UOT 004.056.53

***İmamverdiyev Y.N.*[1]*, Tarverdiyev L.Ə.*[2]**
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]yadigar@lan.ab.az, [2]latif@iit.ab.az

VEB TƏHLÜKƏSİZLİYİN QİYMƏTLƏNDİRİLMƏSİ METODLARININ ANALİZİ

Veb texnologiyalar e-dövlət xidmətlərinin göstərilməsi, biznesin həyata keçirilməsi, sosial şəbəkə və sosial media vasitəsi kimi geniş yayılmışdır. Lakin Veb texnologiya özü ilə birlikdə bir sıra informasiya təhlükəsizliyi problemləri də gətirir və veb sistemləri bədniyyətlilərin cəlbedici hədəfinə çevirir. Bu məqalədə veb təhlükəsizliyin komponentləri, veb təhlükəsizliyin qiymətləndirilməsinə mövcud metodoloji yanaşmalar, veb-tətbiqlərdə boşluqların aşkarlanması üzrə metodlar və veb-saytların reputasiya sistemləri analiz edilir.

Açar sözlər: *veb təhlükəsizlik, veb tətbiqlərin təhlükəsizliyi, veb reputasiya sistemləri, TrustRank, SQL inyeksiya hücumları, XSS hücumlar, Web Mining.*

Giriş

1991-ci ildə TimBernesLee tərəfindən ilk veb-səhifə ideyası reallaşdırıldıqdan sonra qısa müddət ərzində veb-texnologiyalar böyük sürətlə inkişaf etmiş, qlobal informasiya fəzasını bütün istiqamətlərdə əhatə edən Ümumdünya Hörümçək Toru (World Wide Web, WWW) yaranmışdır. Hazırda e-dövlət mühitində, biznes dünyasında və vətəndaş cəmiyyətində tərəflərin informasiya qarşılıqlı təsiri əsasən veb-texnologiyalar vasitəsilə həyata keçirilir.

Hazırda dünyanın əksər ölkələrində bir çox e-dövlət xidməti veb-texnologiyalar vasitəsilə vətəndaşlara və biznes sektoruna əlyetəndir. Bir sıra qiymətləndirmə metodologiyalarında e-dövlətin inkişaf mərhələləri bilavasitə veb-texnologiyalardan istifadə səviyyəsi ilə müəyyən edilir [1]: veb-də təmsilçilik; veb-sayt vasitəsilə qarşılıqlı əlaqə; onlayn tranzaksiyalar; transformasiya. Biznes strukturları həm daxili informasiya sistemlərini, həm də müştərilərlə qarşılıqlı biznes əlaqələrini veb-texnologiyalar əsasında reallaşdırmağa üstünlük verirlər; e-kommersiya, İnternet-bankinq, onlayn ödəniş sistemləri və s. geniş istifadə olunur. Veb 2.0 texnologiyası istifadəçiləri bilavasitə veb-kontentin yaradılmasına qoşur, onlayn sosial şəbəkələrin və sosial medianın geniş inkişafına əlverişli şərait yaradır.

Təəssüf ki, veb-texnologiyaların geniş yayılması özü ilə bir sıra informasiya təhlükəsizliyi problemləri də gətirir. Veb-kontentin yaradılmasında və istifadəçiyə çatdırılmasında bir çox elementlər – veb-server, verilənlər bazası, veb-tətbiqlər, veb-proqramlaşdırma dilləri, veb-brauzerlər və s. iştirak edir. Təbii ki, bu elementlərdə meydana çıxa bilən bütün problemləri qabaqcadan müəyyənləşdirmək mümkün deyil. Nəticədə bədniyyətlilər veb-tətbiqlərə XSS (Cross-Site Scripting), SQL injection kimi spesifik hücumları həyata keçirə bilirlər.

Veb təhlükəsizlik sahəsində ixtisaslaşan şirkətlərin təqdim etdikləri statistik məlumatlara görə veb-saytların 80 %-ində kritik boşluqlar mövcuddur [2]. Başqa bir statistikaya görə, veb-saytların 70%-də ya ziyanlı kontent, ya da heç nədən şübhələnməyən istifadəçini qanuni saytlardan ziyanlı saytlara yönəltmək üçün maskalanmış keçidlər var [3]. Bu boşluqlardan istifadə ehtimalı kifayət qədər yüksəkdir və bu hücumlar həssas korporativ məlumatların, məsələn, kredit kartı məlumatlarının və müştərilərin siyahısının oğurlanmasına gətirib çıxara bilər. Belə hücum faktları çoxdur və veb-hücumlar son dövrlər daha da intensivləşir [4]. Veb sistemlərə olan hücumların qarşısını almaq və baş verə biləcək hücumları əvvəlcədən aşkarlamaq üçün bir sıra metodoloji yanaşmalar və onlarla proqram təminatları mövcuddur.

Veb təhlükəsizliyin komponentləri

Adətən, veb təhlükəsizliyi veb-saytın təhlükəsizliyi ilə eyniləşdirirlər. Lakin veb təhlükəsizlik bütün veb ekosisteminin komponentlərinin təhlükəsizliyindən yaranır:

- istifadəçinin kompüteri və veb-brauzeri;
- şəbəkələrarası ekran, müdaxilələrin aşkarlanması sistemi (Intrusion Detection System, IDS), veb-tətbiq şəbəkələrarası ekranı (Web Application Firewall, WAF);
- yüklənmənin balanslaşdırılması sistemi;
- veb-server;
- veb-tətbiqlər (tətbiqi proqramlar);
- arxa plan (verilənlər bazasını idarəetmə sistemi (VBIS), XML, SOAP və s);
- komponentlər arasındakı əlaqə kanalları.

