirmə seçimləri
• Zəifliyin aşkarlanması və qiymətləndirilməsi.

3) Nessusun müxtəlif şəbəkə zəifliklərini aşkar etmək və qiymətləndirmək bacarığı, o cümlədən:

• Yanlış konfiqurasiya edilmiş şəbəkə cihazları

• Zəif və ya standart etimadnamələr

• Açıq portlar və xidmətlər

• Köhnəlmiş proqram təminatı və çatışmayan yamalar.

Zəifliklərin təsnifatı: Skanlama addımından sonra aşkar edilmiş boşluqlar Nessus Zəiflik Skaneri tərəfindən hazırlanmış hesabata uyğun olaraq sıralanır.

1) Kritik

2) Yüksək

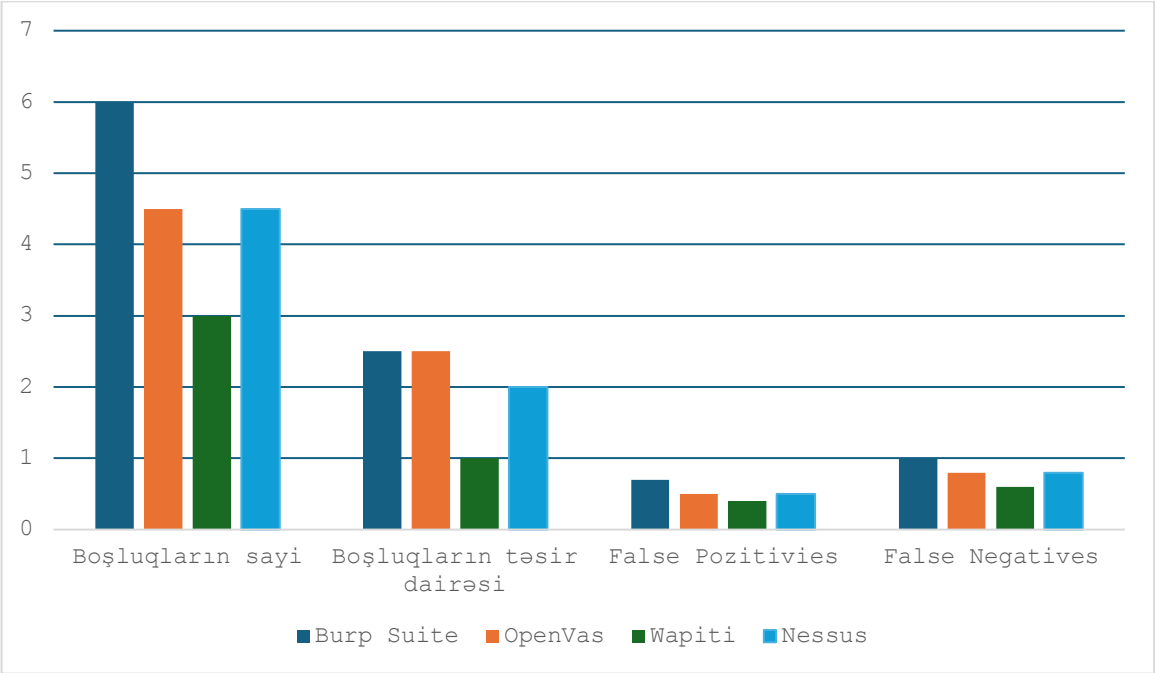
3) Orta

4) Aşağı

Bu işdə hədəf veb-saytda mövcud olan baqların müəyyən edilməsi üçün Nessus zəiflik skanerindən istifadə etdirik. Nessus veb tətbiqi zəifliklərinin qiymətləndirilməsi üçün istifadə olunan açıq mənbə zəiflik skaneridir (Zərərli proqramların aşkarlanması, Ransomware aşkarlanması, Şəbəkə Skanı, Host Kəşfi.). Nesus aləti quraşdırıldıqdan sonra biz aləti bütün portları və protokolları skan etmək üçün konfiqurasiya etdik. Konfiqurasiyadan sonra biz Veb Tətbiqin istifadə olunan domen adları skan edildikdən sonra zəifliklərin şiddətinə görə təsnifat əsasında hesabat hazırlandı.

Nəticə və Müzakirə: Şək.3.1.12 davamlı zəifliyin qiymətləndirilməsi üçün istifadə edilən müxtəlif hibrid platformaları müqayisə edir. Zəifliyin skan edilməsinin nəticələrinə əsasən, Burp Suit Professional aləti zəifliyin aşkarlanması baxımından ən yaxşısını göstərmişdir. Veb proqramlarının təhlükəsizliyini qiymətləndirmək üçün güclü və effektiv vasitə kimi Burp Suite Professional seçilir. Onun uyğunlaşdırıla bilən skan etmə xüsusiyyətləri, interaktiv əl testi üçün dəstək, autentifikasiya və sessiyaların effektiv idarə edilməsi, proksi kimi real vaxt rejimində sınaq funksiyaları və güclü istifadəçi icması tərəfindən dəstəklənən davamlı yeniləmələr, hamısı onu müxtəlif proqramları tapmaqda ,zəifliklər və veb proqram təhlükəsizliyində dəyişən problemlərin həllini effektiv etmək üçün birlikdə işləyir. O, həm Windows, həm də

Linux mühitlərində geniş spektrli boşluqları yoxlaya bilər. Alətlərin Performans göstəricilərinin müqayisəsi aşağıdakı cədvəl.3.1.2-də göstərilmişdir.



Şək.3.1.12 Skanlama alətlərin müqayisəsi (E. A. A. Vega, A. L. S. Orozco, andcom L. J. G. Villalba, 2017)

Dizaynerlər real məlumatlardan istifadə etməklə müxtəlif zəifliyin qiymətləndirilməsi üsullarının müqayisəsini təqdim ediblər (Windows -Nessus və Burp Suite Professional, həmçinin saytlararası skript zəifliyi və kali Linux - Wapiti daxildir). Bu sənəddə tətbiq edilən təklif olunan çərçivə digər faktiki zəiflik mühitləri üçün etalon kimi istifadə oluna bilən OWASP çərçivəsidir. Zəiflik skanımızın nəticələrinə əsasən, Burp Suit Professional aləti zəifliyin aşkarlanması baxımından ən yaxşısını həyata keçirir, çünki o, veb proqramında mövcud ola biləcək bütün növ zəiflikləri skan edə bilir və həm Windows, həm də Linux üçün əlçatandır.

Hər bir alətin də öz üstünlükləri və mənfi cəhətləri var. Amma hər birinin məqsədi təhlükəsiz bir veb mühit təşkil etməkdən ibarətdir. Müxtəlif aşkarlanma alətləri istifadə edərək potensial təhdidləri müəyyən edə bilərik və bu təhdidlərin qarşısının alınması üçün işin növbəti fəslində bir-sıra metod və üsullar təklif edilmişdir.

