SELÇUK ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ

S.Ü. Müh. Bilim ve Tekn. Derg., c.6, s.4, ss. 753-766, 2018
Selcuk Univ. J. Eng. Sci. Tech., v.6, n.4, pp. 753-766, 2018
ISSN: 2147-9364 (Electronic)
DOI: 10.15317/Scitech.2018.165

EVALUATION OF MOST VISITED WEB SITES IN TURKEY IN ASPECTS OF STRUCTURE AND SECURITY

[1]Atakan DAŞDEMİR, [2]Mustafa Nevzat ÖRNEK, [3]Humar Kahramanlı ÖRNEK

[1]Selçuk University Graduate School of Natural Sciences Information Technology Engineering, MS Student, Konya, TÜRKİYE
[2]Konya Technical University, Vocational School of Technical Sciences, Konya, TÜRKİYE
[3]Selçuk University, Faculty of Technology Computer Engineering Department, Konya, TÜRKİYE
[1]ataknet@gmail.com, [2]nevzat@selcuk.edu.tr, [3]hkahramanli@selcuk.edu.tr

(Geliş/Received: 25.08.2017; Kabul/Accepted in Revised Form: 09.04.2018)

ABSTRACT: Applications on World Wide Web have made our daily lives easier with their basic and fast access, neglecting time and place, they have become indispensable. It made Web applications a popular target for malevolent users and increased web security risk. In this study web penetration test which is indispensable for web security and threating risks for web security are mentioned. In Turkey, 60 of the most visited sites were identified in five different categories scanned as an ordinary user to consider a safety assessment of the general situation of the websites. For the review, large sites in news sites, e-commerce, government, universities and other categories have been selected that are thought to have strong security infrastructure. The knowledge about these sites such as used technologies and infrastructure which considers as vulnerability of sites and can be obtained by the ordinal person who uses penetration tests has been investigated in this study. As a result of the research, operating system information and web server information from 62% and 87% of the reviewed sites were identified respectively. Medium and low degree vulnerabilities were found in all scanned websites. With the vulnerability screening tests, weakness map revealed and information about the most identified weaknesses was given.
Key Words: *Penetration tests, Weakness analysis, Web security*

Türkiye'de En Çok Ziyaret Edilen Web Sitelerinin Altyapı ve Güvenlik Açısından Değerlendirilmesi

ÖZ: Dünya Çapında Ağ (www) üzerindeki uygulamalar yere ve zamana bağlı olmadan hızlı erişimi ile günlük hayatımızı kolaylaştırdı ve vazgeçilmez oldu. Bu da web uygulamalarını kötü niyetli kullanıcılar için hedef haline getirdi ve web güvenliği riskini yükseltti. Bu çalışmada web güvenliği ve tehdit riskine karşı kaçınılmaz olan sızma testleri incelenmiştir. Türkiye'de, beş farklı kategorideki 60 en çok ziyaret edilen site belirlenmiş ve güvenlik açısından değerlendirmek amacı ile sıradan bir kullanıcı olarak incelenmiştir. İnceleme için ciddi güvenlik altyapısı olduğu düşünülen haber, e-ticaret, devlet, üniversite ve diğer kategorilerde büyük siteler seçilmiştir. Bu çalışmada sızma testi kullanan sıradan bir kullanıcı tarafından elde edilebilen sitelerde kullanılan teknolojiler ve sitelerin güvenlik açığı olarak kabul edilen altyapı gibi bilgiler incelenmiştir. Çalışmanın sonucu olarak incelenen sitelerin %62'sinde kullanılan işletim sistemi ve %87'sinde kullanılan web sunucu bilgileri belirlenmiştir. İncelenen tüm sitelerde orta ve düşük seviye zafiyet tespit edilmiştir. Zafiyet tarama testi ile zafiyet haritası oluşturulmuş ve en çok karşılaşılan zafiyetlerle ilgili bilgi verilmiştir.

Anahtar Kelimeler: *Sızma testi, Zafiyet analizleri, Web güvenliği*

INTRODUCTION

In this information age we are living in, information is important surely, however its secrecy, integrity and accessibility as in "Information Security" is important as well. Information security is efforts to create a safe information processing platform to protect information or data in electronic environment from unauthorized accesses while saving and transporting without disrupting its integrity (Canbek and Sagiroglu, 2006).