Veb hücumlar kliyent tərəfindən geniş istifadə edilən Adobe PDF Reader, Java, Quick Time, Adobe Flash və Microsoft Office kimi proqramlardakı boşluqları istismar edirlər. Bu boşluqlar təhlükəli veb-saytlara baş çəkənləri yoluxdurmaq üçün də istifadə edilir.

Server tərəfdə SQL operatorlarının inyeksiyası, parolların seçilməsi, əməliyyat sistemi komandalarının yerinə yetirilməsi, kliyent tərəfdə ssenarilərin saytlararası yerinə yetirilməsi, HTTP-sorğunun yenidən yönləndirilməsi kimi hücumlar daha çox istifadə edilir.

Mövcud elmi-praktiki tədqiqatlar daha çox veb-saytların, veb-tətbiqlərin və veb-servislərin təhlükəsizliyini əhatə edir.

Veb-tətbiq veb-serverdə yerləşən tətbiqi proqramdır, avtorizasiyadan keçmiş istifadəçi veb-tətbiqə İnternet və ya İntranet şəbəkəsi ilə giriş əldə edə bilər. Veb-tətbiqlərə formalar, forumlar, e-kommersiya, bloqlar və s. aid edilə bilər. Veb-tətbiqlər adətən, PHP (HypertextPreprocessor), Java EE, Java, Python, Ruby, ASP.NET, C#, VB.NET və klassik ASP (Active Server Pages) kimi proqramlaşdırma dillərindən istifadə etməklə yaradılır.

Veb-tətbiq üçsəviyyəli tətbiqi proqramdır. Adətən, birinci səviyyədə veb-brauzer, ikinci səviyyədə Java servisləri və ya ASP kimi kontent generasiyası texnologiyaları, üçüncü səviyyədə isə korporativ verilənlər bazası olur. Veb-brauzer aralıq səviyyəyə ilkin sorğu göndərir, o da öz növbəsində sorğunu yerinə yetirmək üçün verilənlər bazasına müraciət edir, bazadan verilənləri alır və ya onlara dəyişiklik edir.

Veb-tətbiqlər serverdə yerləşdiyindən onları kliyent maşınlarında proqram təminatı quraşdırılmadan istənilən vaxt modifikasiya etmək olar – bu, təşkilatlarda veb-tətbiqlərin geniş yayılmasının əsas səbəblərindəndir.

Veb-servis arxitekturası kliyentə SOAP (Simple Object Access Protocol) protokolundan istifadə etməklə verilənləri serverdən almağa imkan verən müxtəlif texnologiyalardan ibarətdir. Veb-servis XML-dən istifadə etməklə veb və ya şəbəkə vasitəsilə əlaqə yaratmağa imkan verən veb API interfeysi ilə (application programming interface) təmin edilmişdir. Veb-servislər WSDL (Web Serviced Description Language) kimi tanınan XML formatından istifadə edirlər, burada şəbəkə servisləri komponentlər çoxluğu kimi təsvir olunur. Komponentlər müvafiq şəbəkə protokolundan istifadə etməklə məlumat mübadiləsi edirlər. Veb-servis arxitekturasının vacib elementi bütün servislərin təsvirlərinin olduğu mərkəzi kataloq – UDDI (Universal Description Discovery and İntegration) provayderidir.

Gartnerin tədqiqatlarına görə veb-saytlara yönələn hücumların 75%-i infrastrukturu deyil, tətbiqi proqram səviyyəsini hədəf alır [5]. Bədniyyətlilər bilirlər ki, ənənəvi təhlükəsizlik metodları veb-tətbiqlərə qarşı hücumları dayandıra bilmir. Veb-tətbiqlər mahiyyətcə veb-saytlarda olan verilənlərə müraciət etməyə imkan yaradır. Veb-tətbiqlərdəki sadə boşluqlardan istifadə etməklə, bədniyyətli şəbəkələrarası ekran və IDS sistemlərinin olmasına baxmayaraq, təhlükəsizlik perimetrindən keçərək verilənlərə və hətta şəbəkəyə giriş əldə edə bilər. Veb-tətbiqlərin təhlükəsizliyi HTTP paketlərini yoxlamaqla OSI modelinin (open systems interconnection basic reference model) 7-ci səviyyəsində təhdidlərin emalına əsaslanır.

Veb-də təhlükəsizlik boşluqlarının klassifikasiyası

Veb təhlükəsizlik sahəsində fəaliyyət göstərən WASC (Web Application Security Consortium) və OWASP (Open Web Application Security Project) konsorsiumları veb-tətbiqlərə

xas təhdidlərin (WASC TC v.2) və boşluqların klassifikasiyası (OWASP Top 10) sistemlərini təklif etmişlər [6, 7]. İstifadə edilən terminlərlə əlaqədar bu iki klassifikasiya sistemi arasında müəyyən ziddiyyətlər mövcuddur.

OWASP konsorsiumunun təklif etdiyi boşluqlar klassifikatoru daha məşhurdur. Aşağıda bu klassifikasiya haqqında qısa məlumat verilir. "OWASP Top 10 - 2013 - Release Candidate" [7] siyahısına aşağıdakı 10 boşluq sinfi daxildir:

- A1-İnyeksiya boşluqları;
- A2-Natamam autentifikasiya və sessiyaların idarə edilməsi;
- A3-Saytlararası skriptlər;
- A4-Obyektə birbaşa təhlükəli müraciətlər;
- A5-Təhlükəsizliyin səhv konfiqurasiya edilməsi;
- A6-Həssas məlumatlara təsirlər;
- A7-Funksiyalar səviyyəsində girişə nəzarətin olmaması;
- A8-Saytlararası sorğuların saxtalaşdırılması;
- A9-Məlum zəif komponentlərdən istifadə;
- A10-Yeni saytlara yönləndirmələrin yoxlanmaması.