Alətlər	Nessus	OpenVas	Wapiti
Tapılmış boşluqların növləri	TLS versiyası 1.0 Protokol aşkarlama	Backdoor tapılması	Backup faylı
	TLS versiyası 1.0 Protokol aşkarlama	X Server	Blind SQL inyeksiyası
	Nessus SYN skanlama	Remote kod inyeksiyası boşluğu	Zəif verilənlər
	SSL/TLS versiyası	PostgreSql boşluqları	CLRF inyeksiyası
	SSL sertifkatlaşdırma	PostgreSql zəif şifrləmə	CSRF
	SSL imzalı sertifikatın zəif heş alqoritmi istifadəsi	phpMyAdmin konfuqrasiya faylına PHP kod inyeksiyası	Potensial təhlükəli fayıllar
	SSL Blok şifrləmə dəstəklənməsi	Phpinfo() çıxış məlumatlarının əlçatanlıq	Command execution
	SSL root sertifikatı	PostgreSql boşluqları	Path Traversal
	SSL /TLS son istifadə edilmiş şifrələr	PostgreSql “bitsubstr” Bufer daşması boşluğu	HTTP headeHTTPOnly kuki

	Xidmətlərin aşkarlanması	PostgreSql “intarray” Bufer daşması boşluğu	Təhlükəsiz kuki flag
	TLS next protokol dəstəklənməsi		SQL injection
	TLS versiyası 1.1 Protokol aşkarlama		XSS

Cədvəl.3.1.2 Alətlərin Performans göstəricilərinin müqayisəsi

FƏSİL IV Mövcud Boşluqların və Təhdidlərin Qarşısının alınması Modellərii

4.1 Veb təhdidlərin qarşısının alınması üçün müdafiə mexanizmləri

Veb təhdidlərin qarşısının alınması, veb saytları zərərli proqramlar, fişinq hücumları, SQL inyeksiyası, XSS və digər zəifliklərdən qorumaq üçün nəzərdə tutulmuş müxtəlif texnika və metodları əhatə edən kibertəhlükəsizliyin vacib bir hissəsidir. Veb təhlükə qarşısının alınmasının məqsədi bu təhdidləri müəyyən etmək, azaltmaq və qarşısını almaqdır ki, veb resursların bütövlüyü, əlçatanlığı və məxfiliyi təmin olunsun.

1. Firewall şəbəkənizi xarici hücumlardan qoruyan təhlükəsizlik sistemidir. Bu o deməkdir ki, internetdən və ya digər şəbəkələrdən hər hansı məlumat şəbəkənizə çatmaq üçün firewalldan keçməlidir. Bu sistem məlumat paketlərinin müəyyən edilmiş qaydalara uyğun olub-olmadığını yoxlayır və paket keçid icazəsini müəyyən edir. İcazəsiz girişin, virusların və ya digər zərərli proqramların şəbəkəyə sızmasının qarşısı alına bilər. Firewalllar quruluşlarına görə iki növə bölünür: proqram və apparat təminatı firewall.

- Aparat təminatı firewall xüsusi CPU, yaddaş, əməliyyat sistemi və proqram təminatı ilə təchiz edilmiş qurğulardır. İnterneti və çoxlu kompüterləri olan müəssisələr apparat təminatı firewalllarına üstünlük verirlər. Bu tip firewalllar kompüterdə işləmədiyi üçün performans və sürətdə heç bir azalmaya səbəb olmur. O, həmçinin uzaq işçilər üçün nəzərdə tutulmuş VPN bağlantısına imkan verir. Xüsusilə fərdi internet istifadəçiləri tərəfindən kompüterlərin fonunda aktiv şəkildə işləyən proqramlar olan proqram təminatı firewalllarına üstünlük verilir. Bu tip firewall proqramları yalnız bir sistemi və ya şəbəkəni qoruyur. Şəbəkənizdə birdən çox sistem varsa, birdən çox sistem üçün ayrıca firewall proqramından istifadə etməyiniz tövsiyə olunur.

Arxitekturasına görə firewallın növləri: Paket Filtrləmə Firewall, Dövr Səviyyə Firewall, Proksi əsaslı firewall, stateful firewall, statelss firewall, next generation firewall.

- Paket Filtrləmə Firewall

  Bu firewall trafikdə axan məlumatların başlıq hissəsini oxuyur və bu hissədəki məlumatları analiz edərək işləyir. İş prinsiplərinə baxdığımızda trafikdəki məlumatların mənbə ünvanı, təyinat ünvanı, paketin daxil olmaq istədiyi port, istifadə edəcəyi protokol kimi analizlər nəticəsində paketin keçməsinə icazə verilir və ya əvvəlcədən təyin edilmiş icazələrin əsasında bloklanır. Bu arxitekturanın ən böyük mənfi cəhəti paketi ilk göndərən sistemin, yəni daxil olan sistemin bəzi hallarda aşkar olunmamasıdır. Bu memarlıq köhnə olsa da, hələ də bəzi sistemlərdə istifadə olunmağa davam edir. Belə firewall cihazları OSI modelindəki şəbəkə qatında işləyir.
- **Stateful firewall**

  Stateful və stateless firewall-lar şəbəkə təhlükəsizliyi üçün istifadə olunan iki əsas mexanizmdir. Stateful firewall trafikin vəziyyətini izləyir və əlaqənin hər bir mərhələsini analiz edir. Bu, bağlantının mənbə və təyinat IP ünvanlarını, port nömrələrini və əlaqənin vəziyyətini nəzərə alaraq qərar qəbul etməyə imkan verir. Bu cür firewall-lar daha təhlükəsiz sayılır, çünki onlar hər bir paket haqqında daha çox məlumat saxlayır və daha ətraflı təhlil edə bilir.
- **Stateless firewall**

  Stateless firewall isə hər bir paketi müstəqil şəkildə yoxlayır və keçmiş məlumatlara əsaslanmır. Bu cür firewall-lar daha sadə və sürətlidir, çünki onlar yalnız hər paketin başlığını yoxlayır və ona uyğun qaydalara əsasən qərar qəbul edir. Lakin, stateless firewall-lar daha az təhlükəsiz sayılır, çünki onlar əlaqənin bütöv vəziyyətini nəzərə almadan qərar verir.
- **Veb Tətbiqi Firewallları (WAF)** Xüsusilə veb tətbiqləri qorumaq üçün nəzərdə tutulmuşdur, HTTP trafikini izləyir və filtr edir. WAFlar zərərli sorğuları bloklaya bilər.

- Next Generation Firewall (NGFW)

  Firewall daxil olan və çıxan şəbəkə trafikini idarə etməyi, müəyyən filtrlərdən keçirməyi və şəbəkə trafikindəki zərərli hərəkətləri dayandırmağı hədəfləyir. Bu formada şəbəkənin təhlükəsizliyi təmin edilir. NGFW-lər ənənəvi firewallların xüsusiyyətlərinə malik olmaqla yanaşı yeni nəsil təhlükələrin qarşısının alınması üçün bir sıra əlavə xüsusiyyətlərə malikdir. Yeni özəlliklərdən bəziləri aşağıda göstərilmişdir.

  2. IDPS

     IDPS şəbəkə və sistem fəaliyyətlərini zərərli fəaliyyətlər və ya siyasət pozuntuları üçün monitorinq etmək üçün vacibdir.

     IDS: Şəbəkə trafikini müdaxilə əlamətləri üçün izləyir və analiz edir. Şübhəli fəaliyyət aşkarlandıqda, idarəçilərə xəbərdarlıq göndərir.

     IPS: IDS-ə bənzərdir, lakin aşkar edilmiş müdaxilənin qarşısını almaq üçün hərəkətə keçə bilər, məsələn, zərərli IP ünvanından trafiki bloklamaq.

  3. SSL və TLS

     SSL və TLS veb server və müştəri arasında ötürülən məlumatları şifrələmək üçün istifadə olunan protokollardır. Bu şifrələmə hər hansı dəyişdirilən məlumatın, məsələn, giriş məlumatları və ya şəxsi məlumatların, dinləmələrdən qorunmasını təmin edir.