There are various difficulties with providing information security due to the transformation of managerial needs related to information security into a methodology, improper configuration of network security devices, avoiding security by considering time and cost in projects, the lack of knowledge about information security of institution employees (Boşal, 2017).

We can subcategorize information security as network security, end-user security, data security, application (web) security, identity and access security, security management (Çetinkaya, 2008).

Internet and web security gain importance day by day because of millions of users and being existed in the all areas of life from finance to health, from communication to entertainment. Internet has become indispensable part of our daily lives by providing unprecedented convenience via web and mobile applications (Fung, 2014).

Since web applications are open to all including hackers, because of their definition, security of these applications is troublesome (Khochare et al., 2013).

The Symantec Company (Symantec, 2016) has found at least one weakness in 76% of the sites reviewed in its internationally conducted Web security analysis study. This result is sufficient to demonstrate the seriousness of the situation in the security of web applications. In this study, 60 of the most visited sites were identified in five different categories to consider a safety assessment of the general situation of the Web sites in our country. We aimed to show what kind of information and what vulnerabilities can be found by the ordinary internet user Web penetration tests indispensable for evaluation of web sites in aspects of security. The web penetration tests scan weakness of web sites and give opportunities to take precautions for vulnerabilities (Barbara, 2014).

Doğan (2013) has scrutinized 193 studies about web penetration tests published between 2000 and 2013 and provided information about test approaches, error models, tools, metrics and experimental evidences. One of them was developed by Haque (2016) for web server vulnerability analysis in he context of transport layer security (TLS). Web penetration tests detect vulnerabilities using different attack types. Among these types injections and XSS are very common.

Ruse (2013) has handled injection and XSS attack techniques which are among the most common attack types and protection methods in details and mentioned detection methods.

Jnena (2013) compared a tool which he created himself concerning SQL injection and XSS with other tools in his study about web applications weakness analysis. Huang et al. (2016) analyzed the current situation of Chinese websites sing 57,122 web spoofing events from 2012 to 2015 presented by researchers. According to the authors, the data were collected in four groups including companies listed in the stock exchange, government agencies, educational institutions and new companies. They have created an automatic classifier model for web security vulnerabilities and examined the most common 15 security vulnerabilities and their distribution. In 2015, the number of SQL injections 5,742 (44.87%), XSS 283 (2.21%), Logic error 202 (1.58%), Sensitive data exposure 1,403 (10.96%), Broken access control 515 (4.02%) Command injection 564 (4.41%), Misconfiguration 354 (2.77%), Hack event 1,734 (13.55%), Weak password 733 (5.73%), File upload 117 (0.91%), Path traversal 64 (0.5%), Invalidated redirects 34 (0.27%), CSRF 16 (0.13%), File include 111 (0.87%), Other 924 (7.22%).

They reported that the startup companies had serious security vulnerabilities while government and educational institutions showed more interest to this area.

Yalçınkaya (2012) has made an analysis study on Turkey's 50 public institutions' web site with the basis of web standards broadcasted by Türksat Company. Arsoy (2014) has evaluated e-state web sites according to convenience to international standards and concluded that they have general usability problems. Reducing web security threats is another subject of web security study (Hassan, 2013). It is

important for web security to detect most common attack types and approach different techniques to lower the menaces of web security.

One of the most comprehensive studies about web security is The Open Web Application Security Project (OWASP) founded in 2001 and presents free tools, standards and forms etc. and relevant services to increase application security and awareness. The common threats against web applications are broadcasted up-to-date as top 10 lists by OWASP. OWASP 2017 Top 10 list is below (OWASP, 2017):

1- SQL, OS, XXE and LDAP injection
2- False Identity Authentication and Login Management
3- Cross-Site Scripting (XSS)
4- False Access Control
5- False Security Configuration
6- Obtaining Valuable Information
7- Insufficient Attack Prevention
8- Cross-Site Request Forgery (CSRF)
9- Using Components with Known Security Breaches
10- Defenseless APIs

In this study, determined web sites were scanned using web penetration test methods via statistical sites and open source programs and some information were collected about the technologies and infrastructure they use.

MATERIAL AND METHOD

Penetration tests are the so critical for evaluation of web sites in aspects of structure and security. Thus this study explains penetration test methods and using them.

Penetration Tests in Web Applications Security

Penetration tests are test group which procures the mischiefs beforehand to information technologies infrastructure and institution's data flow by an attacker (Hacker, former employee, Script Kiddie etc.) or malware (worm, virus, Trojan horse, spyware etc.) (Muharremoğlu, 2013). Web security penetration tests and the methods used are shown in Table 1.