Bu boşluqların geniş izahı [7, 8]-də verilmişdir.

WASC klassifikatorunda veb-təhdidlərin aşağıdakı siniflərinə baxılır [9]:

Zəif parol bərpasının yoxlanması (Weak Password Recovery Validation) – bu zəiflik veb-serverə hücum edənə digər istifadəçilərin parollarını icazəsiz əldə etməyə, modifikasiya və ya bərpa etməyə şərait yaradır.

Veb-tətbiqlərdə qeydiyyat zamanı parollardan istifadə olunur. Vaxt keçdikcə parol unudulur. Vəziyyət onunla mürəkkəbləşir ki, istifadəçinin sistemdə yadda saxlamalı olduğu parolların sayı çoxalır. Beləliklə, parolu bərpaetmə funksiyası veb-serverlərin təqdim etdiyi servislərin vacib tərkib hissəsinə çevrilir.

Parolu bərpa sistemi kobud gücdən, sistemin boşluqlarından istifadə etməklə və ya məxfi suala asan tapılan cavab səbəbindən nüfuzdan düşə bilər.

Kobud güc (Brute Force) – İstifadəçinin adını, parolunu, kredit kartının nömrəsini, kriptoqrafik açarı və s. tapmaq üçün istifadə edilən avtomatlaşdırılmış üsuldur. Sistemlərin bir çoxu zəif parollardan və şifrləmə açarlarından istifadə etməyə imkan verir və istifadəçilər çox vaxt asan tapılan və ya lüğətlərdə olan parolları seçirlər. Bundan istifadə edərək bədəməl lüğətdə olan simvollar kombinasiyasını parol kimi istifadə etməyə cəhd edir. Əgər yoxlanan parol sistemə giriş əldə etməyə imkan verirsə, hücum uğurlu sayılır və hücum edən uçot yazısından istifadə edə bilər.

Yetərsiz audentifikasiya (İnsufficient Authentication) – bu təhdid veb-server lazımı audentifikasiya olmadan hücum edənə vacib informasiyaya və ya serverin funksiyalarına giriş əldə etməyə imkan verdikdə meydana çıxır.

Audentifikasiyadan istifadə etməmək üçün bəzi resurslar serverin əsas səhifələrində göstərilməyən müəyyən ünvanlarda və ya digər ümumi istifadə resurslarında "gizlədilir". Başa düşmək vacibdir ki, bədəməl səhifənin ünvanını bilməsə də, səhifə veb-dən əlyetəndir.

Mandat/Sessiya İndentifikatoru (Credential/Session Prediction) – sessiya identifikatorunun təxmin edilən qiyməti başqa istifadəçilərin sessiyalarını ələ keçirməyə imkan verir. Belə hücumlar istifadəçi sessiyasının unikal identifikatorunu qabaqcadan tapmaq və ya təxmin etmək yolu ilə yerinə yetirilir. Bu hücum və sessiyanın ələ keçirilməsi (Session Hijacking) uğurlu olduqda, bədniyyətliyə sorğuları nüfuzdan düşmüş istifadəçi hüquqları ilə veb-serverə göndərmək imkanı verir.

Yetərsiz avtorizasiya (Insufficient Authorization) – veb-server bədniyyətliyə məhdud girişli vacib informasiya və funksiyalara giriş əldə etməyə imkan verdikdə meydana çıxır. İstifadəçinin

audentifikasiyadan keçməsi o demək deyil ki, o, serverin bütün funksiyalarına və məzmununa giriş əldə etməlidir, audentifikasiyadan başqa avtorizasiya da realizə edilməlidir.

Avtorizasiya proseduru istifadəçinin, xidmətin və ya proqramın hansı əməliyyatları yerinə yetirmə hüququnun olduğunu müəyyən edir. Düzgün qurulmuş giriş qaydaları istifadəçinin əməliyyatlarını təhlükəsizlik siyasətinə uyğun olaraq məhdudlaşdırmalıdır. Saytın vacib resurslarına giriş yalnız administratorlara icazə verilməlidir.

Sessiyanın fiksə edilməsi (Session Fixation) – hücumlarından istifadə edərək bədniyyətli istifadəçi sessiyası identifikatoruna verilən qiyməti mənimsədir. Serverin funksional imkanlarından asılı olaraq, sessiya identifikatorunun qiymətini fiksə etmənin bir neçə üsulu var. Bunun üçün ssenarilərin saytlararası yerinə yetirilməsi hücumları və ya HTTP sorğunun köməyi ilə saytın qabaqcadan hazırlanması istifadə edilə bilər. Sessiya identifikatorunun qiymətini fiksə etdikdən sonra, bədniyyətli istifadəçinin sistemə girməsi anını gözləyir. İstifadəçi daxil olduqdan sonra bədniyyətli istifadəçinin adından sistemə girmək üçün sessiya identifikatorundan istifadə edir.

Funksionallığın Sui-istifadəsi (Abuse of Functionality) – veb-saytın xüsusiyyətlərindən və onun funksionallığından istifadə edərək ona və ya digər şəxslərə hücum etməyə imkan verir. Bu hücumlar resursların mənimsənilməsi, girişə nəzarətdən yan keçmək və ya informasiya itkisi kimi müxtəlif nəticələrə malikdir. Sui-istifadənin potensialı və səviyyəsi veb-saytlardan və proqramlardan asılı olaraq dəyişəcəkdir. Funksionallığın sui-istifadəsi hücumu başqa tip hücumların kombinasiyası və ya hücumların başqa istiqamətlərindən istifadə etməklə həyata keçirilir.