  4. CSP

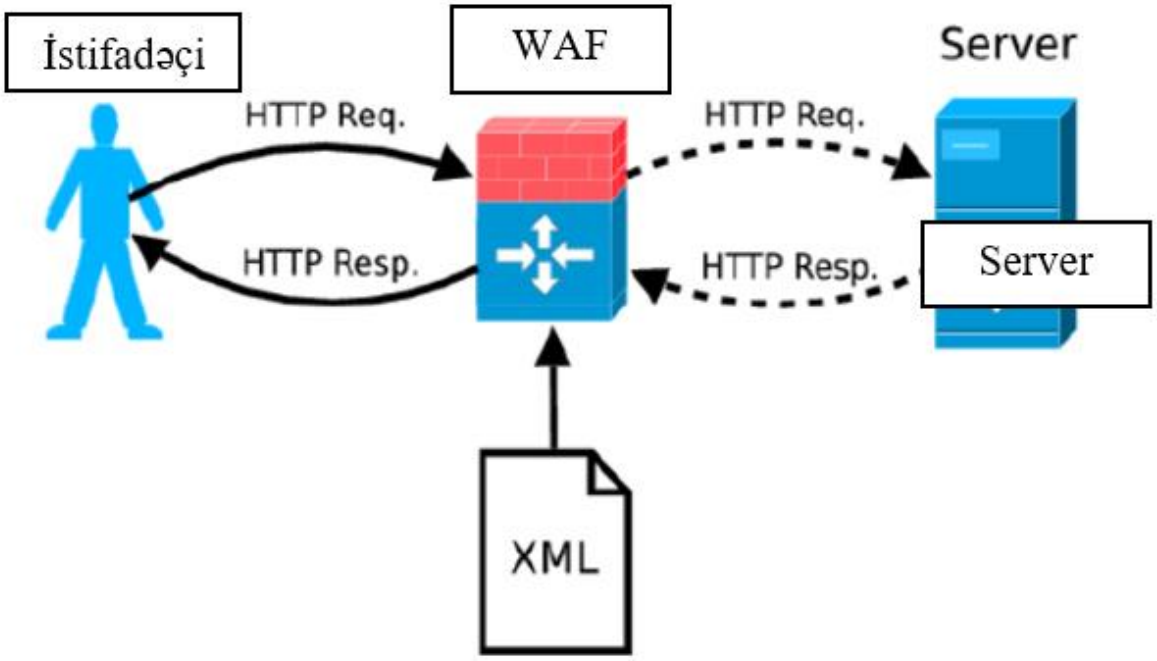
     CSP, XSS hücumlarının qarşısını almaq üçün tətbiq olunan təhlükəsizlik standartıdır. Bu, veb inkişaf etdiricilərə hansı dinamik resursların saytlarında yüklənməsinə icazə verildiyini müəyyən etməyə imkan verir. CSP resurs yükləməni idarə edərək zərərli skriptlərin icrasının qarşısını ala bilər.

Təəssüf ki, şəbəkə və nəqliyyat qatlarında işləyən adi firewalllar veb-xüsusi hücumlardan qorunmaq üçün adətən kifayət etmir. Həqiqətən effektiv olmaq üçün aşkarlama tətbiq təbəqəsinə köçürülməlidir. IDS kompüter sisteminin təhlükəsizliyini poza biləcək zərərli hərəkətləri və davranışları aşkar etmək üçün kompüterdən və ya

şəbəkədən gələn məlumatları təhlil edir. Zərərli davranış aşkar edildikdə, həyəcan siqnalı işə salınır. Ənənəvi olaraq, IDS-lər ya imza aşkarlama sistemləri (həmçinin mənfi yanaşma adlanır) və ya anomaliya aşkarlama sistemləri (pozitiv yanaşma) kimi təsnif edilir. Hibrid müdaxilə aşkarlama sistemi iki yanaşmanın texnikasını özündə birləşdirir. İmzaya əsaslanan yanaşma sistem və proqram təminatının zəif cəhətlərindən istifadə edən məlum hücumların (sistem resurslarından sui-istifadə) imzalarını axtarır. O, hücum imzalarının tez-tez yenilənən verilənlər bazasına qarşı nümunə uyğunlaşdırma üsullarından istifadə edir. Artıq məlum hücumları və ya onların kiçik variasiyalarını aşkar etmək faydalıdır, lakin nümunə tanıma mühərrikini pozan yeni və ya zərərli variasiyaları aşkar etmək deyil. Anomaliyaya əsaslanan yanaşma "normal" və ya "ümumi" davranışdan kənara çıxan davranış və ya kompüter resurslarından istifadəni axtarır (García-Teodoro P., Díaz-Verdejo J., Maciá-Fernández G., Vázquez E. 2009). Bu yanaşmanın əsas prinsipi ondan ibarətdir ki, "hücum davranışı" "normal istifadəçi davranışı"-dan kifayət qədər fərqlidir ki, onu həmin fərqləri kataloqlaşdırmaq və təsvir etməklə aşkar etmək olar. Hər şeydən əvvəl, "normal" davranışı yaxşı müəyyənləşdirmək lazımdır ki, bu da asan məsələ deyil. Normal davranış tam olaraq xarakterizə edildikdən sonra, nizamsız davranış müdaxilə kimi etiketlənəcəkdir. İmzaya əsaslanan IDS-lərin əsas çatışmazlıqlarından biri onların parçalanma, defoltlardan qaçınma, aşağı bant genişliyi hücumları və ya sadəcə nümunənin dəyişdirilməsi kimi yayınma hücumlarına qarşı həssaslığıdır. Bundan əlavə, hücum modelinin uyğunlaşdırılması sistemləri daim yenilənən böyük imza verilənlər bazası tələb edir. Daxil olan trafikin verilənlər bazasındakı hər bir imza ilə müqayisəsi yüksək hesablama zəhməti tələb edir və nəticədə ötürücülük azalır. İmza əsaslı IDS-lərin uğursuz olduğu bu ssenarilərdə anomaliya əsaslı sistemlər normal trafiki imza uyğunluğu olmadan şübhəli fəaliyyətdən ayırmağa imkan verir. Bununla belə, kifayət qədər mürəkkəb mühitlərdə, məsələn, çoxsaylı serverləri və müxtəlif əməliyyat sistemləri olan böyük şəbəkələrdə "normal" şəbəkə trafikinin necə görünməsi barədə müasir və mümkün mənzərəni əldə etmək çətin bir problemdir. Başqa bir çatışmazlıq olaraq, anomaliya əsaslı sistemlərdə yanlış pozitivlərin (səhv

olaraq hücum kimi təsnif edilən hadisələr) dərəcəsi imza əsaslı sistemlərdən daha yüksəkdir.

Veb Tətbiq Firewallları (WAF) veb proqramların təhlükəsizliyini poza biləcək zərərli davranışları aşkar etmək üçün HTTP trafikini (tətbiq qatı) təhlil edir. WAF veb serverə daxil olmağa çalışan müştəri brauzeri tərəfindən göndərilən HTTP sorğularını təhlil edir. Təhlil yalnız tətbiq səviyyəsində aparılır. Sistem mövcud imza əsaslı WAF-lardan fərqli olaraq məlum və naməlum veb hücumlarını aşkar edərək anomaliya əsaslı yanaşmaya əməl edir. ModSecurity (Open Source signature-based Web Application Firewall, 2009) məşhur imza əsaslı WAF-dır. Arxitekturamızda sistem müştəri və veb server arasında yerləşən proxy kimi fəaliyyət göstərir. Eynilə, sistem server daxilində modul kimi yerləşdirilə bilər. Bununla belə, birinci yanaşma veb platformadan müstəqil olmaq üstünlüyünə malikdir. Bu proxy müştəri tərəfindən göndərilən bütün trafiki təhlil edir. Aşkarlama prosesinin girişi HTTP sorğularının toplusundan ibarətdir {r1, r2, . . . rn}. Çıxış hər bir **ri** giriş sorğusu üçün tək bit **ai**-dir, bu sorğunun normal və ya anormal olduğunu göstərir. Proksi iki fərqli iş rejimində işləyə bilir: IDS və ya IPS kimi. Aşkarlama rejimində proksi sadəcə daxil olan paketləri təhlil edir və şübhəli nümunələri tapmağa çalışır. Şübhəli sorğu aşkar edilərsə, proksi xəbərdarlıq göndərir; əks halda qeyri-aktiv qalır. İstənilən halda sorğu veb serverə çatacaq. Aşkarlama rejimində işləyərkən hücumlar uğur qazana bilər, yalançı pozitivlər isə sistemin funksionallığını məhdudlaşdırmır. Qarşısının alınması rejimində proksi müştərilərdən sorğu qəbul edir və onları təhlil edir. Sorğu etibarlıdırsa, proksi onu serverə yönləndirir və alınan cavabı müştəriyə geri göndərir. Əks halda, proksi sorğunu bloklayır və müştəriyə ümumi rədd edilmiş giriş səhifəsini geri göndərir. Beləliklə, proksi ilə server arasında əlaqə yalnız sorğu etibarlı hesab edildikdə qurulur. WAF-ın arxitekturasının diaqramı Şək.4.1.1-də göstərilmişdir.