The purpose of the penetration tests is determining the weaknesses and eliminates them to prevent malevolent people's unauthorized access (Vural, 2007). Method example used also in Web penetration tests is shown below in Figure 1.

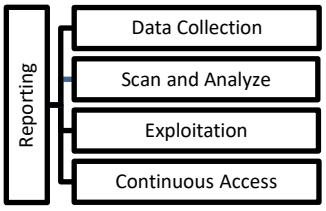

Figure 1. Method used in penetration tests

Table 1. Security test used in penetration tests (Yaşar, 2014).

PENETRATION TESTS	METHODS
Authentication	Brute Force Insufficient Authentication Password Saving Control
Authorization	Guessing Login Info Insufficient Authorization Insufficient Logout Login stabilizing
User based	Cross-site scripting
	Content Forgery
Command Executing	Buffer overflow Typesetting Format LD Injection Operating System Command Injection SQL Injection SSI Injection XPath Injection
Information Exposal	Index listing Information Leak Following Conjecturable Source Location
Logical	Functionality Malfeasance Service Damp Automation Insufficient Supervising

Penetration tests consists of 5 phases as data collection, weakness scan and analyze, exploitation, continuous access and reporting.

a. Data Collection: Data collection can be divided into two as active and passive. Collecting via connection to the source is called active (Fierce, Dig, theHarvester, SubBrute, CeWL like softwares) and collecting without connection to the source, via internet and web sites (Shodan, Google Hack Database, Netcraft like sites) is called passive. Whereas active data collection has the advantage of more and effective data collection, it has the disadvantage of possibility of being detected by the source. The reason for data collection can be summarized as collecting information and finding documents via determining running system and software, IP address, determining running services, social engineering (Muniz and Lakhani, 2015). From the web perspective, collected data like used web host applications and versions, http version, http method, index structure, folder types, used Web Application Firewall and proxy server will be very useful on test stage.

b. Vulnerability Scan and Analysis: Errors or lacks which can be used for exploiting are found with the help of gathered information, then open ports are determined. Patch deficiency of operating system or any program used, is the most important weakness for a system (Polat, 2016). Simple or default password usage, faulty system politics, problems sourced from design of the application or software, gaining applications or software free, can be exemplified as potential menaces which can direct weaknesses. Weakness scan for web applications can be manual (Code examination, command line etc.) or can be done via popular automatic weakness scan tools (Metaspolit, nmap commands, Nessus, Acunetix etc.)

c. Exploitation: Exploitation is the most important stage of the process where control over target system is established. Instead of weakness scan tools, here exploitation oriented tools (password cracking programs, Metasploit application etc.) and exploit named exploitation commands are used. Websites like *https://www.exploit-db.com* which includes exploitation codes to use potential weakness for exploitation purposes, can be collimator. Exploitation is using errors of programs installed in target system by providing the attacker infiltration to the target and executing malicious code in there (Engebretson, 2013).

d. Continuous Access: This is the stage where after accessing the target, erasing the trails as much as possible and having continuous multi-pronged access with methods like backdoors, rootkits, new user or meterpreter shell, tunnel, new network access channel.

e. Reporting: Documents include solutions and suggestions where the data obtained via tests done in previous stages are exegetically written, the test results are analyzed (risk levels, effects on system, order of importance etc.), can be generated at "Reporting" stage (Vural, 2017).

In the study information gathering from penetration tests methods, weakness scanning and analyzing operation steps were taken as basis. Followed method is shown in Figure 2.

