WEB APPLICATION VULNERABILITY TOOLS

Ibrokhimov A. R.
Head of the Department of Cybersecurity of Information Systems,
State Enterprise "Cybersecurity Center", PhD

Haydarov E. D.
Head of the Department of Information Security,
Muhammad al-Khwarizmi TUIT, PhD

ABSTRACT

Today, many organizations developing web applications are finding it important to use scanners to detect vulnerabilities before they are deployed. This article provides an analysis of the tools used to protect against attacks targeting web systems and recommendations for protection .

Keywords: Web Application Firewall, Snort , Suricata , SIEM , IBM QRadar, Acunetix, Netsparker, ThreatMetrix .

INTRODUCTION

Today, due to the constantly growing cybercrime, testing web applications using the human factor is becoming more difficult, because there are vulnerabilities that can be missed during the testing process using the human factor, and the main motivation for this dissertation was to study some scanners that can detect these vulnerabilities. Based on the graduation qualification work, we found that the most effective method is to detect web vulnerabilities using scanners. Since the correct selection of scanners is considered important in detecting vulnerabilities in web application vulnerability scanners, we have two different types of scanners: free (open source) and paid (commercial). The results showed that open source scanners are preferable to paid scanners that are regularly updated to achieve good results. Vulnerability analysis systems – security scanners or vulnerability scanning systems – are responsible for identifying vulnerabilities in a given system. They provide a comprehensive examination of the system to identify vulnerabilities. They are used to identify potential breaches of security policies. The results obtained using the analysis tools provide an assessment of the current state of the system. While these systems cannot detect an attack in progress, they can identify attacks that could be committed. Web application scanning – Internal networks are not the only organizations that need to be protected . They can detect cross-site scripting, SQL injection, and path traversal vulnerabilities. These tools work on a similar principle to vulnerability scanners. Configuration management While many administrators are concerned about zero-day attacks, evidence of misconfigurations and missing patches is a major source of vulnerability for hackers. Many administrators leave such vulnerabilities open for months or years without recognizing or fixing them, even when patches are available. Scanning for and fixing these errors helps ensure the stability of your system, even as assets change. These measures can also be crucial for compliance. Types of Vulnerability Scanning and Detection There are several approaches available to administrators planning their vulnerability scanning strategy. In fact, you can use 1 different as part of your overall security management .

You may want to try different types of scans, as testing your system from different angles will help you cover all the bases. As discussed below, the two main differences are related to the location of the scan (internal vs. external) and the scope (broad vs. limited). Vulnerability analysis systems, also known as security scanners or vulnerability scanners, are responsible for identifying vulnerabilities. They perform a comprehensive scan of a given system to identify vulnerabilities. They are designed to detect potential breaches of security policies. The results obtained from the analysis tools provide an assessment of the current state of the system. While these systems cannot detect an attack in progress, they can identify attacks that could be carried out.

However, Shai Chen's research strongly suggests that some open source scanners, such as Arachni, are becoming as effective as commercial scanners. The research suggests that it is appropriate to use different versions of scanners and different scanners, and that each organization should use the scanner that is most suitable for it and has a reasonable price, because the scanners should be affordable and meet their needs and preferences. The study by Alzahrani, Alquazzaz, Fu, Almashfi, and Zhu, using the "Web Application Security Tools Analysis" method, identified the following: The challenges that companies face in choosing vulnerability scanners. The study first identified the factors that cause distrust in web applications, the vulnerabilities in web applications, and the ways to address the most common vulnerabilities.

For example, research conducted for XSS SQL Injection (database data disclosure vulnerability) has suggested the following.

Cross-Site Scripter (XSSer) – An open-source (free) framework used to detect vulnerabilities related to Cascading Style Sheets in web applications.

SQLninja , Havij, SQL Inject – used to find SQL injection vulnerabilities.

In cases where web application vulnerability scanners use different plugins, different results have been recorded from many scanners. When scanners have different configuration settings and the configuration settings are inconsistent, and when the plugins provided for the scanners are not detected, the detection coefficient will be low because the vulnerability found by the scanner is not available among its plugins, and as a result, the number of failures to find the sought-after vulnerability will certainly increase.

There are also various tools available to detect web attacks. Below are some of these tools:

1. Web Application Firewalls (WAFs):

– AWS WAF: WAF, provided by Amazon Web Services, protects web applications in the AWS environment from SQL Injection, Cross-Site Scripting (XSS), and other common web attacks. Example: If your web application is hosted on an AWS EC2 instance, you can configure AWS WAF to block specific IP addresses or detect HTTP requests and take appropriate action.

– Cloudflare WAF: Cloudflare WAF protects your web application from globally distributed DDoS attacks, SQL Injection, and XSS attacks. Example: If your e-commerce website is powered by Cloudflare, Cloudflare WAF automatically blocks malicious traffic and keeps your site protected at all times.

– Akamai Kona Site Defender: This WAF tool is used to protect against large-scale DDoS attacks and other sophisticated attacks. Example: A media website with high traffic can use Akamai Kona Site Defender because it can effectively detect and block large-scale attacks.

2. Intrusion Detection Systems (IDS):

– Snort: This open source IDS system is used to detect and prevent network attacks. Example: By configuring Snort on a network analyzer computer, you can monitor all network traffic and detect malicious activities where necessary.