Buferin daşması (Buffer-Overflow) – buferin daşmasından istifadə edilməsi bədniyyətliyə sistemin yaddaşında verilənlərin yenidən yazılması üsulu ilə proqramın icra yolunu dəyişməyə imkan verir. Buferin daşmasından istifadə edərək bədniyyətli prosesin ünvan hissəsini dəyişdirməyə nail olur. Buferin daşması proqramlardakı səhvlərin ən geniş yayılmış səbəblərindəndir. O, verilənlərin həcmi onlara ayrılmış buferin uzunluğundan böyük olduqda, baş verir. Bufer daşdıqda, verilənlər yaddaşın başqa sahələrinə yazılır. Bu da səhvin meydana çıxmasına səbəb olur. Əgər bədniyyətlinin daşma prosesini idarə etmək imkanı olarsa, bu bir sıra ciddi problemlər yarada bilər.

Kontentin saxtalaşdırılması (Content Spoofing) – bədniyyətli bu hücumdan istifadə edərək istifadəçini səhifənin kənar mənbədən ötürüldüyünə deyil, veb-server tərəfindən generasiya edildiyinə inanmağa məcbur edir. Xüsusi yaradılmış istinad, elektron poçt məlumatları ani mübadilə sistemi ilə göndərilməklə, elanlar lövhəsində nəşr edilməklə və ya ssenarilərin saytlararası yerinə yetirilməsindən istifadə etməklə istifadəçinin brauzerinə göndərilə bilər. Əgər hücum edən istifadəçini xüsusi yaradılmış istinad üzrə keçməyə təhrik edərsə, istifadəçidə elə təəssürat yaradıla bilər ki, o serverdəki verilənlərə baxır, halbuki onların bir hissəsi bədniyyətli tərəfindən generasiya edilir.

Xidmətdən imtina (Denial of Service DoS) – bu sinif hücumlar veb-serverin əlyetənliyinin pozulmasına yönəlib. Adətən xidmətdən imtinaya yönələn hücumlar şəbəkə səviyyəsində realizə olunur, lakin onlar tətbiqi səviyyəyə də yönələ bilər. Bədniyyətli veb-tətbiqlərin funksiyalarından istifadə etməklə sistemin kritik resurslarını tükədə bilər və ya sistemin işini dayandırmağa səbəb olan boşluqlardan istifadə edə bilər.

Adətən DoS hücumları hesablama gücləri, operativ yaddaş, disk fəzası və ya rabitə kanalının buraxma qabiliyyəti kimi kritik sistem resurslarının tükədilməsinə yönəlir. Əgər resurslardan hər hansı biri maksimal dərəcədə yüklənsə, proqram bütövlükdə əlyetməz olacaq.

Bu hücumlar veb-tətbiqin komponentlərindən istənilən birinə yönələ bilər, məsələn, verilənlər bazası serveri, autentifikasiya serveri və s. Bədniyyətliyə xeyli resurs tələb edən şəbəkə səviyyəsi hücumlarından fərqli olaraq, tətbiqi səviyyə hücumlarını realizə etmək asandır.

Veb-saytlarda boşluqların analizi metodları

Veb-təhlükəsizliyin test edilməsi çox vacib və kirtik məsələdir, çünki bu gün e-hökumət xidmətlərinin veb-texnologiyalar vasitəsi ilə həyata keçirildiyi, özəl sektorun İnternet vasitəsilə biznes fəaliyyəti göstərdiyi bir şəraitdə veb-resursların korlanması həmin təşkilatlar üçün son dərəcə neqativ sonluqla nəticələnə bilər. Veb-saytlarda boşluqların analizi zamanı əmin olmaq lazımdır ki, veb-saytlarda kifayət qədər autentifikasiya və avtorizasiya mexanizmləri istifadə edilir.

Veb-saytların təhlükəsizliyinin test edilməsi üçün bir sıra metodlar mövcuddur [6,7].

Veb-tətbiqlərdə boşluqların test edilməsinin OWASP metoduna görə 9 kateqoriyada birləşdirilmiş 60-dan artıq test yerinə yetirilməlidir [6]:

- konfiqurasiyaların idarə edilməsinin test edilməsi;
- iş məntiqinin test edilməsi;
- autentifikasiyanın test edilməsi;
- avtorizasiyanın test edilməsi;
- sessiyaların idarə edilməsinin test edilməsi;
- verilənlərin düzgünlüyünün yoxlanılmasının test edilməsi;
- xidmətdən imtinanın test edilməsi;
- veb-servislərin test edilməsi;
- AJAX (Asynchronous Javascript and XML)-ın test edilməsi.

Ümumiyyətlə, proqram təminatının təhlükəsizliyinin test edilməsində nüfuzetmə testləri (penetration testing), "qara qutu", "ağ qutu", fuzzing testləri kimi metodlar tətbiq edilir [10–13].

"Qara qutu" test metodunda veb-tətbiqin ilkin kodları istifadə edilmir. Boşluqların axtarışı "əllə" və avtomatik skanerlərin istifadəsi ilə aparılır. Bu test metodu bədniyyətlinin hərəkətlərinə daha yaxındır [12].

"Ağ qutu" test metodunda veb-tətbiqin ilkin kodları analiz edilir. Statik və dinamik analiz metodlarından istifadə edilir. Statik testlərdə ilkin kodun analizi aparılır, müəyyən boşluqlar yoxlanır. Dinamik testlərdə tətbiqi proqram yerinə yetirilir və verilən sorğu üçün cavabın gözlənilən olub-olmaması yoxlanır. Bu metod boşluqlar haqqında tam hesabat verir, çünki təkcə mövcud boşluqları deyil, potensial boşluqları da aşkarlamağa imkan verir [13].