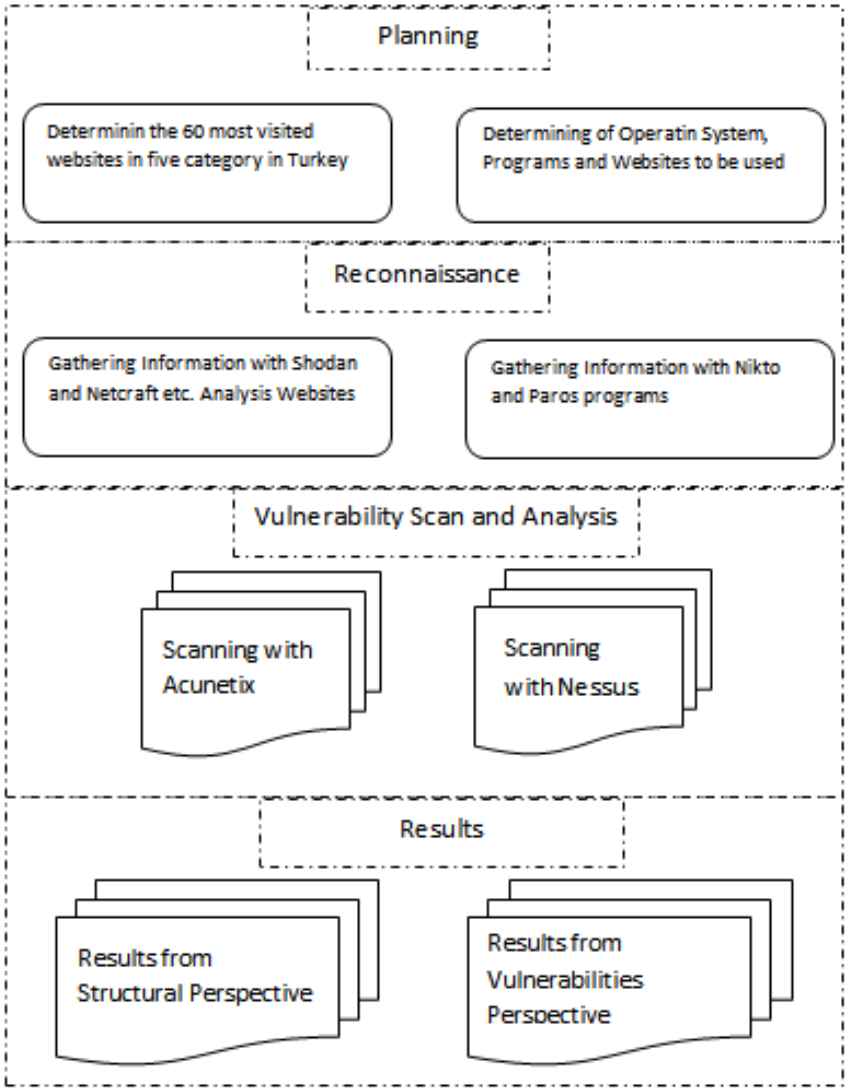

Figure 2. Method followed

For working material from most visited sites as five different groups and for each group 12 sites in university, news, e-commerce, government and other categories are determined based on *https://ww.alexa.com* website statistics. Examined news websites are named as "Group-1", e-commerce websites are named as "Group-2" government websites are named as "Group-3", university websites are named as "Group-4" and the other websites are named as "Group-5". As university group state universities have been examined whereas in news e-commerce and other group websites private websites are examined. Others group includes private websites in different categories like portal, entertainment.

In the process Kali Linux and Microsoft Windows 8 operating systems are used. In order to gather information about websites, Shodan and Netcraft analysis websites and open source coded Nikto and Paros applications under Kali Linux were used. For weakness scan popular Acunetix v10 (*https://www.acunetix. com* trial version) program which works on Microsoft Windows platform and Nessus program's trial version 6.10.5 (*https://www.tenable.com*) were used.

In the study information gathering from penetration tests methods, weakness scanning and analyzing operation steps were taken as basis. Followed method is shown in Fig 2.
In the light of followed method; first determined websites' information about infrastructure and technology is gathered and then comparisons were made via weakness scan.

a. Information to be gathered from the perspective of structure and technology they use are shown in Table 2.

Table 2. Gathering information

Information to be collected about the websites	
1.	Host's operating system for determined websites
2.	Their choosing as web server
3.	The platform they work on
4.	Security equipment used
5.	Web Tracers

In order to gather and evaluate the information about websites, firstly determined websites were scanned at Shodan and Netcraft websites which are analysis websites. Then necessary information about websites were gathered using Niktos and Paros applications which are information gathering purposed scanner programs in Kali Linux.
According to the method followed; second step is vulnerability scan.

b. Determined websites are scanned first with Acunetix program and then with commercial Nessus programs trail version for weakness detection and found weaknesses' detailing.

Information to be gathered for vulnerability analysis:
- Weakness level of websites,
- On which category which weaknesses are encountered,
- Weakness evaluation.

