Veb-saytlarda təhlükəsizlik boşluqlarının analizi

Lətif Tarverdiyev[1], Yadigar İmamverdiyev[2]

AMEA İnformasiya Texnologiyaları İnstitutu

[1]latif@iit.ab.az, [2]yadigar@lan.ab.az

***Xülasə*— Veb-texnologiyalar e-dövlətdə, sosial mediada, mobil platformalarda, bank tranzaksiyalarında və s. geniş istifadə olunur. Bu səbəbdən də onlar bədniyyətlilərin hücum hədəflərinə çevrilir və veb-sistemlərdə informasiya təhlükəsizliyinin təmin olunması olduqca aktualdır. Bu işdə veb-saytların mövcud təhlükəsizlik boşluqlarının avtomatik analizi üzrə eksperimentlər aparılır və həmin analizin nəticələri təqdim olunur.**

Açar sözlər*— *veb-sayt; veb təhlükəsizlik;təhlükəsizlik boşluqları; inyeksiya hücumları; saytlararası skript hücumları

I. GİRİŞ

Veb-saytlar vətəndaşlara, dövlət, kommersiya və ictimai təşkilatlara İnternet şəbəkəsi ilə məlumat mübadiləsinə və e-xidmətlər göstərməyə imkan verən çox güclü bir alətdir. Bu səbəbdən də onlar bədniyyətlilərin hədəfinə çevrilirlər. Lakin təşkilatların çoxu öz veb-saytlarının tərtibatına böyük diqqət ayırsalar da, onların təhlükəsiz fəaliyyəti ilə az maraqlanırlar.

Qeyd edək ki, korporativ şəbəkələrdə tətbiq olunan bir çox proqramlar veb-platformada hazırlanır və şəbəkənin əsas veb-proqramlar sisteminə – veb-portala qoşulur. Bu zaman yeni yazılmış proqramın şəbəkənin hər bir istifadəçisinin kompüterinə yüklənməsinə ehtiyac qalmır və bununla korporativ resurslara böyük qənaət edilir. Lakin korporativ şəbəkələrdə veb-resurslardan ibarət sistemin mürəkkəbliyi artır və onların hər hansı birinin işinin pozulması korporativ şəbəkənin fəaliyyətində böyük problemlər yarada bilər.

"Symantec" şirkətinin 2013-cü ildə təqdim etdiyi statistikaya əsasən, İnternet təhlükəsizliyi boşluqlarının sayı əvvəlki illərə nisbətən artmaqdadır [1]. Bu göstərici 2012-ci il üçün 5291 təşkil edir. 2011-ci ilə nisbətən 6% artmışdır. Qeyd edək ki, 2011-ci ildə bu göstərici 4989 təşkil etmişdir. Bu göstəricilər boşluqların əvvəlki illərə nisbətən getdikcə artacağını göstərir və 2013-cü ilin yanvar ayı üçün verilən statistika 503 təşkil etmişdir.

Veb-saytlar Ümumdünya Hörümçək Toru (World Wide Web, WWW) ilə yanaşı, 1990-cı illərin əvvəllərində meydana çıxmışdır. İlkin olaraq, hipermətnlərin vasitəsi ilə statik məlumatları özündə cəmləyən veb-saytlar günümüzədək sürətli inkişaf mərhələsi keçmiş və geniş yayılmışdır. İlk dövrlərlə müqayisədə indiki veb-saytlar öz dinamikliyi və funksionallığı ilə olduqca fərqlənir. Veb-saytların dinamik yenilənməsi, funksionallığı, günün istənilən vaxtında istənilən yerdən əlyetən olması veb-saytların informasiya təhlükəsizliyi problemlərini daha da kəskinləşdirir.

Veb-saytlarda olan boşluqların əvvəlcədən müəyyən olunması yarana biləcək bu və ya digər problemləri aradan qaldırmağa kömək edə bilər. Bunu nəzərə alaraq, bu işdə veb-saytlarda təhlükəsizlik boşluqlarının avtomatik analizi məsələlərinə baxılır, aparılmış eksperimentlərin nəticələri təhlil olunur.

