IJAMEC

International Journal of
Applied Mathematics,
Electronics and Computers

ISSN:2147-8228 www.atscience.org/IJAMEC

Advanced Technology and Science

Original Research Paper

Evaluation of Most Visited E-Commerce Web Sites in Turkey in Aspects of Structure and Security

Atakan DAŞDEMİR[1], Mustafa Nevzat ÖRNEK*[2], Humar KAHRAMANLI[2]

DOI: 10.18100/ijamec.2018138630

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, 12 of the most visited e-commerce sites were scanned as an ordinary user to consider a safety assessment of the general situation of the websites. 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.

Keywords: *penetration tests, web security, weakness analysis*

1. Introduction

The information is important in this century. However its secrecy, integrity and accessibility as in “Information Security” is important as well. Information security is the effort to create a secure information processing platform to protect information or data in the electronic environment from unauthorized access while preserving and transporting without disrupting its integrity [1]. There are various difficulties in ensuring information security due to the transformation of management needs related to information security, in methodology, improper configuration of network security devices, avoiding security by taking into account time and costs in projects, lack of knowledge about the information security of the institution's employees [2]. Internet and web security are increasing every day due to millions of users and exist in all areas of life from finance to health, from communication to entertainment. The Internet has become an integral part of our daily lives, providing unprecedented convenience through web and mobile applications [3].

Since web applications are open to all including hackers, because of their definition, security of these applications is troublesome [4].

Since nowadays the information security is important, there are many studies in literature. Polat [5] mentioned the importance of penetration testing, which should be done intermittently for information security, especially for the information security, by talking about the types of infiltration tests, the study methodology and the application forms. Stiawan et al. [6] analyzed cyber-attack techniques and the penetration test anatomy for assisting security officers to perform appropriate self-security assessment on their network systems. Sandhya et al. [7] focused on solving the problem of threat of expose of data issue by surveying various tools for penetration testing. In addition they provided a sample for basic penetration testing using Wireshark. Nixon and Haile [8] used some penetration tests on WLAN security protocols and MAC Filtering. They used computer with Kali Linux operating system for this aim. As a result of various experiments they observed that there are many loopholes in WLAN and proposed a solution to secure the WLAN using Pseudo Random MAC Address Generation Algorithm called PRMACGA. Bullee et al. [9] investigated the extent of persuasion principles are used in successful social engineering attacks. They extracted 74 scenarios from social engineering literature and analyzed. Each scenario was split into attack steps, containing single interactions between offender and target. For each attack step, persuasion principles were identified. As a result of the scenario analysis they determined how to exploit the human element in security. Wu et al. [10] analyzed the measures that a social planner such as the government or industry association controls firms’ security decisions. The obtained results show that taken precautions measures are not always is effective. They recommend to social planners to enhance or attenuate the controlling level of the two security decisions based on realistic security and business environments. Čisar et al. [11] discussed the assessment of information system security. The authors focused on three major features of the system for the security of an information system: availability, integrity and confidentiality. The paper presents a wide-ranging overview of possible uses, benefits and drawbacks of Kali Linux Operating System. Stasinopoulos et al. [12] proposed an open-source tool which named as Commix that automates the process of detecting and exploiting command injection flaws on Web applications. They presented and elaborate on the software architecture and detection engine of Commix as well its extra functionalities that greatly facilitate penetration testers and security researchers in the detection and exploitation of command injection vulnerabilities.

[1] *Graduate School of Natural Sciences, Selcuk University, Konya, TÜRKİYE*

[2] *Department of Computer Engineering, Technology Faculty, Selcuk University, Konya, TÜRKİYE*

* *Corresponding Author: nevzat@selcuk.edu.tr*

In this study, several e-commerce 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.

2. Material and Method

Penetration tests are important for assessing websites in terms of structure and security. Thus, this study explains the methods of penetration tests and their use.

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.) [13]. Web security penetration tests and the methods used are shown in Table 1.

Table 1.Security Test used in Penetration Tests [14]

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

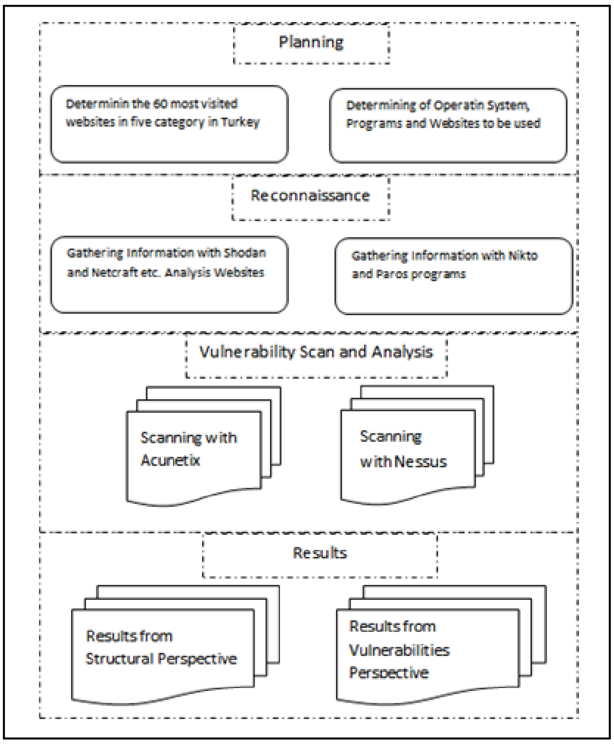
Planning
Determinin the 60 most visited websites in five category in Turkey
Determining of Operatin System, Programs and Websites to be used
Reconnaissance
Gathering Information with Shodan and Netcraft etc. Analysis Websites
Gathering Information with Nikto and Paros programs
Vulnerability Scan and Analysis
Scanning with Acunetix
Scanning with Nessus
Results
Results from Structural Perspective
Results from Vulnerabilities Perspective

Fig. 1. Method Followed

The purpose for the penetration tests is to determine and eliminate the weaknesses of web sites and prevent accessing of unauthorized persons. [15]. Penetration tests consists of 5 phases as data collection, weakness scan and analyze, exploitation, continuous access and reporting.