– Suricata: This is a high-performance IDS/IPS system used to analyze network traffic and detect threats. Example: By installing Suricata in an environment used for network analysis, it is possible to detect complex and multi-layered threats.

3. Security Information and Event Management (SIEM) Tools:

– Splunk: Used for analyzing large amounts of data and detecting web application attacks. Example: By configuring Splunk to collect and analyze network and application logs, malicious activity can be detected and responded to.

– IBM QRadar: This SIEM tool is used to detect and respond to network and application threats. Example: IBM QRadar collects and analyzes all network events, resulting in real-time information about attacks and threats.

4. Vulnerability Scanners:

– Acunetix: This automated web application scanner detects SQL Injection, XSS, and other common vulnerabilities. Example: You can scan a website with Acunetix and get recommendations to identify and fix vulnerabilities on the site.

– Netsparker: This scanner is used to detect web application and API vulnerabilities. Example: By applying Netsparker to a web application, all vulnerabilities can be analyzed and security vulnerabilities can be fixed.

5. Behavioral Analysis Tools:

– Imperva: This tool detects threats by monitoring anomalies and behavioral changes. Example: By applying Imperva to a web application, it is possible to detect and block actions that deviate from normal user behavior.

– ThreatMetrix: This tool detects fraud and threats through behavioral analysis and digital identity. Example: An online banking web application can use ThreatMetrix to monitor anomalies in user activity and detect fraud.

6. Endpoint Protection Platforms (EPP):

– Symantec Endpoint Protection: This tool protects against web-based threats and malware. Example: By installing Symantec Endpoint Protection on company computers, all network traffic and applications can be protected against malware.

– McAfee Endpoint Security: This tool protects against malicious data and web-based attacks. Example: By installing McAfee Endpoint Security on work computers, you can ensure the security of all users and protect them from malware.

These tools are designed to counter different types of threats, and the right combination of them provides a high level of security.

Below is a tabular comparative analysis of web attack detection tools (Table 1):

Table 1 **Comparative analysis of web attack detection tools**

Vehicle type	Vehicle name	Main functions	Advantages	Disadvantages
Web Application Firewalls (WAFs)	AWS WAF	Protects web applications from common web attacks	Adaptable to the AWS ecosystem, real-time data filtering	Only works in AWS environment
	Cloudflare WAF	Protection against DDoS attacks and other web application vulnerabilities	Globally distributed, automatic optimization	Advanced setup and management
	Akamai Kona Site Defender	Protection against large-scale DDoS attacks and sophisticated attacks	Effective against high traffic and large-scale attacks	High price
Intrusion Detection Systems (IDS)	Snort	Open source network attack detection and prevention system	Open source, widely used	Requires extensive setup and technical expertise
	Meerkat	High-performance IDS/IPS system	Detect network threats quickly and effectively	May require extensive setup and resources
Security Information and Event Management (SIEM) Tools	Splunk	Big data analysis and web application attack detection	Easy to scale and configure, manage large amounts of data	High cost, may require resources
	IBM QRadar	Identify and respond to network and application threats	Large-scale network event analysis, real-time monitoring	Requires complex setup and technical expertise
Vulnerability Scanners	Acunetix	Identifying vulnerabilities in web applications	Automated scanner, widely used	Requires frequent updates to detect new vulnerabilities
	Netsparker	Automated scanner for detecting web application and API vulnerabilities	High-precision, automated analysis	High price
Behavioral Analysis Tools	Imperva	Monitoring anomalies and behavioral changes	Easy to configure, real-time monitoring	May misidentify abnormal behavior
	ThreatMetrix	Fraud detection through behavioral analysis and digital identification	Effective against fraud, widely used	High price
Endpoint Protection Platforms (EPP)	Symantec Endpoint Protection	Protection against web-based threats and malware	Widespread, effective protection	May require resources
	McAfee Endpoint Security	Protection against malicious data and web-based attacks	Widespread, effective protection	May require resources

This table using every one of the tool advantages and disadvantages about wider to the concept has to be These tools should be selected and customized based on the company and application requirements .

REFERENCES

1. Керимов К.Ф. Адаптивная модель защиты электронных ресурсов от угроз информационной безопасности в электронных ресурсах. // Журнал―Мухаммад ал-Хоразмий авлодлари‖. – Ташкент, 2020. – №3(13) – С.3-7.
2. Pooja Chaudhary, Brij B. Gupta, A.K.Singh, Securing heterogeneous embedded devices against XSS attack in intelligent IoT system, Computers & Security Volume 118, July 2022.
3. Экатерина Гурина, Никита Ключников, Ксениа Антипова, Dmitry Koroteev, Making the black-box brighter: Interpreting machine learning algorithm for forecasting drilling accidents, Journal of Petroleum Science and Engineering Volume 218, November 2022
4. Ҳамдамов Р.Ҳ., Иброҳимов А.Р., Корпоратив тармоқ хавфсизлиги муаммоларини йечиш йўллари,«Ахборот коммуникация технологиялари ва дастурий таъминот яратишда инновацион ғоялар» Республика илмий-техник конференцияси, Самарқанд-2021, Б. 334-337.
5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие: — М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. 416 с.