Pixy [14] kimi bir sıra metodlar boşluqların tapılması üçün statik analiz metodlarına əsaslanır. Amnesia [15] kimi digər metodlar boşluqları icra vaxtı aşkar etmək üçün statik analiz və dinamik analiz metodlarını birgə istifadə edir. Statik analiz kodu tam əhatə etsə də, testlər tez-tez qeyri-dəqiq nəticələnir. Parosun [16] istifadə etdiyi nüfuzetmə testləri (penetration testing) geniş yayılmış test metodudur, dəqiq nəticələr verir, lakin kodu əhatə etmə səviyyəsi aşağıdır.

"Qara qutu" test metoduna əlavə olaraq aparılan fuzzing testlər veb-proqramlar üçün yaxşı nəticələr verir. Fuzzing testlər zamanı tətbiqi proqrama ilkin verilənlər əvəzinə düzgün olmayan, təsadüfi və ya proqramın məntiqində nəzərə alınmayan verilənlər verilir. Çox zaman təsadüfi verilənlər istifadə edilir. Düzgün olmayan giriş verilənləri müvafiq səhv məlumatları yaratmalıdır. Əgər bu zaman proqramın işi dayanırsa və ya işini qəza ilə qurtarırsa, onda bu proqramda nasazlığın tapılması deməkdir və bu müəyyən boşluğun tapılmasına gətirib çıxara bilər.

Test məlumatlarının generasiyası üçün [17]-də təsvir edilmiş alqoritmdən istifadə edilir. Məsələn, *str* dəyişənində olan giriş məlumatları üçün *str == "mod"* predikatının TRUE olacağı test məlumatları əldə etmək üçün hər bir sətir əvvəlcə

$$\xi(str) = \sum_{i=0}^{L-1} str[i]\, x\omega^{L-i-1}$$

alqoritminə əsasən mənfi olmayan tam ədədə inikas olunur. Burada L – *str* sətrinin uzunluğudur, ω = 128 kimi təyin edilir.

İki sətir arasındakı məsafəni hesablamaq üçün

$$dis(str_1, str_2) = \left| \sum_{i=0}^{L_1-1} str_1[i]\, x\omega^{L-i-1} - \sum_{i=0}^{L_2-1} str_2[i]\, x\omega^{L-i-1} - \right|$$

məsafə funksiyasından istifadə edilir. Alqoritm giriş məlumatının hər bir simvolunu tədricən o vaxta kimi dəyişdirir ki, *str* dəyişəninin giriş qiyməti "*mod*" olsun.

Fuzzinq testlərini avtomatik yerinə yetirmək üçün bir sıra proqram vasitələri vardır. OWASP JBroFuzz boşluq fazzeri HTTP, SOAP, XML, LDAP və digər şəbəkə protokolları ilə işləyir. Bu fazzer XSS, SQL-inyeksiya, buferin daşması, format sətrinin səhvləri və s. kimi boşluqların qeyri-standart metodlarla çoxsaylı yoxlanmasını yerinə yetirir.

Funksional testlərdə ayrı-ayrı funksiyaların düzgün işləməsi yoxlanılır. Veb-tətbiqlərdə funksional testlərə istinadların yoxlanması, istifadəçinin etdiyi dəyişikliklərin veb-səhifədə, verilənlər bazasında əks olunmasının yoxlanması daxil ola bilər.

Veb reputasiya sistemləri

Veb-saytların təhlükəsizliyini əvvəlcədən müəyyən etmək üçün veb reputasiya sistemlərindən istifadə edilir. Reputasiya sayta inamın səviyyəsini göstərir. İstifadəçilər fırıldaqçı və etibarsız İnternet mağazalardan istifadə zamanı arzuolunmaz kontentlərin yüklənməsi və fişinq kimi fırıldaqçılığa məruz qalmamaq üçün reputasiyası yüksək olan veb-saytlardan istifadə etməlidirlər.

Veb reputasiya indeksləri veb-saytın müəyyən xarakteristikalarını (ISP/WebHost, IP ünvanlarını), kontentini (JavaScript, PHP, ASP.NET, üzə çıxan pəncərələr, yönləndirmələr, yükləmələr və s.) nəzərə alaraq 0–100 ballıq sistemə əsasən beş kriteriyaya görə qiymətləndirir. Reputasiya göstəriciləri 0–20 aralığında dəyişən saytlar yüksək riskli, 21–40 aralığında dəyişən saytlar naməlum və şübhəli saytlar, 41–60 aralığında dəyişən saytlar orta riskli, 61–80 aralığında dəyişən saytlar aşağı riskli, 81–100 aralığında dəyişən saytlar isə etibarlı saytlar qrupuna daxildir [18].

Veb-saytların reputasiyasının qiymətləndirilməsini həyata keçirən bir çox proqram təminatları (Avast WebRep, AVG LinkScanner, Dr. Web LinkChecker, McAfee, SiteAdvisor, Norton Safe Web, Intel) mövcuddur. Bunlardan ən çox istifadə olunan WOT (Web of Trust) plaqinidir [19].

WOT brauzerlər üçün nəzərdə tutulmuş pulsuz plaqindir, İnternet-istifadəçilərə reputasiyası aşağı olan saytlarda informasiya axtarışı və ya alış-veriş zamanı xəbərdarlıq edir. WOT Google Chrome, Safari, Internet Explorer, Mozilla Firefox və Opera kimi brauzerlərlə işləyə bilir [20]. Quraşdırıldıqdan sonra brauzerin alətlər panelində WOT loqotipi görünür. İstifadəçi yeni sayta keçdikdə, saytın reputasiyasından asılı olaraq loqotipin rəngi dəyişir. Yaşıl rəng saytın təhlükəsiz olduğunu bildirir, sarı rəng ehtiyatlı olmağı, qırmızı rəng isə sayta getməməyi məsləhət görür.