II. VEB-SAYTLARDA BOŞLUQLARIN KLASSİFİKASİYASI

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

- istifadəçinin kompüteri və veb-brauzeri;
- komponentlər arasındakı əlaqə kanalları;
- veb-server;
- tətbiqi-proqramlar;
- şəbəkələrarası ekran, IDS (İntrusion Detection System), WAF(Web Application Firewall);
- yükləmənin balanslaşdırılması sistemi;
- back end (VBIS, XML, SOAP və s).

Bu komponentlərin hər hansı birində yaranan boşluqlar bədniyyətlinin veb-serverə, verilənlər bazasına daxil olmasına, qorunan məlumatların əlyetən olmasına gətirib çıxara bilər.

"Gartner" tədqiqatlarına görə veb-saytlara hücumların 75%-i infrastrukturu deyil, tətbiqi proqram səviyyəsini hədəf alır [2]. Ənənəvi perimetr təhlükəsizliyi metodları veb-tətbiqlərə qarşı hücumları dayandıra bilmir, çünki veb-tətbiqlər mahiyyətcə istifadəçilərin veb-saytlarda olan verilənlərə müraciət etməsinə xidmət edirlər. 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-təhlükəsizlik sahəsində fəaliyyət göstərən WASC (Web Application Security Consortium) və OWASP (Open Web Application Security Project) konsorsiumları tətbiqlərə xas təhdidlərin (WASC TC v. 2) və boşluqların klassifikasiyası (OWASP Top 10) sistemlərini təklif etmişlər [3, 4]. Bu iki klassifikasiya sistemi arasında istifadə edilən terminlərlə əlaqədar müəyyən ziddiyyətlər mövcuddur.

WASC klassifikatoruna görə, veb-boşluqların sinifləri aşağıdakılardır: tətbiqi proqramın səhv konfiqurasiyası; kataloqun indekslənməsi; fayl sistemində icazələrin düzgün olmaması; təhlükəli indekslənmə; yetərsiz anti-avtomatlaşdırma; yetərsiz autentifikasiya/avtorizasiya; parolun yetərsiz bərpası; sessiyanın başa çatmasın yetərsiz nəzarət, nəqliyyat səviyyəsinin yetərsiz mühafizəsi; serverin səhv konfiqurasiyası və s.

WASC klassifikatoruna görə təhdidlərə misal olaraq, aşağıdakıları göstərmək olar: funksiyalardan sui-istifadə; kobud güc; buferin daşması; kontentin spufinqi; identifikasiya məlumatlarının/sessiyanın təxmin edilməsi; xidmətdən imtina;

əməliyyat sistemi(ƏS) komandalarının icrası; SQL-inyeksiya; cross-site scripting və s.

OWASP konsorsiumunun təklif etdiyi boşluqlar klassifikatoru daha məşhurdur. Aşağıda bu klassifikasiya haqqında qısa məlumat verilir. "OWASP Top 10 - 2013 - Release Candidate" [4] siyahısına aşağıdakı 10 boşluq sinfi daxildir. Bu boşluqların qısa izahına baxaq.

A1 İnyeksiya boşluqları – SQL, ƏS və LDAP inyeksiyaları yoxlanmamış verilənlər komanda və ya sorğunun hissəsi kimi interpretatora göndərildikdə baş verir. Bədniyyətlinin ziyankar verilənləri interpretatoru arzuolunmaz komandaları yerinə yetirməyə və icazəsiz məlumatlara girməyə məcbur edə bilər.

A2 Natamam autentifikasiya və sessiyaların idarə edilməsi – tətbiqi proqramların autentifikasiyanın və sessiyaların idarə edilməsi ilə əlaqəli olan funksiyaları çox zaman düzgün realizə olunmurlar və bədniyyətliyə parolları, açarları, sessiya tokenlərini əldə etməyə imkan verirlər.

A3 Saytlararası skriptlər – XSS boşluları tətbiqi proqram yoxlanmamış verilənləri veb-brauzerə göndərdikdə baş verir. XSS bədniyyətliyə qurbanın brauzerində skriptləri yerinə yetirməyə imkan verir, bununla istifadəçi sessiyasını ələ keçirmək, veb-saytın baş səhifəsini dəyişmək və ya istifadəçiləri ziyankar saytlara yönləndirmək olar.

A4 Obyektə təhlükəli birbaşa müraciətlər – obyektə birbaşa müraciətlər proqramçı daxili realizə obyektlərinə fayl, kataloq və ya verilənlər bazası indekslərinə müraciət yerləşdirdikdə baş verir. Girişə nəzarət yoxlanması olmasa, bədniyyətli icazə verilməyən saytlara girmək üçün bu müraciətləri manipulyasiya edə bilər.