For working material most visited 12 e-commerce sites from Turkey are determined based on https://ww.alexa.com website statistics. 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 Figure 1. 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.

3. Results

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. Results below are obtained at the end of the studies.

3.1. Structural Results

The information of operating system used, web host software, platform they work on, Security equipment they used, location and web trackers of websites which are chosen from the Turkey's top visited websites, is below in Tables 3, 4, 5, and 6. 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

Operating Systems	Numbers
Windows 2003 Server	1
Windows 2008 Server	4
Windows 2012 Server	-
Windows 2016 Server	-
Linux	3
Undetected	4

As seen on Table 3 web server use Linux as operating system with the 25%, while 33.33% of them uses Win 2008. 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

Web Servers of Websites	Numbers
IIS 7.5	3
IIS 8.5	2
Nginx	2
Apache	2
Undetected	3

As seen on Table 4 the percentage of IIS (last version 10.0) choosers as web host software is 41.67% and all of them are using old version. On examined websites it has been seen that web host Nginx (latest version 1.13) software has being used with 16.6%. The older versions of Nginx software could be reason to some weaknesses like remote exploit. There are not websites which uses PWS software and IIS 7.0.

Table 5. Working Platforms

Working Platforms	Numbers
.net	7
PHP	4
Undetected	1

According to Table 5 .NET is the most using platform with 58.33%.

Table 6. Security Equipment

Security Equipment	Numbers
F5 BigIp	2
Citrix Netscaler	2
Undetected	8

As shown as Table 6, 4 (33.33%) websites uses security equipment, while others equipments of other 8 websites could not be detected. It has been seen that Citrix Netascaler and F5 BIGIP uses by 2 websites as WAF which can distribute traffic between the determined hosts as distributer and is a protector against especially injection and XSS attacks.

3.2. 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 7.

Table 7. Degrees of Vulnerabilities found by Acunetix v10

Degrees of Vulnerabilities	Numbers
Low	31
Medium	9
High	-

As shown in Table 7, no site has high risk vulnerability and many of vulnerabilities is a low degree.

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 8.

As shown in Table 8, no sites have high risk vulnerability and many of sites have medium vulnerabilities.

Table 8. Degrees of Vulnerabilities found by Nessus v6.10.5

Degrees of Vulnerabilities	Numbers
Low	2
Medium	10
High	-

4. Conclusion and Suggestions

This research generates a template for Turkey's top visited 12 e-commerce 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 25%.
- As the web server, 16.67% is preferred to nginx software.
- When it comes to the platform used .NET is the most preferred with 58.33%.
- Determined websites are using security equipment with 33.33%.
- At the end of the Acunetix software scans "Clickjacking:X-Frame-Option Header Missing" and "Cookie Without HttpOnly Flag Set are the most common weakness in low level risks with %25.
- According to Nessus program "Web Application Potentially Vulnerable to Clickjacking" is the most common weakness in medium level risks with %80 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 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
- Against the CSRF exploit threat which is seen in most web sites CAPTCHA usage or 'I am not a robot' using is suggested.

References

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

[2] S. Boşal, "Kamuda Bilgi Güvenliği Ve Iller Bankasi A.Ş. Örneği", Uzmanlık Tezi, İller Bankasi Anonim Şirketi Ankara, 2017.

[3] P.H.A. Fung, "Mitigations of Web Application Security Risks," Ph.D. dissertation, Information Engineering The Chinese University, Hong Kong, 2014.

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

[5] Ç. Polat, "Penetration tests and security solutions for corporate networks", Master of Science Thesis, Dokuz Eylül University İzmir, 1-182, 2016.

[6] D. Stiawan, M.Y. Idris, A.H. Abdullah, F. Aljaber, R. Budiarto, "Cyber-Attack Penetration Test and Vulnerability Analysis", International Journal of Online Engineering, Vol 13, No 1: 125-132, 2017.

[7] S. Sandhya, S. Purkayastha, E. Joshua, A. Dee, "Assessment of Website Security by Penetration Testing Using Wireshark", International Conference on Advanced Computing and Communication Systems, Coimbatore, INDIA, 2017.

[8] S. Nixon, Y. Haile, "Analyzing Vulnerabilities on WLAN Security Protocols and Enhance its Security by using Pseudo Random MAC Address", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS'2017), 2017.

[9] J.H. Bullée, L. Montoya, W. Pieters, M. Junger, P. Hartel, "On the anatomy of social engineering attacks—A literature-based dissection of successful attacks", Journal of Investigative Psychology and Offender Profiling, Volume 15, Issue 1, 20–45, 2017.

[10] Y. Wu, G. Feng, R.Y.K. Fung, "Comparison of information security decisions under different security and business environments, Journal of the Operational Research Society, 2018.

[11] P. Čisar, S.M. Maravi, I. Fürstner, "Security Assessment with Kali Linux", Bánki Közlemények1(1) 49 – 52, 2018.

[12] A. Stasinopoulos, C. Ntantogian, C. Xenakis, "Commix: automating evaluation and exploitation of command injection vulnerabilities in Web applications", International Journal of Information Security, 2018. https://doi.org/10.1007/s10207-018-0399-z

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

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

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