RESULTS AND SUGGESTIONS

Information about websites analyzed, gathered in the perspective of structure and technology they use and information gathered in the perspective of weakness analysis are tested for each three groups individually. Results below are obtained at the end of the studies:

Structural Results

The information of operating system used, web host software, platform they work on, Security equipment they used, location and web trackers in the 60 websites which are chosen from the Turkey's top visited websites, is below in Tables 3, 4, 5, 6, and 7. It is the known fact that finding out the operating system used in server and web server software can be helpful to information gathering which is the first step of attack. Thus, Web Application Firewall (WAF) software hinders the information gathering procedures called footprint. Hence, no information was gathered about some websites' operating system and web hosts.

Table 3. Operating systems of hosts

	Win 2003	Win 2008	Win 2012	Linux	Undetected
Group-1	-	2	-	7	3
Group-2	1	4	-	3	4
Group-3	-	-	1	2	9
Group-4	-	1	1	8	2
Group-5	-	3	1	3	5
Total	**1**	**10**	**3**	**23**	**23**

As seen on Table 3 web server use Linux as operating system with the percentage of 62, and it has been preferred by universities the most as 67%. There has been a website detected which is using Windows 2003 server on which Microsoft has no support since July 14, 2015 and it will not have security patch anymore.

Table 4. Web servers of websites

	IIS 7.0	IIS 7.5	IIS 8.5	Nginx	Apache	PWS	Undetected
Group-1	-	2	1	4	-	5	-
Group-2	-	3	2	2	2	-	3
Group-3	-	2	2	3	1	-	4
Group-4	1	-	2	3	5	-	1
Group-5	-	2	3	5	1	1	-
Total	**1**	**9**	**10**	**17**	**9**	**6**	**8**

As seen on Table 4 the percentage of IIS (last version 10.0) choosers as web host software is 33% and all of them are using old version. When websites provides exploit support scanned, exploit codes (like overriding the authorization) were detected especially on IIS 7.5 and older versions. On examined websites it has been seen that web host Nginx (latest version 1.13) software has being used with 28%. The older versions of Nginx software could be reason to some weaknesses like remote exploit. There also has been some websites using PWS software with 10%.

Table 5. Working platforms

	.net	PHP	Undetected
Group-1	3	9	-
Group-2	7	4	1
Group-3	8	3	1
Group-4	3	8	1
Group-5	6	6	-
Total	**27**	**30**	**3**

According to Table 5, PHP is the most using platform with 50%. Especially it has been preferred by websites of news and university.

Table 6. Security equipment

	F5 BigIp	Citrix Netscaler	Undetected
Group-1	2	2	8
Group-2	2	2	8
Group-3	6	3	3
Group-4	-	3	9
Group-5	2	4	6
Total	**12**	**14**	**34**

As shown as Table 6, 26 (43%) websites uses security equipment. It has been seen that 14 websites uses Citrix Netascaler and 12 websites uses F5 BIGIP network product devices as WAF which can distribute traffic between the determined hosts as distributer and is a protector against especially injection and XSS attacks.

Table 7. Web trackers

	Analysis	CDN	Widget	Ad
Group -1	12	7	11	8
Group -2	10	7	3	12
Group -3	4	4	3	-
Group -4	4	8	1	-
Group -5	10	8	7	5
Total	**40**	**34**	**25**	**25**

Web tracker which share demographic information, buying habits, area of interests and more information with third parties, implementation is 22% at university websites whereas the all the other websites are using them and they are used for statistic/analysis, CDN (Content Distribution Network), widget and advertising. Websites are most using analysis web trackers with 67%.

Results from Weaknesses Perspective

Acunetix and Nessus programs find vulnerabilities in four level categories. These categories are high, medium, low and information. Information level can be ignored. While high level is critical and must be taken prevent immediately. In this study determined Websites were scanned in the computer laboratory by Acunetix and Nessus programs on 14th, 15th and 16th June 2017.

a. Evaluation of the scan results with Acunetix:

A total of 60 websites, each of which lasted an hour, were scanned with Acunetix program. Degrees of vulnerability information found in the results of scanning with the Acunetix program are shown in Table 8.

As shown in Table 8, no site has high risk vulnerability. Medium vulnerability is found most in the Group-5. Low-grade vulnerability quantities are found in close proximity to each other on groups. It is detected that all the websites have weaknesses when we examine Table 8. All found vulnerabilities are detailed in Table 9.