A5 Təhlükəsizliyin səhv konfiqurasiya edilməsi – yaxşı təhlükəsizlik tətbiqi proqramlar, tətbiqi proqram serverləri, ver-serverlər, verilənlər bazası serverləri və platformalar üçün təhlükəsiz konfiqurasiyanın müəyyən edilməsini və tətbiq edilməsini tələb edir.

A6 Həssas məlumatlara təsirlər – bir çox veb-tətbiqlər kredit kartları, vergi ödəyicilərinin identifikatorları kimi həssas verilənləri düzgün mühafizə etmir. Bədniyyətli belə zəif mühafizə edilmiş məlumatları oğurlaya və identifikator oğurluğu, kredit kart dələduzluğu və digər cinayətləri edə bilər. Həssas verilənlər saxlandıqda və ötürüldükdə şifrləmə kimi əlavə mühafizəyə layiqdirlər.

A7 Funksiyalar səviyyəsində girişə nəzarətin olmaması – bütün veb-tətbiqlər hər hansı funksiyanı istifadəçi interfeysində görünən etməzdən qabaq funksiya səviyyəsində giriş hüquqlarını yoxlayırlar. Lakin tətbiqi proqramların həmin giriş yoxlamalarını funksiyaya müraciət edildikdə serverdə də yoxlamalıdır. Əgər sorğular yoxlanmırsa, onda bədniyyətli sorğuları saxtalaşdıraraq funksiyalara icazəsiz giriş əldə edə bilər.

A8 Saytlararası sorğuların saxtalaşdırılması – CSRF hücumu istifadəçinin brauzerini saxta HTTP sorğularını boşluq olan tətbiqi proqrama göndərməyə məcbur edir; tətbiqi proqram sorguları həqiqi qəbul edir; sorğulara qurbanın sessiya kukiləri və avtomatik qoşulan digər autentifikasiya informasiyası daxil olur.

A9 Məlum zəif komponentlərdən istifadə – proqram təminatı kitabxanaları və modulları kimi zəif komponentlər, demək olar ki, həmişə tam imtiyaz ilə icra olunurlar. Buna görə də, onlar istismar edilsə, verilənlərin ciddi itkisinə və serverin ələ keçirilməsinə səbəb ola bilərlər. Belə zəif komponentlərdən istifadə edən tətbiqi proqramlar müdafiəni yararaq bir çox mümkün hücuma yol açа bilər.

A10 Yeni saytlara yönləndirmələrin yoxlanmaması – veb-tətbiqlər istifadəçiləri tez-tez digər səhifələrə və veb-saytlara yönləndirirlər və son ünvanları müəyyən etmək üçün yoxlanmamış verilənlərdən istifadə edirlər. Düzgün yoxlanma olmasa, bədniyyətli qurbanları fişinq və ya ziyankar proqram saytlarına yönləndirə bilər.

III. VEB-SAYTLARDA BOŞLUQLARIN ANALİZİ METODLARI

Veb-təhlükəsizliyin test edilməsi çox vacib və kritikdir, çünki bu gün e-hökumət xidmətlərinin veb-texnologiyalar 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 istismar edilir.

Veb-saytların təhlükəsizliyinin test edilməsi üçün bir sıra metodolar mövcuddur[5, 6, 7, 8].

Veb-tətbiqlərdə boşluqların test edilməsinin OWASP metodikasına görə 9 kateqoriyada birləşdirilmiş 60-dan artıq test yerinə yetirilməlidir [5]:

- 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-ın test edilməsi.

Ümumiyyətlə, proqram təminatının təhlükəsizliyinin test edilməsində nüfuzetmə testləri (ing. penetration testing), "qara qutu", "ağ qutu", fuzzing testləri, funksional testinq kimi metodlar tətbiq edilir.

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

"Ağ qutu" test metodunda veb-tətbiqin ilkin kodları analiz edilir. Statik və dinamik analiz metodlarından istifadə edilir. Statik testlərdə statik 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 daha tam hesabat verir, çünki təkcə mövcud boşluqları deyil, potensial boşluqları da aşkarlamağa imkan verir.