Şək.4.1.1 WAF-ın arxitekturası (ModSecurity, 2009)

Aşkarlama prosesindən əvvəl sistemə xüsusi veb proqramında normal davranışın nə olduğu barədə dəqiq bir məlumat lazımdır. Bu məqsədlə sistem veb tətbiqinin normal davranışının hərtərəfli təsvirini ehtiva edən XML faylına əsaslanır şək.4.1.2. Sorğu qəbul edildikdən sonra sistem onu normal davranış modeli ilə müqayisə edir. Əgər fərq verilən hədləri keçərsə, sorğu hücum kimi qeyd olunur və xəbərdarlıq işə salınır. XML faylı HTTP davranışlarının, HTTP başlıqlarının, əldə edilmiş resursların (faylların), arqumentlərin və arqumentlər üçün dəyərlərin düzgünlüyü ilə bağlı qaydaları ehtiva edir. Bu faylda üç əsas qovşaq var:

Hərəkətlər - Verbs node sadəcə icazə verilən HTTP fellərinin siyahısını müəyyən edir.

Başlıqlar. Başlıq qovşağı bəzi HTTP başlıqlarının siyahısını və onların icazə verilən dəyərlərini müəyyənləşdirir.

Kataloqlar. Kataloqlar qovşağı, veb tətbiqinin kataloq strukturuna yaxın uyğunluqda ağaca bənzər bir quruluşa malikdir.

1. Veb tətbiqi məkanındakı hər bir kataloq XML faylında kataloq qovşağı ilə təmsil olunur və bu, kataloqların içərisində qovluqların yerləşdirilməsinə imkan verir. Atribut adı bu qovşaqları müəyyən edir.

2. Veb proqram məkanındakı hər bir fayl kataloq qovşağında fayl node ilə təmsil olunur və onun atribut adı ilə müəyyən edilir.

3. Daxiletmə arqumentləri müvafiq fayl node daxilində arqument qovşaqları ilə təmsil olunur. Hər bir arqument öz adı və arqument çatışmırsa sorğunun rədd edilib-edilməməsinin lazım olduğunu göstərən bir boolean dəyəri ilə müəyyən edilir.

4. Arqumentlər üçün hüquqi dəyərlər müvafiq arqument qovşağında stats node ilə təmsil olunan bəzi statistik qaydalara cavab verməlidir. Bu statistik xüsusiyyətlər birlikdə gözlənilən dəyərlərin təsvirini verir. Hər bir müvafiq xüsusiyyət stats node daxilində bir atributla müəyyən edilir. Öz yanaşmamızda aşağıdakı müvafiq xüsusiyyətləri nəzərdən keçirdik:

• icazə verilən xüsusi simvollar dəsti (hərflərdən və rəqəmlərdən fərqlidir).

• lengthMin: minimum giriş uzunluğu

• lengthMax: maksimum giriş uzunluğu

• letterMin: hərflərin minimum faizi

• letterMax: hərflərin maksimum faizi

• digitMin: rəqəmlərin minimum faizi

• digitMax: rəqəmlərin maksimum faizi

• specialMin: xüsusi simvolların minimum faizi (“xüsusi” hesab edilən simvollara daxil olanların)

• specialMax: xüsusi simvolların maksimum faizi (“xüsusi” hesab edilən simvollara daxil olanların)

```
<?xml version="1.0" encoding="iso-8859-1"
 standalone="no"?>
<configuration>
<verbs>
<verb>GET</verb>
<verb>POST</verb>
</verbs>
<headers>
<rule name="Accept-Charset"
value="ISO-8859-1"/>
</headers>
<directories>
<directory name="shop">
<file name="index.jsp"/>
<directory name="public">
<file name="add.jsp">
<argument name="quantity"
requiredField="true">
<stats maxDigit="100"
maxLength="3"
maxLetter="0"
maxOther="0"
minDigit="100"
minLength="1"
minLetter="0"
minOther="0"
special="" />
<argument name="product_name"
requiredField="true">
<stats maxDigit="0"
maxLength="15"
maxLetter="92.94"
maxOther="10.01"
minDigit="0"
minLength="5"
minLetter="89.91"
 minOther="7.15"
 special="" />
 <argument name="price"
 requiredField="true">
 <stats maxDigit="100"
 maxLength="3"
 maxLetter="0"
 maxOther="0"
 minDigit="100"
 minLength="1"
 minLetter="0"
 minOther="0"
 special="" />
 ...  </directories>
 </configuration>
```

Şək.4.1.2 XML fayl nümunəsi (Kənan Həsənov, 2024)

WAF-ın mexanizmləri həm statik, həm də dinamik hücumları aşkar edə bilir. İcazə verilən qovluqlar və fayllar tam dəqiqləşdirildikdə, sistemi üçüncü tərəflərin

yanlış konfiqurasiyasından və məlum zəifliklərdən qoruyur. Bu zəifliklərə qarşı hücumlar adətən çox yaxşı sənədləşdirilir və ictimailəşdirilir. Onlar qanuni istifadəçinin heç vaxt birbaşa tələb etməyəcəyi və beləliklə, aşkarlanması asan olan veb serverlərdə standart olaraq mövcud olan resursların sorğulanmasına etibar edirlər. Buna görə də, kataloqlar və faylların sadalanması köhnəlmiş fayl mövcudluğu, standart fayl və ya nümunə fayl mövcudluğu, server mənbə faylının açıqlanması, HTTP metodunun etibarlılığı, URL girişinin məhdudlaşdırılmaması, veb tətbiqi və serverin yanlış konfiqurasiyası və s.-dən istifadə edən hücumların qarşısını ala bilər.

Parametrləri manipulyasiya edən hücumlar statistik intervalların düzgün müəyyən edilməsi ilə çəpərlənir. Bufer daşması vəziyyətində uzunluq xüsusiyyəti böyük əhəmiyyət kəsb edir. Bir çox hücumlar zərərli hərəkətlər etmək üçün xüsusi simvollardan (adətən hərflərdən və rəqəmlərdən fərqli) istifadə edir. Məsələn, bu, gözlənilmədən yerinə yetirilən sorğu və ya əmrləri əldə etmək üçün SQL-də xüsusi məna daşıyan simvollardan istifadə edən SQL inyeksiyasına aiddir. Bu səbəbdən, hərflərin, rəqəmlərin və xüsusi simvolların minimum və maksimum faizi bu hücumların tanınması üçün çox vacibdir. Bundan əlavə, giriş arqumentində mövcud olan hər hansı bir xüsusi simvol "xüsusi" adlanan xüsusiyyətə daxil edilmədiyi təqdirdə icazə verilmir. Interval yoxlaması CRLF inyeksiyası, etibarsız parametrlər, əmr inyeksiyası, XSS, SQL injection, bufer daşması, pozulmuş autentifikasiya və sessiyanın idarə edilməsi və s. kimi zəifliklərdən istifadə edən hücumları dayandırmağa kömək edir.