WOT veb-saytın reputasiyasını 4 kriteriyaya əsasən qiymətləndirir. Bunlara etibarlılıq, konfidensiallıq, satıcının etibarlılığı və uşaqların təhlükəsizliyi aiddir. Saytın reputasiyası WOT-istifadəçilərinin verdikləri qiymətlər və etibarlı mənbələrdən alınmış informasiya (məsələn, fişinq saytlarının siyahısı) əsasında hesablanır.

WOT reputasiyanın bir sıra problemləri var. Bəzən təhlükəsiz sayt aşağı reputasiya indeksi və əksinə, təhlükəli sayt yüksək reputasiya indeksi ala bilər. Bundan əlavə, istifadəçilərin reputasiya indeksi ilə manipulyasiya etmək imkanı da var.

Cisco IronPort veb reputasiya texnologiyasında veb reputasiya süzgəcləri veb trafik və şəbəkə aktivliyi ilə bağlı 200-dən artıq müxtəlif parametrləri analiz edərək saytın reputasiyasını

müəyyən edir [21]. Cisco IronPort qurğusu Cisco Security Intelligence Operations (SIO) bulud təhlükəsizlik servisindən istifadə edir, Cisco SIO öz növbəsində verilənləri təhdidlərin SensorBase monitorinqi şəbəkəsindən alır və mürəkkəb analiz əsasında hər bir parametrin çəkisini müəyyən edir və saytın reytinqini [-10,10] intervalında hesablayır. Reputasiyanın qiyməti veb obyektdə ziyanlı proqram təminatının olması ehtimalı ilə əlaqəlidir, -10 ən yüksək, +10 isə ən aşağı ehtimala uyğundur.

Bəzi axtarış sistemləri (Google, Yahoo) spama qarşı mübarizə məqsədi ilə veb-saytların reputasiya səviyyəsini müəyyən etmək üçün TrustRank alqoritmindən istifadə edirlər [22]. Qeyd edək ki, hazırda bir çox veb-saytlar axtarış sistemlərində öz reytinqlərini yüksəltmək üçün müxtəlif spam metodlarından istifadə edirlər. Belə veb-səhifələri işarələmək üçün veb-spam termini işlədilir.

TrustRank saytın reputasiya ranqını müəyyən etmək üçün domenin yaşı, tarixi və səviyyəsi, kontentin unikallığı, nüfuzlu kataloqlarda qeydiyyatının olması, resursun yenilənməsi tezliyi, sayta olan istinadların sayı, saytdan digər saytlara istinadların sayı və s. kimi parametrlər istifadə edir.

TrustRank veb-spam olan səhifələrin yarım-avtomatik şəkildə müəyyən olunmasında istifadə olunan istinad-analiz metodudur. TrustRank alqoritminin əsas ideyası ondan ibarətdir ki, iki veb-səhifə arasındakı istinad onlar arasında inamı bildirir və adətən, yaxşı səhifələr yaxşı səhifələrə, spam-səhifələr isə spam-səhifələrə istinad yerləşdirirlər. TrustRankın iş prinsipi aşağıdakı kimidir. Əvvəlcə ekspertlər veb-də yaxşı tanınan və inam göstərilən saytların siyahısını tərtib edirlər. Bu saytların hər birinə inam qiymətləri (məsələn, 100 ballıq şkala ilə) təyin edilir. Sonra PageRank alqoritminin biased PageRank variantından [23, 24] istifadə etməklə bu inam qiyməti səhifələrdən çıxan istinadlara yayılır. Hesablamaların sonunda yaxşı saytlar yüksək inam qiymətlərinə malik olur, inam qiymətləri seçilmiş sərhəd qiymətlərindən kiçik olan veb-səhifələr isə veb-spam hesab olunurlar.

Web Mining metodlarının veb təhlükəsizliyə tətbiqləri

Web Mining – intellektual analiz metodlarından istifadə edərək veb-də olan sənədlərin və xidmətlərin avtomatik aşkar edilməsi, veb-resurslardan informasiyanın üzə çıxarılması və İnternetdə ümumi qanunauyğunluqların aşkarlanması metodudur [25].

Web Miningin aşağıdakı istiqamətlərini ayırırlar:

- Web Content Mining (veb-məzmunun çıxarılması);
- Web Structure Mining (veb-strukturun çıxarılması);
- Web Usage Mining (veb-resurslardan istifadənin intellektual analizi).

Web Content Mining – İnternetdə əlyetən sənədlərin və ya onların təsvirinin məzmunundan informasiyanın əldə edilməsi prosesidir [26]. İnternet şəbəkəsində informasiyanın axtarışı çətin və zəhmətli prosesdir. Məhz Web Miningin bu istiqaməti onu həll edir. Web Mining informasiya axtarışının, maşın təliminin və verilənlərin intellektual analizinin imkanlarına əsaslanır.

Web Structure Mining – İnternetdə informasiyanın strukturunun aşkar edilməsi prosesidir [27]. Bu istiqamət veb-səhifələr arasında əlaqələri gözdən keçirir və onlar arasında qarşılıqlı əlaqələrə əsaslanır. Bu model oxşar veb-resursların axtarışı, həmçinin müəllif saytlarının tanınması üçün istifadə edilə bilər.