Table 8. Degrees of vulnerabilities found by Acunetix v10

	Low	Medium	High
Group -1	23	17	-
Group -2	31	9	-
Group -3	17	8	-
Group -4	21	13	-
Group -5	14	24	-
Total	**106**	**71**	**0**

Table 9. Acunetix v10 results

	Risk Degree	ACUNETIX Vulnerability	Q
Group-1	High	-	0
	Medium	·HTML Form Without CSRF Protection ·Insecure crossdomain.xml file ·User Credentialsare Sent in ClearText ·elmah.axd Information Discloser ·Slow HTTP Denial of Service Attack	11 2 2 1 1
	Low	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Option Method is Enabled ·ASP.NET version Discloser ·Possible virtual host found	9 6 3 2 3
Group-2	High	-	0
	Medium	·HTML Form Without CSRF Protection ·ASP.NET error message ·HTTPS Connection with weak key length	6 1 2
	Low	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Option Method is Enabled ·ASP.NET version Discloser ·Possible virtualhost found	10 10 6 4 1
Group-3	High	-	0
	Medium	·HTML Form Without CSRF Protection ·Slow HTTP Denial of Service Attack	6 2
	Low	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Sesion cookies coped to parent domain ·Login page password-guessing attack ·Possible virtual host found	9 3 1 1 2 1

		·File Upload	
Group-4	High	-	0
	Medium	·HTML Form Without CSRF Protection ·Insecure crossdomain.xml file ·Slow HTTP Denial of Service Attack ·Same site scripting ·ASP.NET error message ·User Credentialsare Sent in ClearText ·Apache httpOnly cookie disclosure	5 1 3 1 1 1 1
	Low	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Possible sensitive directories ·ASP.NET version Discloser ·Option Method is Enabled ·File Upload ·Trace Method is Enabled	10 5 1 1 2 1 1
Group-5	High	-	0
	Medium	·HTML Form Without CSRF Protection ·User Credentialsare Sent in ClearText ·Insecure crossdomain.xml file ·Same Site Scripting	8 2 3 1
	Low	·Clickjacking:X-Frame-Option Header Missing ·Cookie Without HttpOnly Flag Set ·Option Method is Enabled ·Possible virtual host found ·Sesion cookies coped to parent domain ·File Upload ·Trace Method is Enabled ·ASP.NET version Discloser	10 5 2 2 1 2 1 1

Acording to Acunetix scanning;

- No high level thread has been detected in all groups.
- At medium level "*HTML From without CSRF Protection*" weakness which can cause CSRF exploit especially in forms, is highest at 92% in Group-1 and almost 50% in the other groups. To get rid of this weakness CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) or "I am not a robot" usage along with CSRF token usage might be the most secure solution.
- At low level when Table 9 is scrutinized, we can see that 76% of the all risks are generated from usage of "Header, Cookie, and Method" and using "*Same-Origin*" method is the most common way to prevent these weaknesses. Missing of "*Clickjacking: X-Frame-Option Header Missing*" which causes unwanted direction sourced by usage of Iframe/frame, is at 80% at all groups.

b. Evaluation of the scan results with Nessus:

Determined websites were scanned with Nessus program. Each of them lasted an hour. Degrees of

vulnerability information found in the results of scanning with the Nessus program are shown in Table 10.

Table 10. Degrees of vulnerabilities found by Nessus v6.10.5

	Low	Medium	High
Group -1	3	26	1
Group -2	2	10	-
Group -3	1	12	-
Group -4	1	13	2
Group -5	3	27	-
Total	**10**	**88**	**3**

As shown in Table 10, two university sites and one news site have high risk vulnerability. Medium vulnerability is found most in the Group-5 and Group-1.

Table 11. Nessus v6.10.5 Results

	Risk Degree	NESSUS	
		Vulnerability	Q
Group-1	High	·PHP 7.0.x < 7.0.12 Multiple Vulnerabilities	1
	Medium	·Web Application Potentially Vulnerable to Clickjacking	10
		·.bash_history Files Disclosed via Web Server	1
		·PHP expose_php Information Disclosure	1
		·CGI Generic XSS	5
		·CGI Generic HTML Injections	5
		CGI Generic Cookie Injection Scripting	3
		IIS Detailed Error Information Disclosure	1
	Low	Web Server Transmits Cleartext Credentials	2
		Web Server PROPFIND Method Internal IP Disclosure	1
Group-2	High		-
	Medium	Web Application Potentially Vulnerable to Clickjacking	8
		·CGI Generic HTML Injections	1
		·CGI Generic XSS	1
	Low	Web Server HTTP Header Internal IP Disclosure	2
		·Web Server Transmits Cleartext Credentials	1
Group-3	High		-
	Medium	Web Application Potentially Vulnerable to Clickjacking	8
		CGI Generic XSS	1
		PHP expose_PHP Information Disclosure	1
		WordPress User Enumeration	1
		ASP.NET DEBUG Method Enabled	1
	Low	Web Server Transmits Cleartext Credentials	1