Biz sadə və səmərəli veb hücumun aşkarlanması sistemini və ya WAF təqdim etdik. Sistem anomaliya əsaslı metodologiyaya əsaslandığı üçün o, veb proqramlarını həm məlum, həm də naməlum hücumlardan qoruya bilər. Sistem daxiletmə sorğularını təhlil edir və onların anormal olub-olmamasına qərar verir. Qərar vermək üçün WAF veb tətbiqinin normal davranışını təyin edən XML faylına əsaslanır. Təcrübələr göstərir ki, XML faylı verilmiş hədəf tətbiqi üçün normallığı düzgün müəyyən etdikcə, mükəmmələ yaxın nəticələr əldə edilir. Beləliklə, əsas problem istənilən veb tətbiqi üçün tam avtomatlaşdırılmış şəkildə dəqiq XML faylının necə yaradılmasıdır. Biz göstəririk ki, hədəf tətbiq üçün çox böyük miqdarda normal (zərərli olmayan) trafik

mövcuddur, bu avtomatik konfiqurasiya giriş trafikinin statistik xarakteristikası ilə mümkündür.

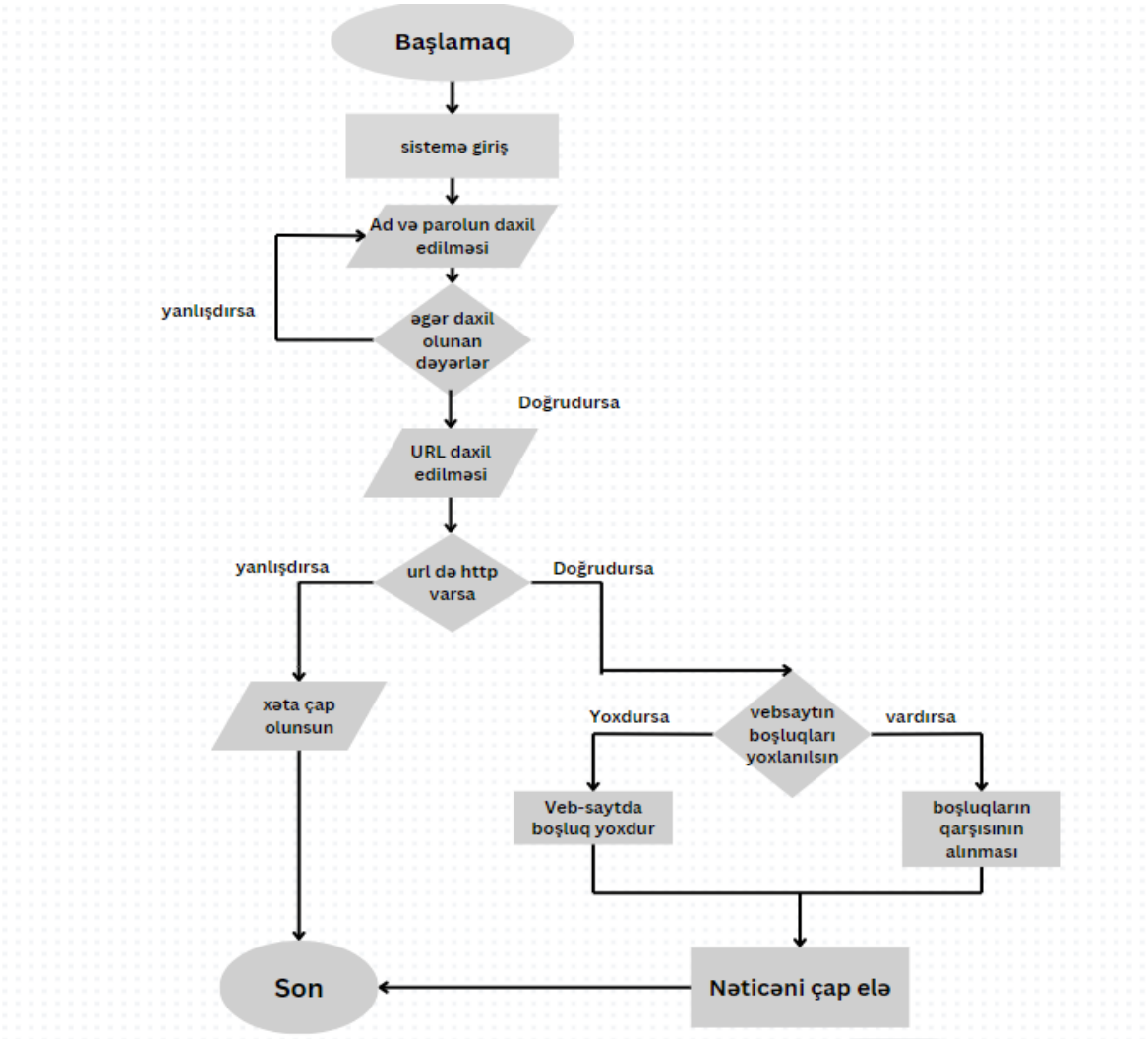
4.2 Veb təhdidlərin qarşısının alınması üçün mövcud modellər

Veb proqramları internet üzərindən təqdim olunan bir çox xidmətlər üçün əsas interfeys rolunu oynayan qurumların mühüm aspektinə çevrilmişdir. Nəticə etibarilə, bu xidmətlərin artan nüfuzu ilə əlaqədar olaraq veb proqramlara qarşı hücumlar artır. Təhlükəsizliyə marağın olmaması, qeyri-kafi məlumatlılıq və təhlükəsiz proqram təminatının inkişaf etdirilməsi üsullarından istifadə edilməməsi də daxil olmaqla bir neçə faktor səbəbindən veb tətbiqləri hücumların əsas hədəfinə çevrilib. Veb əsaslı hücumların təxminən 70%-nin uğurlu olduğu təxmin edilir. Ənənəvi firewalllar şəbəkə qatının hücumlarının qarşısını almaqda təsirli olsa da, veb proqramları hədəf alan hücumlardan müdafiədə zəif olur. Buna görə də, mahiyyət etibarilə etibarsız mühit olan internetdə veb proqramları , həssas məlumatları qorumaq və zəiflikləri azaltmaq üçün gücləndirilmiş təhlükəsizlik tədbirlərinə ciddi ehtiyac var.

Təhlükəsizlik zəiflikləri və xətalar aşkar edildikdən sonra təklif etdiyimiz yanaşma vebsayta hücumların qarşısını almaq üçün proqramçıya əməl etməli olduğu bir sıra təlimatları təklif edir (Najla Odeh, Sherin Hijazi, 2023). Ümumilikdə, metod potensial zəiflikləri müəyyən etməklə və onların azaldılmasına dair təlimatlar təqdim etməklə veb proqramlarda təhlükəsizlik zəifliklərinin aşkarlanması və qarşısının alınması üçün kompleks yanaşma təmin etmək məqsədi daşıyır **şək.4.2.1** və **şək.4.2.2**.