Web Usage Mining – istifadəçinin hərəkət marşrutunda şablonların və onunla bağlı bir neçə veb-saytla qarşılıqlı əlaqə nəticəsində yığılmış və ya əldə edilmiş məlumatların avtomatik aşkar edilməsidir [28]. Bu istiqamət veb-serverlərin loq-fayllarından məlumatların çıxarılmasına əsaslanır. Bu analizin hədəfi İnternet şəbəkəsinin bu və ya digər resurslarından istifadə zamanı ziyarətçilərin seçimlərinin üzə çıxarılmasıdır. İnformasiya təhlükəsizliyində daha çox Web Usage Mining tətbiq edilir.

Web Usage Mining texnologiyası onu korporasiyalar və həmçinin dövlət idarələri üçün cazibədar edən bir sıra üstünlüklərə malikdir [29]:

- bu texnologiya elektron ticarətin artmasına gətirib çıxaran fərdiləşdirilmiş marketinqi yaratmağa imkan yaradır.
- dövlət orqanları təhlükələrin (təhdidlərin) təsnifatı və terrorizmlə mübarizə üçün bu texnologiyadan istifadə edirlər.

Web Usage Mining – proksi-serverdən, brauzerdən, istifadəçinin sessiya məlumatlarından, istifadəçinin giriş loqlarından faydalı məlumatların çıxarılması prosesidir. Sadə dillə desək, Web Usage Mining istifadəçilərin İnternetdə nə axtardıqlarını müəyyənləşdirən prosesdir. Bəzi istifadəçilər yalnız maraqlı mətn məlumatlarından istifadə etsələr də, digərləri multimedia məlumatlarına daha çox üstünlük verir [30].

Veb-serverlərdə backdoor və ya informasiya itkisini veb mining metodlarını veb-loq və veb-tətbiqlərin loq fayllarına tətbiq edərək aşkar etmək mümkündür. Veb-serverin təhlükəsizliyinin yüksəldilməsi qanunsuz girişlərdən dəyəcək ziyanların qarşısını ala bilər. Birincisi, sistemin veb-loqlarından informasiya itkisinin qanunauyğunluğunun aşkar edilməsi üçün CGI (Computer-generated imagery) skriptlərindən istifadə edilir. İkincisi, sistem administratorları üçün öz kodlarını təkmilləşdirmək və veb-saytların təhlükəsizliyini artırmaq üçün bu metodlardan nümunələr təklif olunur. Daha çox informasiya əldə etmək üçün veb-loqların və veb-tətbiqlərin loqlarının birləşməsindən ibarət məlumatlar analiz edilir. Serverlərin sessiyalarının klasterləşməsi, texnika əsasında qruplaşdırmanın sıxlığı resursların dəyərinin azalması və ən böyük effektivliyin alınması üçün istifadə olunur [31].

Loq-fayllar istifadəçinin adını, IP-ünvanını, vaxt ştampını, giriş sorğusunu, göndərilən URL-i (Uniform Resource Locator), göndərilən informasiyanın həcmi haqqında məlumatları özündə cəmləyir. Bu loq-faylları təhlil edərək istifadəçi haqqında müfəssəl məlumata sahib olmaq mümkündür [32, 33].

Son illərdə veb-də məlumatların intellektual analizi əhəmiyyətli sahəyə çevrilmişdir. Əsasən bu İnternetdən əlyetən informasiyanın böyük miqdara malik olması ilə bağlıdır, əksər elmi cəmiyyətlərin və son zamanlar elektron ticarətin marağını cəlb edir [34].

Nəticə

Veb texnologiyası sosial şəbəkələr, e-hökumət servislərinin göstərilməsi, elektron ticarət, bank tranzaksiyalarının həyata keçirilməsi vasitəsi kimi veb-texnologiyaların qəbul edilməsini şərtləndirilmişdir. Veb-texnologiyaların sürətlə inkişafı və geniş istifadəsi təhlükəsizlik problemlərini ortaya çıxarır.

Bu məqalədə veb-tətbiqlərin təhlükəsizlik problemləri araşdırılmış, veb-tətbiqlərin təhlükəsizlik komponentləri, veb-saytlarda olan boşluqların aşkarlanması metodları, boşluqların analizi alətləri haqqında məlumat və boşluqların klassifikasiyası göstərilmişdir. Veb-saytların təhlükəsizliyinin qiymətləndirilməsində istifadə olunan veb-reputasiya sistemləri, TrustRank və vebdə verilənlərin intellektual analiz metodlarının veb-təhlükəsizlikdə istifadəsi analiz edilmişdir.

Ədəbiyyat

1. Baum C., Di Maio A. Gartners four phases of e-government model, 2000, http://www.gartner.com/DisplayDocument?id=317292.
2. Positive Technologies статистика уязвимостей веб-приложений, 2012, http://ptsecurity.ru/download/analitika_web.pdf.
3. Websense Security Labs State of Internet Security, Q3 – Q4, 2008, http://community.websense.com/blogs/websense-features/archive/2010/02/01/websense-security-labs-report-state-of-internet-security-q3-q4-2009.aspx.
4. Tappenden A.F., Beatty P., Miller J. Security Testing of Web-Based Systems via HTTPUnit. AGILE , 2005, pp.29–38.
5. Business Justification for Application Security Assessment,