Group-4	High	PHP 7.0.x < 7.0.16 Multiple Vulnerabilities	1
		PHP Unsupported Version Detection	1
	Medium	Web Application Potentially Vulnerable to Clickjacking	6
		PHP expose_PHP Information Disclosure	1
		Git Repository Served by Web Server	1
		HTTP TRACE / TRACK Methods Allowed	1
		PHP expose_PHP Information Disclosure	1
		ASP.NET DEBUG Method Enabled	1
		CGI Generic XSS	1
		CGI Generic HTML Injections	1
	Low	·Web Server Transmits Cleartext Credentials	1
Group-5	High		-
	Medium	Web App. Potentially Vulnerable - Clickjacking	7
		CGI Generic XSS	5
		CGI Generic Path Traversal	2
		ASP.NET DEBUG Method Enabled	1
		PHP expose PHP Information Disclosure	1
		CGI Generic HTML Injections	5
		CGI Generic Cookie Injection Scripting	1
		Backup Files Disclosure	1
		HTTP TRACE / TRACK Methods Allowed	2
		PHP expose PHPPHP Information Disclosure	2
	Low	·Web Server HTTP Header Internal IP Disclosure	1
		·Web Server Transmits Cleartext Credentials	2

Low-grade vulnerability quantities are found in close proximity to each other on groups. According to Nessus program all the websites have weaknesses. Vulnerability details are shown in Table 11

There has been a critic level weakness detected because of PHP version being old which is used in Group-1 and Group-4

- As an average level weakness, "*Web Application Potentially Vulnerable to Clickjacking*" weakness which is seen as low level threat and causes unwanted directions, is seen in Group-1 with 83 % and in Group-2 and Group-3 websites with 67% .
- "*Web Server Transmits Cleartext* Credentials" weakness which is sending low level user information without cryptography, is seen all groups and total of 8 sites.
- "*Header, Cookie, Method*" usage sourced low level weakness which were found by Acunetix program, are given as information in Nessus program instead of thread.

Suggestions

This research generates a template for Turkey's top visited websites both in the perspective of technology they use and in the perspective of their weaknesses, and sets and example to see structure and deficiencies. It has been shown what kind of information can be collected on a public website and what kind of vulnerability scanning can be done by an ordinary user.

Web applications constitute the great part of security flaws since they are both open to public and they are time and place independent. This study shows that the most of visited web sites in Turkey has considerable number of vulnerabilities. Especially average level weaknesses cannot be ignored.

As a result of the study:

- Unix or Unix derivative operating system is the most prefer with 38%.
- As the web server, 28% is preferred to nginx software.
- When it comes to the platform used PHP is the most preferred with 50%.
- Determined websites are using security equipment with 43%.
- Within the first Alexa 500 companies have security departments.
- At the end of the Acunetix software scans "HTML From without CSRF Protection" is the most common weakness in medium level risks with %60.
- According to Acunetix program "Clickjacking: X-Frame-Option Header Missing" is the most common weakness in low level risks with %80.
- According to Nessus program "Web Application Potentially Vulnerable to Clickjacking" is the most common weakness in medium level risks with %65 are founded.
- For the considerable number of vulnerabilities, web applications should be tested for penetration in determined periods to determine possible attacks or threats beforehand, to see deficiencies and take precautions against them.
- The most visited sites are used firewall which is managed by specialists. There are small amount of vulnerability in such sites and the information that can be available by hackers is less than the sites without firewall.
- The reason for the inadequacy of security of universities and government corporations are the frequently relocation or leave of employment of information processing staff.
- The reason for the differences in the security of the group is a result of the different business policies.
- People with low knowledge-level websites are increasing their weaknesses.
- Using ready codes increases weaknesses.
- In examined websites, using up-to-date software issue must be concerned since it is the reason they have high level risky weaknesses.
- It has been determined that collecting information from sites which uses WAF is difficult. Using of WAF is recommended to avoid gathering the information required for attackers.
- To check websites against weaknesses of OSWAP Top 10 list manually or with a program is necessary to have precautions against common weaknesses.
- Group-1 websites should take precautions against information gathering which is the first step of attacks.
- Weaknesses sourced by using "Header, Cookie, and Method" is common in all groups and precautions should be taken against them.
- Against the CSRF exploit threat which is seen in Group-2 and Group-3 as high as 80%, CAPTCHA usage or 'I am not a robot' using is suggested.