Hücumların Qarşısının alınması metdoları

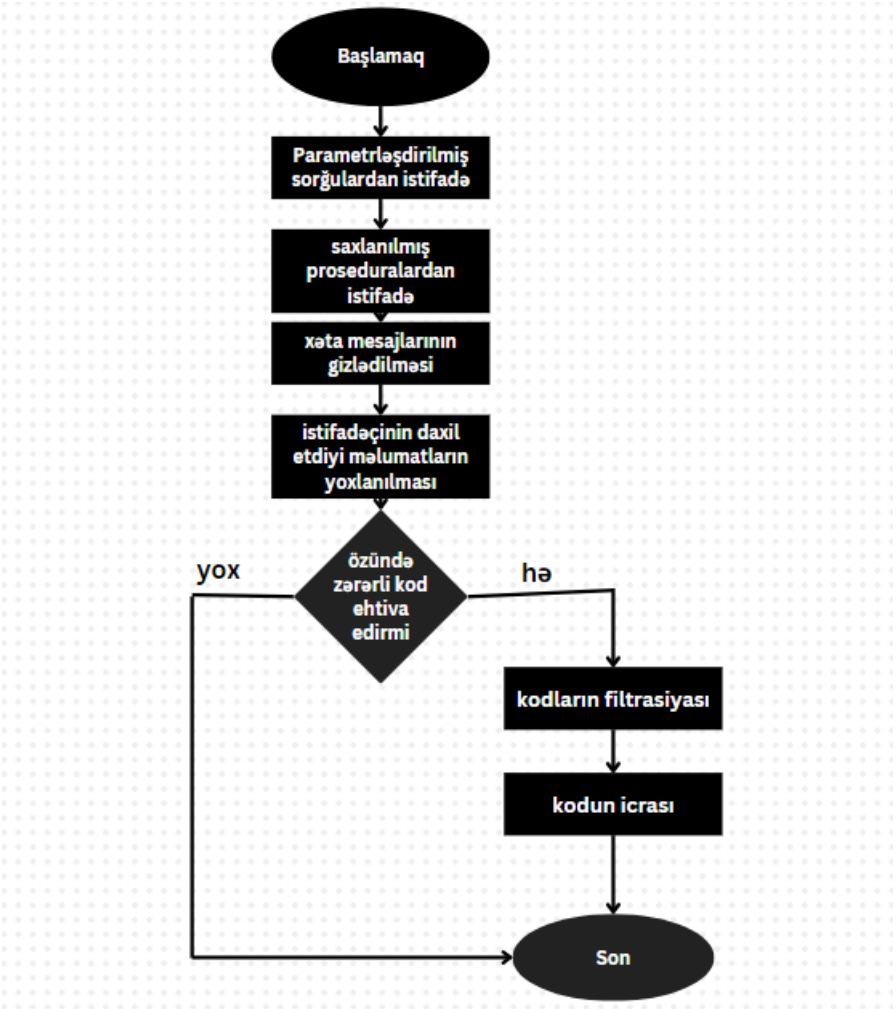
Hakerlər şəxsi və həssas məlumatları idarə etmək üçün back-end tərəfdə DBMS-də SQL-dən istifadə edən vebsaytlara hücum etdikdə, kredit kartı məlumatları, hesab adları və parollar kimi dəyərli və həssas məlumatlara giriş əldə etmək üçün SQLI hücumundan istifadə edirlər. Buna görə də təklif olunan sistem SQLI hücumlarının qarşısını almaq üçün lazımi mexanizm təqdim edir. **Şək.4.2.3** təlimatları göstərir.



Şək.4.2.1. Təklif olunan metodun blok-sxemi (Najla Odeh, Sherin Hijazi, 2023)

```
/*************************************************************************/
1. Start
2. step1
    a. Login to proposed system
    b. Input username and password
    c. If data not valid, go to step 2b
3. step2
    a. Input URL
    b. Check if URL has http:
        i. If no, go to step 5
        ii. If yes, go to step 3c
    c. Check website vulnerability
4. step3
    a. If the site is infected, do the prevent process
        i. Perform prevent process
        ii. Print report
    b. If the site is not infected, print report
5. End
*************************************************************************/
```

Şək.4.2.2. Təklif olunan metodun alqoritmi

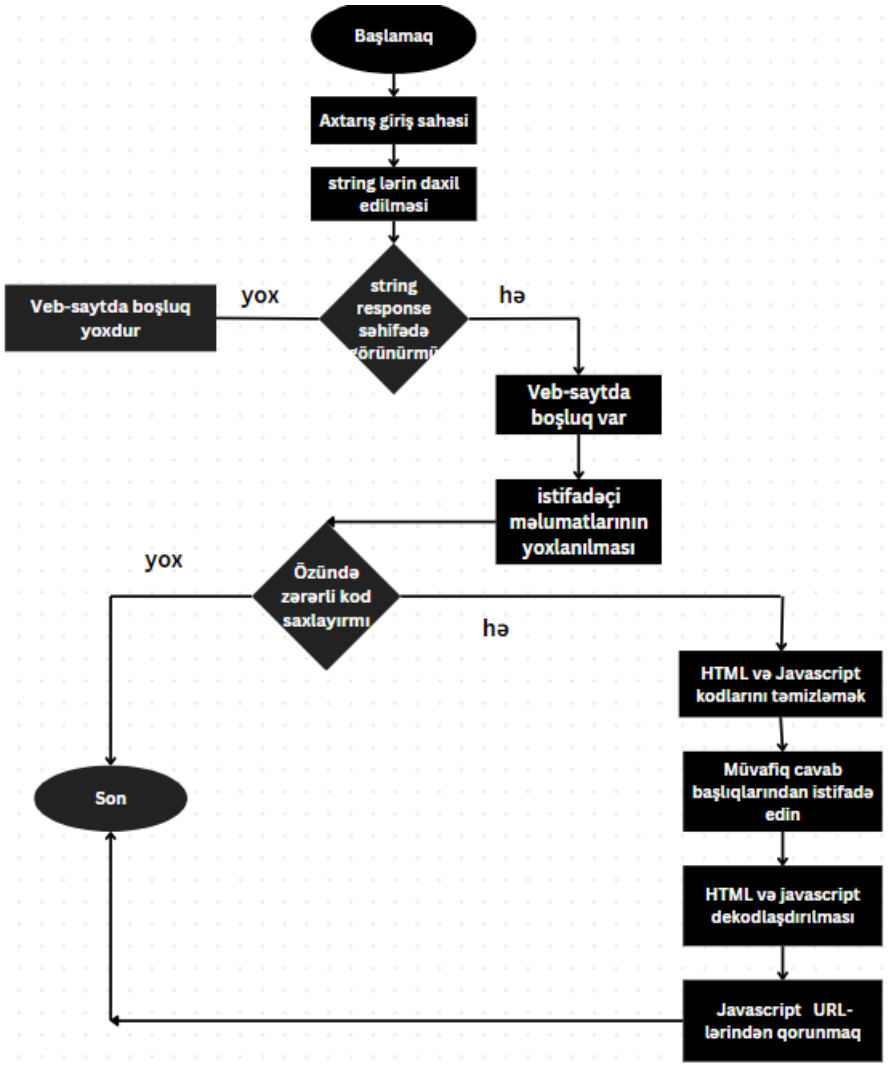


Şək.4.2.3 SQLI boşluğunun qarşısının alınması (Najla Odeh, Sherin Hijazi, 2023)

SQL inyeksiyalarının qarşısını almaq üçün ən yaxşı mexanizm parametrləşdirilmiş sorğular (hazırlanmış ifadələr) və saxlanılan prosedurlar kimi təhlükəsiz proqramlaşdırma üsullarından istifadə etməkdir. İstifadəçi qeydlərinə etibar etməmək də vacibdir; dinamik SQL sorğularında istifadə edilməzdən əvvəl onlar həmişə təmizlənməlidirlər. SQL sorğularını işə salmazdan əvvəl potensial təhlükəli kodu aşkar etmək və aradan qaldırmaq üçün müntəzəm sorğulardan istifadə edilə bilər. Verilənlər bazası bağlantısı üçün istifadəçi giriş icazələri müəyyən edilməlidir və verilənlər bazasına qoşulmaq üçün istifadə olunan hesablar yalnız onlara lazım olan giriş imtiyazlarına malik olmalıdır. Xəta mesajlarının vacib məlumatları və ya səhvin hardan qaynaqlandığına dair hər hansı bir məlumatı özündə saxlamaması vacibdir. Hansı SQL sorğularının xətaya səbəb olduğunu göstərmək əvəzinə sadə fərdi xəta mesajlarından istifadə etmək olar.

