ЖАРАТЫЛЫСТАНУ ЖӘНЕ ТЕХНИКАЛЫҚ ҒЫЛЫМДАР

NATURAL AND TECHNICAL SCIENCES

IRSTI 06.58.45

N. Abdinurova[1], M. Galiyev[2], A. Aitkulov[3]
[1,2,3]Suleyman Demirel University, Kaskelen, Kazakhstan

OWASP VULNERABILITIES SCANNING OF A PRIVATE UNIVERSITY WEBSITES

Abstract. The web keeps expanding and attacks continue to go up against the web. This paper draws on scanning the private university websites for The Open Web Application Security Project (OWASP) and web attack mitigation solutions. Methods for vulnerability scanning as well as mechanisms for developing web protection will be studied. This study is the framework for future work that will end with the advancement of web scanning and security in order to suggest better innovations.

Keywords: Vulnerability, Scan, Protect, OWASP, Web attack.

***

Аңдатпа. Желі кеңеюін жалғастыруда және желіге қарсы шабуылдар да жалғасуда. Бұл мақала университеттердің жеке веб-сайттарын ашық веб-қосымшалардың қауіпсіздігі жобасына (OWASP) және веб-шабуылдарды жеңілдету шешімдеріне негізделген. Осалдықтарды сканерлеу әдістері, сондай-ақ веб-қорғауды әзірлеу тетіктері зерделенетін болады. Бұл зерттеу ең жақсы инновацияларды ұсыну үшін веб-сканерлеуді және қауіпсіздікті дамытумен аяқталатын болашақ жұмыс үшін негіз болып табылады.

Түйін сөздер: Осалдық, сканерлеу, қорғау, OWASP, Веб-шабуыл.

***

Аннотация. Сеть продолжает расширяться, и атаки продолжают идти против сети. Эта статья основана на сканировании веб-сайтов частных университетов для проекта безопасности открытых веб-приложений (OWASP) и решений по смягчению веб-атак. Будут изучены

методы сканирования уязвимостей, а также механизмы разработки веб-защиты. Это исследование является основой для будущей работы, которая завершится развитием веб-сканирования и безопасности, чтобы предложить лучшие инновации.

Ключевые слова: Уязвимость, Сканирование, Защита, OWASP, Веб-атака.

Introduction

OWASP is a not-for-profit organization dedicated to strengthening the security of applications. It achieves this objective by providing data, including clear lists of common vulnerabilities, and services to help inform developers about the possible security problems that may exist in their code, such as testing tools and intentionally insecure applications. One of the best-known and commonly used cybersecurity tools in nature is the OWASP Top Ten List of web application vulnerabilities.[1] This list is intended to outline the vulnerabilities within their applications that web application developers should be most aware of.

The main purpose of this work is to scan private university websites for OWASP vulnerabilities and prevent hacking attacks. Nowadays, security and privacy of data is playing a big role, as in universities too. If the data is not secure enough or the system is not strong enough it can cause a crash of infrastructure.

The topic of web protection or OWASP vulnerabilities has been the subject of several recent studies. One of them is to use blockchain technology to prevent OWASP top ten attacks. Blockchain primarily lacks guidance and tools for blockchain-specific security. Blockchain technology, however, is not unlike conventional IT infrastructure, and the blockchain is therefore subject to many of the vulnerabilities that occur in other environments. Of the ten vulnerabilities listed in the current version of the Top Ten List of OWASP, only one does not map blockchain well because the XML format of blockchain is not used.[2]

Another article was published in November 2020 to learn more about OWASP vulnerabilities. It says about hundreds of works on methods of server-side web security, and many of them suggest improved models of protection. Current Web Application Firewalls (WAFs) only have basic security laws, which do not take developments in the field into account.[3] Between the testing items and the WAF methods, there is a significant difference.

For scanning and testing the websites it needs some tools. And the comparison was made between these tools and applications. The findings of comparative assessment of the scanners indicated that scanners work differently in various categories. Therefore, in scanning web vulnerabilities, no scanner can be called an all-rounder. However, combining the performances of these two scanners in both benchmarks, we concluded that ZAP performed better than Arachni in SQLI, XSS and CMDI categories. In the LDAP group, Arachni, on the other hand, performed much better [4].

Methods and Materials

The Linux Kali operating system was used in order to launch vulnerability scanning tools. Since it is a free OS and has over 600 instruments for penetration testing and security analytics, Kali Linux is used by hackers. Kali follows an open-source model and on Git all the code is available and tweaking permitted. Kali has multi-language support that makes it possible for users to function in their native language. Kali Linux is fully customizable all the way down to the kernel according to its convenience.

To identify any vulnerabilities from the website OWASP ZAP 2.9.0 was used. In order to detect these threats, OWASP Zed Attack Proxy gives you the power. And it's open-source, so you are free to use it. It helps you find the security vulnerabilities in your application.

For better scanning of vulnerabilities, it was used in an application named Legion 0.3.6. Legion is an open source, easy-to-use, super-extensible and semi-automated network penetration testing tool that aids in discovery, reconnaissance and exploitation of information systems. It has some features like automatic recon and scanning with NMAP, whataweb, nikto, Vulners, Hydra, SMBenum, dirbuster, sslyzer, webslayer and more (with almost 100 auto-scheduled scripts).

Data and Results

Automated scan attacks the given url and shows where the webpage is the most vulnerable.When the process ends analyzing the website, information about any vulnerabilities will be shown in Alerts. Here are some results from scanning SDU websites.