"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 proqram asılırsa və ya işini qəza ilə qurtarırsa, onda bu proqramda defektin tapılması deməkdir və bu müəyyən boşluğun tapılmasına gətirib çıxara bilər.

Fuzzinq testlərini avtomatik yerinə yetirmək üçün bir sıra proqram vasitələri fazzerlər 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 metodlarlaçoxsaylı 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.

IV. VEB-SAYTLARDA BOŞLUQLARIN ANALİZİ ALƏTLƏRİ

Veb-saytlarda boşluqların avtomatik analizi üzrə bir sıra proqram təminatı məhsulları mövcuddur (Acuentix WVS, Netsparker Community Edition, HP WebInspect, IBM Security AppScan və s.). Hər bir proqram təminatının veb-saytlarda boşluqların analizinə özünəməxsus yanaşmaları, üstünlükləri və nöqsanları vardır. Bu işdə Acuentix WVS (Web Vulnerability Scanner) proqram təminatı istifadə edilir.

Acuentix WVS istənilən veb-saytda boşluqları yoxlayır və XSS boşluqlarını identifikasiya edir, yaranan boşluqlar və görüləcək tədbirlər haqqında ümumi məlumat verir [7]. Acuentix WVS skaneri SOAP, XML, AJAX və JSON kimi veb-texnologiyaları anlayır, yüz minlərlə veb-səhifəni fasiləsiz və sürətlə skan etməyə imkan verir və bir sıra innovativ funksiyaları özündə cəmləyir:

- *İnnovativ AcuSensor texnologiyası* – qara qutu metodu ilə ilkin kodların (source code) daxilində yerləşdirilən əks-əlaqə sensorlarının köməyi ilə boşluqların dəqiq yoxlanılmasını həyata keçirir [8].
- *Avtomatik JavaScript analizatoru* – Ajax vəVeb 2.0 tətbiqlərinin təhlükəsizliyini test etməyə imkan verir.
- *SQL inyeksiya və XSS* (Cross Site Scripting) hücumlarını aşkarlamaq testləri yerinə yetirilir.
- *Vizual makro-yazıcı* – veb forma və parolların qorunduğu sahələri test edir.

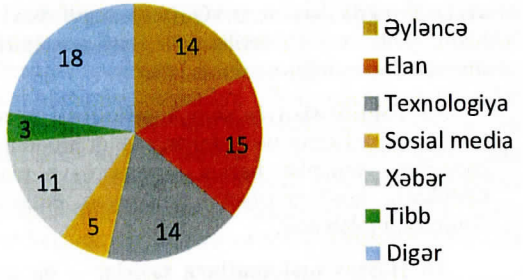
Acuentix WVS testerlərin veb-tətbiqlərdə təhükəsiz yayılması üçün özünün avtomatlaşdırılmış skanlama mexanizminə əlavə olaraq digər qabaqcıl alətlər də daxil edir:

- *HTTP Editor* – veb serverə yönələn HTTP/HTTPS sorğuları və gələn cavabları analiz edir.
- *HTTP Sniffer* – HTTP/HTTPS trafiki vasitəsi ilə göndərilən məlumatların tutulmasını və müdaxilələrin edilməsini həyata keçirir.
- *HTTP Fuzzer*–veb tətbiqlərin, daxil olan məlumatların, gözlənilməyən və həqiqi olmayan istənilən faylın fuzzing testləri vasitəsilə yoxlanmasını həyata keçirir. Əllə edilən və günlər alan yoxlamaları protokolun köməyi ilə bir neçə dəqiqəyə etmək mümkündür.
- *Blind SQL injection* – avtomatlaşdırılmış verilənlər bazasına müdaxilələr etmək üçünalətdir.

Acunetix WVS skanerinin işinin nəticəsində müxtəlif təfsilatlı hesabatlar (rəhbərlik üçün qısa hesabat, mühəndislər üçün boşluqlar haqqında ətraflı texniki hesabat, əvvəlki testin nəticələri ilə müqayisə hesabatı və s.) formalaşdırılır, boşluqların aradan qaldırılması üçün tövsiyələr və İnternetdə müvafiq resurslara linklər verilir.