XSS Zəifliklərinin qarşısının alınması

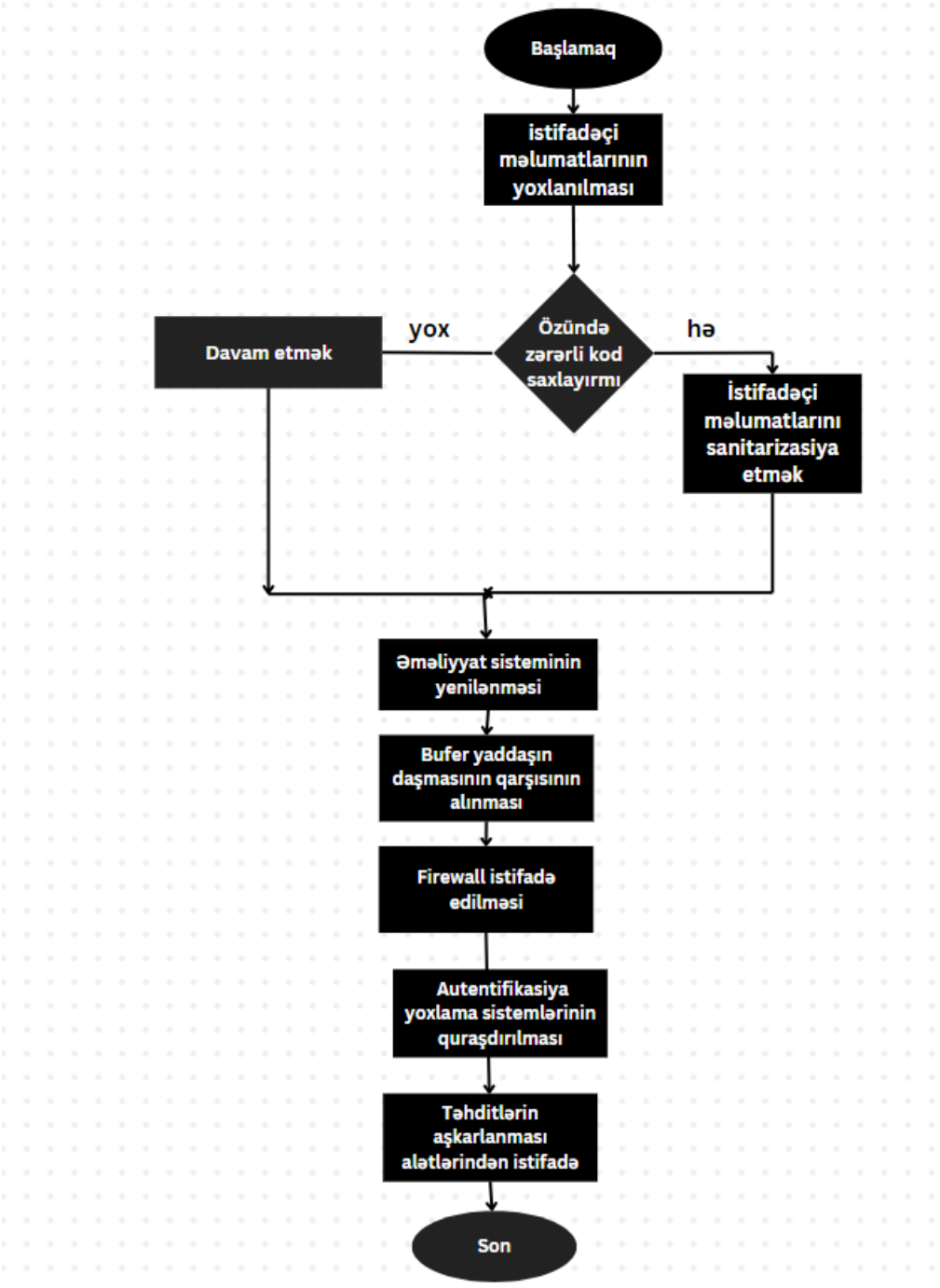
XSS hücumları veb-sayt hücumlarının ən məşhur növlərindən biridir. Təklif olunan sistem XSS hücumunun qarşısını almaq üçün mexanizm təqdim edir. **Şək.4.2.4** təlimatları göstərir.



Şək.4.2.4 XSS Zəifliklərinin qarşısının alınması metodunun blok-sxemi (Najla Odeh, Sherin Hijazi, 2023)

XSS zəifliyinin qarşısını almaq üçün tətbiq bütün girişləri yoxlamalı, yalnız etibarlı məlumatlara icazə verilməsini təmin etməli və istifadəçiyə təqdim edilməzdən əvvəl veb saytında görünən hər hansı bir dəyişənin şifrələndiyini təsdiqləməlidir. Məzmun təhlükəsizliyi siyasətinə də riayət edilməlidir. Məzmun təhlükəsizliyi siyasəti (CSP) XSS-də qalan zəifliklər aradan qaldırmaq üçün son müdafiə xətti kimi istifadə edilə bilər.

Uzaqdan kod icra hücumu (ing. A remote code execution attack) serverdə kodu icra edən uzaqdan hücumçunu əhatə edir. Təcavüzkar dünyanın istənilən yerində ola bilər və ya təcavüzkar olduğu yerdən cihaz və ya serverə daxil olmaq və eyni zamanda əmrləri yerinə yetirmək üçün zəiflikdən istifadə edir. Təklif olunan sistem RCE hücumunun qarşısını almaq üçün mexanizm təqdim edir. **Şək.4.2.5** addımları göstərir.



Şək.4.2.5 RCE boşluqlarının qarşısının alınması blok-sxemi (Najla Odeh, Sherin Hijazi, 2023)

RCE zəifliyinin qarşısını almaq üçün istifadəçi girişinin dezinfeksiya edilməsini təmin etmək vacibdir və ən yaxşısı qiymətləndirilmiş kodda istifadəçi daxiletməsindən istifadə etməməkdir. İstifadəçiyə müvafiq proqramlaşdırma dili ilə təhlil edilmiş faylların məzmununu dəyişdirməyə icazə verilməməlidir. Əməliyyat sistemini yeni saxlamaq və bufer daşqınından qorunma istifadə etmək lazımdır. Həmçinin bir firewall istifadə edərək təhdidlərin vaxtında aşkar edilməsini təmin etmək olar.

Nəticə olaraq, bu iş veb proqramlardakı zəifliklərin aşkarlanması və qarşısının alınması sistemini təqdim edir, xüsusilə bu növlərə diqqət yetirir: SQL inyeksiyası, saytlar arası skript hücumları və uzaqdan kod icrası. İşdə hər bir zəiflik növünün necə işlədiyi və onları müəyyən etmək üçün aşkarlama metodunun necə tətbiq oluna biləcəyi barədə ətraflı izahatlar verilmişdir. Tədqiqatın elmi əsaslandırması məxfi məlumatı poza biləcək zəifliklərin qarşısını almaq və aşkar etməklə veb tətbiqi təhlükəsizliyini artırmaq üçün kritik ehtiyacı həll etməkdir. Gələcək tədqiqatlar da, digər növ zəiflikləri qiymətləndirmək və səhvlər üçün avtomatlaşdırılmış sistem düzəlişlərini daxil etməklə bu iş genişləndirilə bilər. Veb tətbiqləri getdikcə daha çox yayıldıqca və mürəkkəbləşdikcə bu sahədə irəliləyişlər kritik olaraq qalacaq.

NƏTİCƏ

Magistr dissertasiya mövzusu əlaqədar veb-sayt və platformalarin analizi ilə başlamış, qarşıya qoyulmuş bir neçə məsələ istiqamətində tədqiqatlar aparılmaqla aşağıdakı nəticələrlə yekunlaşmışdır:

- Veb-sayt və platformaların konsepsiyasının arxitektur-texnoloji prinsipləri araşdırılmış;
- Veb mühitində olan kritik kodlaşdırma təhlil olunmuş;
- Kritik kodlaşdırmanı əhatə edən mümkün hücum ssenariləri, təhdidləri və boşluqları göstərilmiş;
- Təhdidlərin aşkarlanması üçün vasitələr və alətlər haqqında məlumat verilmiş;
- Platformalarda olan hücumların statistikası çıxarılmış;
- Veb-saytlara olan hücumların, təhdidlərin qarşısının alınması üçün tədbirlər, mexanizmlər işlənmiş;
- Həssas məlumatların oğurlanmasının qarşısının alınması üçün müxtəlif öyrənmə metodları göstərilmiş;
- Hücumlara məruz qalmamaq üçün istifadəçi maarifləndirilməsinin aparılması haqqında məlumat verilmişdir.