https: // www. Owasp .org / index. php / Business_Justification_for_Application_Security Assesment.
6. OWASP Testing Project, http://www.owasp.org/index.php/Category:OWASP_Testing_Project.
7. The OpenWeb Application Security Project. OWASP Testing Guide V3.0, http://www.owasp.org/index.php/Category:OWASP_Testing_Project.
8. Imamverdiyev Y.N., Tarverdiyev L.A. Analysis of web security vulnerabilities / 1st National Scientific-Practical Conference on "Problems of Information Security" dedicated to the 90th birthday anniversary of national leader of the Azerbaijani people Heydar Aliyev, 2013, pp. 122–125.
9. The WASC Threat Classification v2.0, http://projects.webappsec.org/w/page/13246978/Threat%20Classification.
10. Arkin B., Stender S., McGraw G. Software penetration testing. IEEE Security & Privacy, 2005, no.3, pp. 84–87.
11. Thompson H.H. Application penetration testing. IEEE Security & Privacy, 2005, no.3, pp. 66–69.
12. Hope P.,Walther B. Web Security Testing Cookbook. O'Reilly, Sebastopol, 2008, pp.1–285.
13. Antunes N., and Vieira M. Security Testing in SOAs: Techniques and Tools, in Innovative technologies for dependable OTS-based critical systems, 2013, vol. 1, pp. 159–174.
14. Jovanovic N., Kruegel C., Kirda E. Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper) / Proc. of the 2006 IEEE Symposium on Security and Privacy, 2006, pp. 258–263.
15. Halfond W., Orso A. AMNESIA: Analysis and Monitoring for NEutralizing SQLInjection Attacks / Proc. of the 20th IEEE/ACM International Conference on Automated Software Engineering (ASE), 2005, pp. 174–183.
16. Chinotec Technologies Company. Paros, http://www.parosproxy.org
17. Zhao R., Lyu M.R. Character String Predicate Based Automatic Software Test Data Generation / Proc. of the Third international Conference on Quality Software (QSIC 2003), 2003, pp. 255–262.
18. How Web Reputation increases your online protection / GFI white paper, 2011, pp. 2–7.
19. Website reputation ratings, http://en.wikipedia.org/wiki/Website_reputation_ratings#cite_note-1.
20. WOT (Web of Trust), http://www.mywot.com/ru/support/tour
21. CISCO IronPort Web Reputation Technology: Protecting Against URL Based Threats http://www.cisco.com/en/US/prod/vpndevc/ps10142/ps10164/web_rep_index.html.
22. Gyongyi Z., Garcia-Molina H., Pedersen J. Combating Web Spam with TrustRank / Proc. of the 30th VLDB Conference, Toronto, Canada, 2004, pp. 576–587.
23. Bianchini M., Gori M. and Scarselli F. Inside Page-Rank. Tech. rep., University of Siena, 2003, pp. 92–128.
24. Langville A. and Meyer C. Deeper inside PageRank. Tech. rep., North Carolina State University, 2003, pp. 1–33.
25. Hsinchun C., Michael C. Web Mining: Machine Learning for Web Applications // Annual Review of Information Science and Technology (ARIST), 2004, vol. 38, pp. 289–329.
26. Sivaramakrishnan J., Balakrishnan V. Web Mining Functions in an Academic Search Application / Faculty of Computer Science and Engineering, BITS – PILANI, Dubai, U.A.E, 2009, pp. 132–139.
27. Srivastava J., Desikan P., Kumar V. Web Mining – Concepts, Applications, and Research Directions / Chapter 21, 2004, pp. 51–71.
28. Bing L. Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data. Springer, 2011, 642 p.

29. Paola B., Damian M., Hernan M., Ramón G.M. Web Usage Mining Using Self Organized Maps // IJCSNS International Journal of Computer Science and Network Security, 2007, vol.7, №6, pp. 45–50.
30. Sharma A. Web Usage Mining: Data Preprocessing, Pattern Discovery and Pattern Analysis on the RIT Web Data, 2008, pp. 1–44.
31. Zhang G., Gu G., Li J. The design and implementation of web mining in web sites security // Journal of Marine Science and Application, 2003, vol. 2, №1, pp. 81–86.
32. Joshila L.K.G., Maheswari V., Dhinaharan N. Analysis of web logs and web user in Web Mining // International Journal of Network Security & Its Applications, 2011, vol.3, №1, pp. 99–110.
33. Юсифов Ф.Ф. Извлечение знаний из Internet с использованием лог-файлов // Проблемы информационных технологий, 2010, №1, с.45–54.
34. Malika M., Bharat B., Mukesh M. Data Mining for web security: UserWatcher / CERIAS Tech Report 2001-20, https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2001-20.pdf.

УДК 004.056.53

Имамвердиев Ядигар Н.[1], Тарвердиев Лятиф А.[2]
Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]yadigar@lan.ab.az, [2]latif@iit.ab.az

Анализ методов оценки безопасности веб-технологий

Веб-технологии широко распространены в электронных государственных услугах, реализации бизнеса, социальных сетях и как средства социальных медиа. Это влечет за собой ряд вопросов информационной безопасности, и веб-система становится привлекательной мишенью для злоумышленника. В данной статье анализируются компоненты веб-безопасности, существующие методологические подходы к оценке веб-безопасности, методы для обнаружения уязвимостей в веб-приложениях и системы репутации веб-сайтов.

Ключевые слова: *безопасность веб, безопасность веб-приложений, системы веб-репутации, TrustRank, атаки SQL инъекции, XSS атаки, Web Mining.*

Yadigar N. İmamverdiyev[1], Latif A. Tarverdiyev[2]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]yadigar@lan.ab.az, [2]latif@iit.ab.az

Web security assessment methods analysis

Web technologies are widespread as a means of e-government services, business implementations, social networking and social media. It brings a number of information security issues and becomes an attractive target for web system malware. The paper analyzes the web security components, methodological approaches to web security assessment, the methods for detecting gaps of web-applications, and reputation systems web-sites.

Keywords: *web security, web application security, web reputation systems, TrustRank, SQL injection attacks, XSS attacks,Web Mining.*