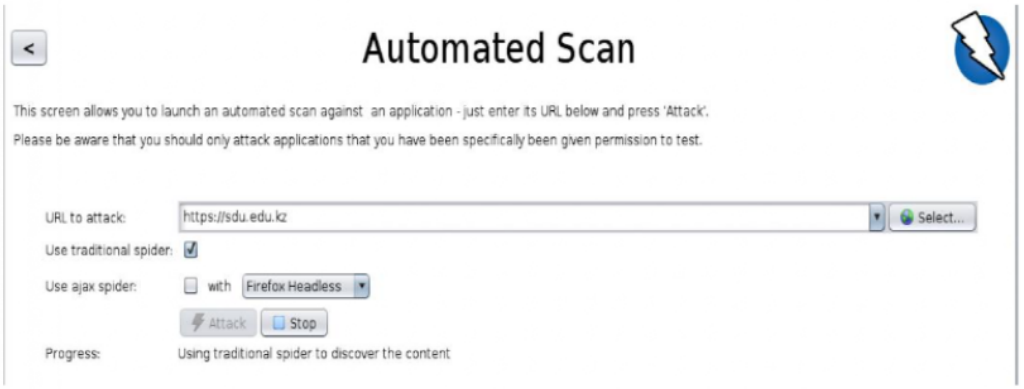

Figure 1. Automated Scan

As it is described in the figure 1, Alerts are specified by different flag colors. Red, yellow and blue by the level of risk respectively. By new scanning there were detected two medium types of alerts.

Directory Browsing	
URL:	http://sdu.edu.kz/wp-content/uploads/
Risk:	Medium
Confidence:	Medium
Parameter:	
Attack:	Parent Directory
Evidence:	
CWE ID:	548
WASC ID:	48
Source:	Active (0 - Directory Browsing)

Figure 2. Parent Directory Detection

The first one is a parent directory attack on a website. By this attack hackers can see or view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information. If the system is vulnerable to bypassing directories, an attacker can use this vulnerability to exit the root directory and access other parts of the file system. This allows the attacker to view files with limited access, which can provide the attacker with additional information that is necessary for further hacking of the system. Depending on how access to the Website is configured, the attacker will execute commands, posing as a user associated with the "website". Therefore, it all depends on what access the site user has in the system [5].

There are two ways of preventing this attack. First of all, ensure you have installed the latest version of your web server software, and sure that all patches have been applied. Secondly, effectively filter any user input. Ideally remove everything but the known good data and filter metacharacters from the user input. This will ensure that only what should be entered in the field will be submitted to the server.

X-Frame-Options Header Not Set	
URL:	https://sdu.edu.kz
Risk:	Medium
Confidence:	Medium
Parameter:	X-Frame-Options
Attack:	
Evidence:	
CWE ID:	16
WASC ID:	15
Source:	Passive (10020 - X-Frame-Options Header)

Figure 3. Clickjacking

The second one is a "clickjacking" attack with X-Frame-Options parameter. Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide

credentials or sensitive information, transfer money, or purchase products online. And some solutions can be: to use "Sameorigin" or use "Deny-Allow-From" to allow specific websites to frame in a web page. Sameorigin allows opening a page inside a frame only if the parent document has the same source. Deny-Allow-From allows the page to be opened inside the frame only if the parent document is located on the domain specified in the header.

Discussion

By this point all the necessary preparations have been made. Now as long as website weaknesses are found by Legion, but it was found 2 medium level vulnerabilities by OWASP ZAP. And solutions were researched and suggested. The same type of scanning was made to other university websites. They are namely: for the SDU portal which is "my.sdu.edu.kz" and "pms.sdu.edu.kz", it is the same vulnerability, Cross-site scripting(XSS). XSS is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. First of all for the future work it is to analyze this vulnerability and find a solution.

Conclusion

This study provides a detailed survey of current techniques in the web application vulnerability research field. There were two vulnerabilities detected. First, a parent directory attack on a website. By this attack hackers can see or view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. Second, "clickjacking" is a way to trick users into clicking on a victim site without understanding what is going on. It is dangerous if important actions can be performed on a click. This type of attack is quite dangerous, because when developing interfaces, we do not assume that a hacker can click on behalf of a user. Therefore, vulnerabilities can be found in completely unexpected places. To protect against this attack, we recommend using X-Frame-Options: Sameorigin on pages or even entire sites that are not intended to be viewed in a frame.

There were outlined a number of unanswered questions that still need to be answered. The security of university data is very important in terms of education. That is why this research is aimed to be clearly completed.

References

1 Jinfeng Li, Vulnerabilities Mapping based on OWASP-SANS: A Survey for Static Application Security Testing (SAST), Annals of Emerging Technologies in Computing, July 2020.UCL Department of Electronic & Electrical Engineering. *Visible Light Communications*. URL: https://www.ee.ucl.ac.uk/pilab/research-1/visible-light-communications.

2 Elsevier, B.Y. Mapping the OWASP Top Ten to Blockchain, The International Workshop on Blockchain Security (IWBCS 2020),

November 2-5, M adeira, Portugal. *Howard Poston/Procedia Computer Science* 177 (2020): pp. 613–617.

3 Ouissem Ben Fredj and Omar Cheikhrouhou, An OWASP Top Ten Driven Survey on Web Application Protection Methods, University of Sousse, Tunisia, November (2020): pp.1-16.

4 Balume Mburano and Weisheng Si, Evaluation of Web Vulnerability Scanners Based on OWASP Benchmark, School of Computing, Engineering and Mathematics, Western Sydney University, Australia, December (2018): pp. 1-7.

5 Acunetix Website by Invicti, Directory Traversal Attacks, URL: https://www.acunetix.com/websitesecurity/directory-traversal/.