ƏDƏBİYYAT SİYAHISI

"Analyzing web traffic: Ecml/pkdd 2007 discovery challenge," http://www.lirmm.fr/pkdd2007-challenge/.

Arvind Goutam , Vijay Tiwari "Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application" 16 March 2020. **DOI:** 10.1109/ISCON47742.2019.9036175

B. Gallagher and T. Eliassi-Rad, "Classification of http attacks: a study on the ecml/pkdd 2007 discovery challenge," Lawrence Livermore National Laboratory (LLNL), Livermore, CA, Tech. Rep., July 2009.

Benson V, Saridakis G, Tennakoon H, Ezingeard JN (2015) The role of security notices and online consumer behaviour: an empirical study of social networking users. Int J Hum Comput Stud 80:36–44. https://www.researchgate.net/publication/275634525_The_role_of_security_notices_and_online_consumer_behaviour_an_empirical_study_of_social_networking_users

Betarte, G., Gimenez, E., Martinez, R., & Pardo, A. (2018). Improving Web Application Firewalls through Anomaly Detection. 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). **DOI:** 10.1109/ICMLA.2018.00124

Butler W. Lampson, "Computer security in the real world". IEEE Computer 37, 6 (June 2004), pp. 37-46. DOI:10.1109/MC.2004.17

C. Folini. (2016) Handling false positives with the owasp modsecurity core rule set. [Online]. Available:https://www.netnea.com/cms/apache-tutorial-8handling-false-positives-modsecurity-core-rule-set/

C. Raıssi, J. Brissaud, G. Dray, P. Poncelet, M. Roche, and M. Teisseire, "Web analyzing traffic challenge: description and results," in Proceedings of the ECML/PKDD, 2007, pp. 47–52.

David Watson, " Web App Attacks: Web application attacks" Network Security, Volume 2007 Issue 10, October 2007, Pages 10-

14.https://www.academia.edu/52676511/Survey_of_Web_Application_and_Internet_Security_Threats.

Gaik-Yee Chana, Fang-Fang Chuaa and Chien-Sing Leeb, "Fuzzy association rules vs fuzzy associative patterns in defending against web service attacks", 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, 2015, pp. 524-529. https://doi.org/10.3233/JIFS-169007

García-Teodoro P., Díaz-Verdejo J., Maciá-Fernández G., Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges, Computers and Security, 28, 1-2, 18-28 (2009)

Gregory Terzian "The Web Platform Explanied" Mar 27,2023 https://medium.com/the-web-platform-explained/introducing-theweb-platform-da6b98c52ead

H. Tabrizchi and M. K. Rafsanjani, "A survey on security challenges in cloud computing: Issues, threats, and solutions," Journal of Supercomputing, vol. 76, no. 12, pp. 9493–9532, 2020. DOI:10.1007/s11227-020-03213-1

https://www.giac.org/paper/gsec/2298/mitigating-web-application-risks-security-code-review-appscan/103975

https://www.isis.vanderbilt.edu/sites/isis.vanderbilt.edu/files/bibcite_files/main_0_0.pdf

Jing Wang , Hongjun Wu "URFDS: Systematic discovery of Unvalidated Redirects and Forwards in web applications" 07 December 2015. DOI: 10.1109/CNS.2015.7346891

K. Pachopoulos, D. Valsamou, D. Mavroeidis, and M. Vazirgiannis, "Feature extraction from web traffic data for the application of data mining algorithms in attack identification." Citeseer, 2007.

Kevin Spett, "SQL Injection", Whitepaper, 2002 SPI Dynamic Inc. https://repo.zenksecurity.com/Techniques%20d.attaques%20%20.%20%20Failles/SQL%20Injection.pdf

Kumar, D. Garg and P. S. Rana, "Ensemble approach to detect profile injection attack in recommender system", International Conference on Advances in

Computing, Communications and Informatics (ICACCI), , Kochi, 2015, pp. 1734-1740. DOI: 10.1109/ICACCI.2015.7275575

M. Exbrayat, “Ecml/pkdd challenge: analyzing web traffic a boundaries signature approach,” 2007, p. 53.

Marjan Korosec and Joze Duhovnik, "Identification and optimization of key process parameters in noncontact laser scanning for reverse engineering", Journal of ComputerAided Design , Volume 42 Issue 8, August, 2010 , pages 744-748. https://www.academia.edu/52676511/Survey_of_Web_Application_and_Internet_Security_Threats

Mburano, B.; Si, W. Evaluation of web vulnerability scanners based on owasp benchmark. In Proceedings of the 2018 26th International Conference on Systems Engineering (ICSEng), Sydney, NSW, Australia, 18–20 December 2018; pp. 1–6. https://doi.org/10.1109/ICSENG.2018.8638176

Mina Askari, Reihaneh Safavi-Naini, and Ken Barker, "An information theoretic privacy and utility measure for data sanitization mechanisms", Proceedings of the second ACM conference on Data and Application Security and Privacy (CODASPY), 2012 ACM. https://doi.org/10.1145/2133601.2133637

ModSecurity. Open Source signature-based Web Application Firewall. http://www.modsecurity.org (2009)

Naderi-Afooshteh, Anh Nguyen-Tuong, M. Bagheri-Marzijarani, J. D. Hiser and J. W. Davidson, “Joza: Hybrid Taint Inference for Defeating Web Application SQL Injection Attacks”, 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Rio de Janeiro, 2015, pp. 172-183. **DOI:** 10.1109/DSN.2015.13

Najla Odeh, Sherin Hijazi, "Detecting and Preventing Common Web Application Vulnerabilities: A Comprehensive Approach", International Journal of Information Technology and Computer Science(IJITCS), Vol.15, No.3, pp.26-41, 2023. DOI:10.5815/ijitcs.2023.03.03

Novel approaches to identify and prevent cyber attacks in web Sodagudi, S., Kotha, S.K., David Raju, M.Proceedings of the 3rd International Conference on

Computing Methodologies and Communication, ICCMC 2019, 2019, pp.1099-1101, 8819822. **DOI:** 10.1109/ICCMC.2019.8819822

Novel approaches to identify and prevent cyber attacks in webSodagudi, S., Kotha, S.K., David Raju, M.Proceedings of the 3rd International Conference on Computing Methodologies and Communication, ICCMC 2019, 2019, pp.1099-1101, 8819822

OWASP. Owasp modsecurity core rule set project. [Online]. Available: https://www.owasp.org/index.php/

Pandiaraja, P., and J. Manikandan, "Web proxy based detection and protection mechanisms against client based HTTP attacks", IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2015. **DOI:** 10.1109/ICCPCT.2015.7159344

Peder Jungck, and Simon S.Y. Shim, "Issues in High Speed Internet Security", Computing Practices published by the IEEE Computer Society, 2004 IEEE.

R. Shukla and M. Singh, "PythonHoneyMonkey: Detecting malicious web URLs on client side honeypot systems", 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), Noida, 2014, pp. 1-5. **DOI:** 10.1109/MC.2004.58

Rahul Johari and Pankaj Sharma, "A Survey on Web Application Vulnerabilities (SQLIA, XSS) Exploitation, Proceedings of the 2012 International Conference on Communication Systems and Network Technologies Pages. DOI: 10.1109/CSNT.2012.104

Sahoo SR, Gupta BB (2020) Fake profle detection in multimedia big data on online social networks. Int J Inf Comput Secur 12(2–3):303–331. https://doi.org/10.1504/IJICS.2020.105181

Shebli, H.M.Z.A.; Beheshti, B.D. A study on penetration testing process and tools. In Proceedings of the 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 4 May 2018. DOI:10.1109/LISAT.2018.8378035

Steve Petite, “ANATOMY OF A WEB APPLICATION: Security Considerations”, White Paper, Sanctum Inc., July, 2001.

Xiaowei Li and Yuan Xue, “A Survey on Web Application Security”, Technical report, Vanderbilt University, 2011.