V. EKSPERİMENTLƏRİN TƏŞKİLİ VƏ NƏTİCƏLƏRİN ANALİZİ

Veb-saytlarda boşluqların avtomatik analizi aparılmışdır. Təqdim olunan işdə Acuentix WVS proqram təminatından istifadə edilməklə eksperimentləraparılmışdır. Əyləncə, texnologiya, tibb, xəbər, sosial media, elan və s. saytları olmaqla 80 sayt analiz edilmişdir. Saytların qruplar üzrə sayı şəkil 1-də göstərilib. Saytların yoxlanılmasına orta hesabla 1-5 saat tələb edilir.



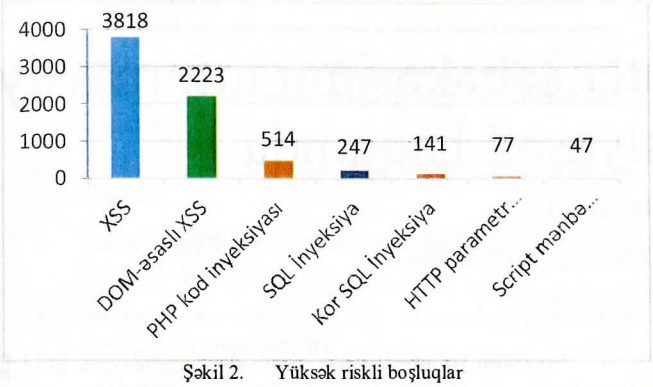
Şəkil 1. Qruplar üzrə paylanma

Acuentix WVS aşkarlanmış boşluqları yüksək (High), orta (Medium), aşağı (low) və məlumat xarakterli risk qruplarına bölür. Aşkarlanmış boşluqların paylanması cədvəl 1-də göstərilmişdir.

CƏDVƏL 1. BOŞLUQLARIN PAYLANMASI

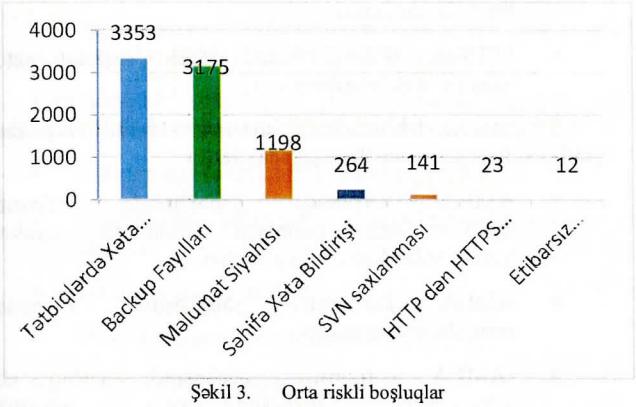
Risk dərəcəsi	**Boşluqların sayı**
Yüksək	7081
Orta	8214
Aşağı	4716
Məlumat	41819

80 veb-saytda 7081 yüksək riskli boşluqlar aşkarlanmışdır. Belə boşluqlar daXSS (3818), DOM-əsasında XSS (2223), PHP-kod inyeksiyası (514), SQL Inyeksiyası (247) və s.üstünlük təşkil edir. Yüksək riskli boşluqların paylanması top 7 olaraq şəkil 2-də göstərilmişdir.



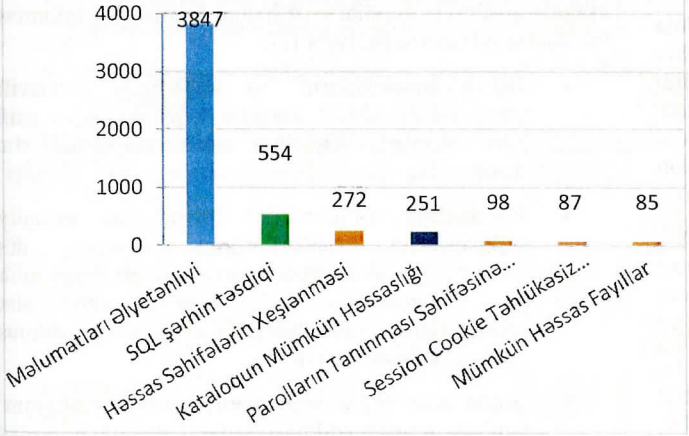
Şəkil 2. Yüksək riskli boşluqlar

Orta risk boşluqlarında tətbiqlərdə xəta bildirişi (3353), Backup faylları (3175), Məlumat Siyahısı (1198), Səhifə Xəta Bildirişi (264) və s. boşluqlarüstünlük təşkil edir. 8214 orta riskli boşluqlar aşkarlanmışdır. Orta riskli boşluqların paylanması top 7 olaraq şəkil 3-də göstərilmişdir.