REFERENCES

Anonymous, 2016, https://www.symantec.com/content/dam/ symantec /docs/reports/istr-21-2016-en.pdf, 2016.

Anonymous, 2017, https://www.owasp.org/index.php/Top_ 10_2017-Top_10,

Arsoy, S., 2014, "e-Devlet Web Sitelerinin Kullanılabilirlik Yönünden Standartlara ve Rehberlere Göre Değerlendirilmesi," M.S. thesis, Fen Bilimleri Enstitüsü, Yıldız Teknik Üniversitesi, İstanbul

Barbara, S., 2014, *Advanced Automated Web Application Vulnerability Analysis,* Ph.D. Dissertation, University of California.

Boşal, S., 2017, *Kamuda Bilgi Güvenliği ve Iller Bankasi A.Ş. Örneği*, Uzmanlık Tezi, İller Bankasi Anonim Şirketi Ankara.

Canbek, G., Sağıroğlu Ş., 2006, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme," *Politeknik Dergisi*, Vol 9(3), pp. 165-174.

Çetinkaya, M., 2008, *Bilgi Güvenliği Yönetim Sistemi Altyapisinin Değerlendirilmesi Için Bir Test Araci Geliştirilmesi*, M.S. Thesis, İstanbul Kültür Üniversitesi, İstanbul.

Doğan, S., 2013, *Web Application Testing: A Systematic Literature Review*, M.S. Thesis, The Middle East Technical University, Ankara.

Engebretson, P., 2013, *The Basics of Hacking and Penetration Testin*g, Second Edition, Elsevier Inc Syngress, Waltham,

Fung, P.H.A., 2014, Mitigations *of Web Application Security Risks*, Ph.D. Dissertation, Information Engineering The Chinese University, Hong Kong

Haque, S., 2016, Web Server Vulnerability Analysis in the Context of Transport Layer Security (TLS)", *IJCSI International Journal of Computer Science Issues*, Vol.13(5), pp.11-19.

Hassan, M., 2013, *Toward Automated Dıscovery of Web Application Security Vulnerabilities*, M.S. Thesis, California State University, California.

Huang, C., Liu, J.Y, Fang, Y., Zuo, Z., 2016, "A Study on Web Security Incidents in China by Analyzing Vulnerability Disclosure Platforms, *Computers & Security*, Vol.58 (May), pp. 47-62.

Jnena, R., 2013, *Modern Approach for WEB Applications Vulnerability Analysis*, M.S. Thesis, The Islamic University of Gaza, Gaza.

Khochare, N., Chalurkar, S., Meshram, B.B., 2013, "Web Application Vulnerabilities Detection Techniques Survey," *IJCSNS International Journal of Computer Science and Network Security*, Vol.13(6)6, pp. 71-77.

Muharremoğlu, G., 2013, *Kurumsal Bilgi Güvenliğinde Zafiyet, Saldırı ve Savunma Öğelerinin İncelenmesi*, M.S. Thesis, Fen Bilimleri Enstitüsü İstanbul Üniversitesi, İstanbul.

Muniz, J., Lakhani, A., 2015, *Web Penetration Testing with Kali Linux*, Packt Publishing Ltd. First Edition, Birmingham.

Polat, Ç., 2016, *Penetration Tests and Security Solutions For Corporate Networks*, M.S. Thesis Dokuz Eylül University, İzmir.

Ruse, M.E., 2013, *Model Checking Techniques For Vulnerability Analysis of Web Applications*, Ph.D. Dissertation, Iowa State University, Iowa.

Vural, Y., 2007, *Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri*, M.S. Thesis, Fen Bilimler Enstitüsü Gazi Üniversitesi, Ankara.

Yalçınkaya, S., 2012, *Assessıng Standard Compliance Of Public Institution Web Sites of Turkey*, M.S. Thesis, The Middle East Technical University, Ankara.

Yaşar, H., 2014., *Kurumsal Siber Güvenliğe Yönelik Tehditler ve Mücadele Yöntemleri: Eylem Planı Örneği*, M.S. Thesis, Bilişim Enstitüsü Gazi Üniversitesi, Ankara,