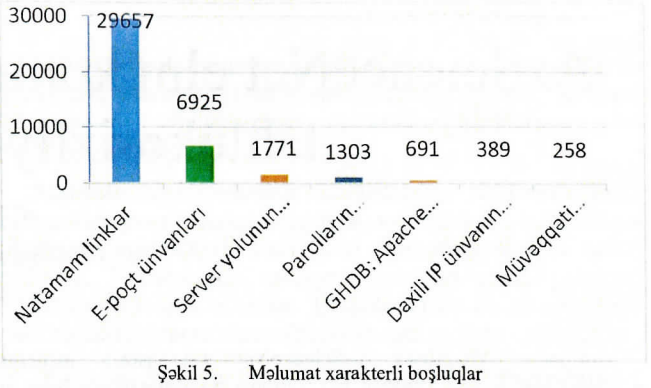
Şəkil 3. Orta riskli boşluqlar

Aşağı risk boşluqlarında istifadəçi məlumatları əlyetənliyi (3353), SQL şərhin təsdiqi (3175), həssas səhifələrin keşlənməsi (1198), kataloqun mümkün həssaslığı (264) və s. boşluqlarüstünlük təşkil edir. 4716 orta riskli boşluqlar aşkarlanmışdır. Aşağı riskli boşluqların paylanması top 7 olaraq şəkil 4-də göstərilmişdir.



Şəkil 4. Orta riskli boşluqlar

Məlumat xarakterli risk boşluqlarında natamam linklər (29657), e-poçt ünvanları (6925), server yolunun açıqlanması (1771), parolların avtomatik tamamlanması (1303) və s. boşluqlar üstünlük təşkil edir. Məlumat xarakterli boşluqların paylanması top 7 olaraq şəkil 5-də göstərilmişdir.



Şəkil 5. Məlumat xarakterli boşluqlar

NƏTİCƏ

Veb-saytların interaktivlik, tranzaksiyaları yerinə yetirmək imkanları artdıqca, onlara müraciət edilə bilən qurğuların dairəsi genişləndikcə, veb-saytların təhlükəsizliyinin etibarlı təmin edilməsi məsələsi daha da aktuallaşır.

Bu işdə Acuentix WVS proqram təminatının köməyi ilə avtomatlaşdırılmış üsulla veb-saytlarda təhlükəsizlik boşluqlarının qiymətləndirilməsi üzrə eksperimentlər aparılıb və nəticələr analiz olunub. Texnologiya, elan, əyləncə və s. olmaqla 80 veb-sayt analiz olunub və 61830 boşluq aşkar edilib. Aşkarlanmış boşluqlar yüksək, orta, aşağı və məlumat xarakterli olaraq qiymətləndirilir, boşluqların bu siniflər üzrə paylanması təhlil olunub.

ƏDƏBİYYAT

[1] Symantec Inc. Symantec Internet Security Threat Report: Vol. 18. Technical report, Symantec Inc., April 2013

[2] Business Justification for Application SecurityAssessment https://www.owasp.org/index.php/Business_Justification_for_Application_Security_Assessment

[3] WASC: The WASC Threat Classification: http://projects.webappsec.org/w/page/13246978/Threat%20Classification

[4] OWASP: OWASP Top 10 - 2013 - Release Candidate http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013%20-%20RC1.pdf

[5] OWASP: OWASP Testing Guide v3. 2008, 349 p. https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

[6] D. Stuttard, M. Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2nd Edition," 2011, 912 p.

[7] Marco, F. Victoria, V. Giovanni, "Vulnerability Analysis of Web-Based Applications," *Testing and Analysis of Web Services (eds. L. Baresi and E. Dinitto)*, pp. 363-393, 2007.

[8] M.Sutton, A.Greene, P. Amini, "Fuzzing: Brute Force Vulnerability Discovery," Addison-Wesley Professional, 2007. – 576 p.

[9] Acunetix: Acunetix web vulnerability scanner. http://www.acunetix.com/vulnerabilityscanner/

[10] Acunetix: AcuSensor technology http://www.acunetix.com/vulnerability-scanner/acusensor.htm