Spectrum Journal of Innovation, Reforms and Development

Volume 20, October, 2023 | ISSN (E): 2751-1731

Website: www.sjird.journalspark.org

EVALUATION OF THE EFFECTIVENESS OF METHODS OF DETECTING WEAKNESSES AND NETWORK ATTACKS

Ibrokhimov A. R.
Head of the Department of Information Systems and
Resources of the "Cybersecurity Center"

Haydarov E. D.
Associate Professor of the Department of Cryptology of TUIT
Named after Muhammad Al-Khwarazmi

Abstract

The article contains the evaluation of the effectiveness of the methods of detecting vulnerabilities and network attacks, the recommendations proposed by the Cyber Security Center to increase the effectiveness of the detection of vulnerabilities and network attacks and the provision of information security, the results of the three-step testing method for detecting vulnerabilities on servers, the results of the evaluation of the effectiveness of the VITE method of detecting network attacks given.

Keywords: network attacks, vulnerability, website, OWASP, injection vulnerabilities, business logic vulnerabilities, session management vulnerabilities, web server vulnerability detection software, web server data protection software from network attacks, VITE.

Introduction

Today, in cyberspace, in particular, a number of works are being carried out aimed at increasing the level of security of information systems and websites and ensuring cyber security, as well as ensuring the security of information and communication technologies of users, and information security it is necessary to regularly increase the level of knowledge of the security administrator in the field. A number of recommendations have been made by the Cyber Security Center to identify vulnerabilities and network attacks and increase the effectiveness of information security. These are:

1. Use of licensed and certified operating systems and programs.

2. Regularly update the latest versions of operating systems, software and security components. Implementation of updating works from official sources.

3. Use security plugins that scan for, remove, and protect against future malware.

4. Regular backup of databases, files, mail, etc.

5. Delete unused plugins.

6. Strengthen password-based authentication - it is recommended to use a complex and non-repeatable password for the administrator account, personal cabinet on the website of the service provider and credentials (account) on the server (for example, for dedicated or co-

location hosting) will be done. When changing the password, it is recommended to use the rules for creating passwords for accounts (accounts) with upper and lower case letters, numbers, special characters and a minimum length of 8 characters. It is recommended to set up two-factor authentication (where this option is available). It is also recommended to limit the number of login attempts (to protect against "bruteforce" attacks).

7. Providing access to the information system or website from devices (computers, tablets) with antivirus programs installed with updated virus databases.

8. Carrying out examinations on compliance of information systems and resources with information security requirements. Timely elimination of identified weaknesses based on the recommendations sent based on the results of the expertise.

9. To regularly improve the skills and knowledge of users (employees) in the field of information and communication technologies and information security.

10. Rapid detection and appropriate measures to eliminate threats and consequences of cyber security incidents.

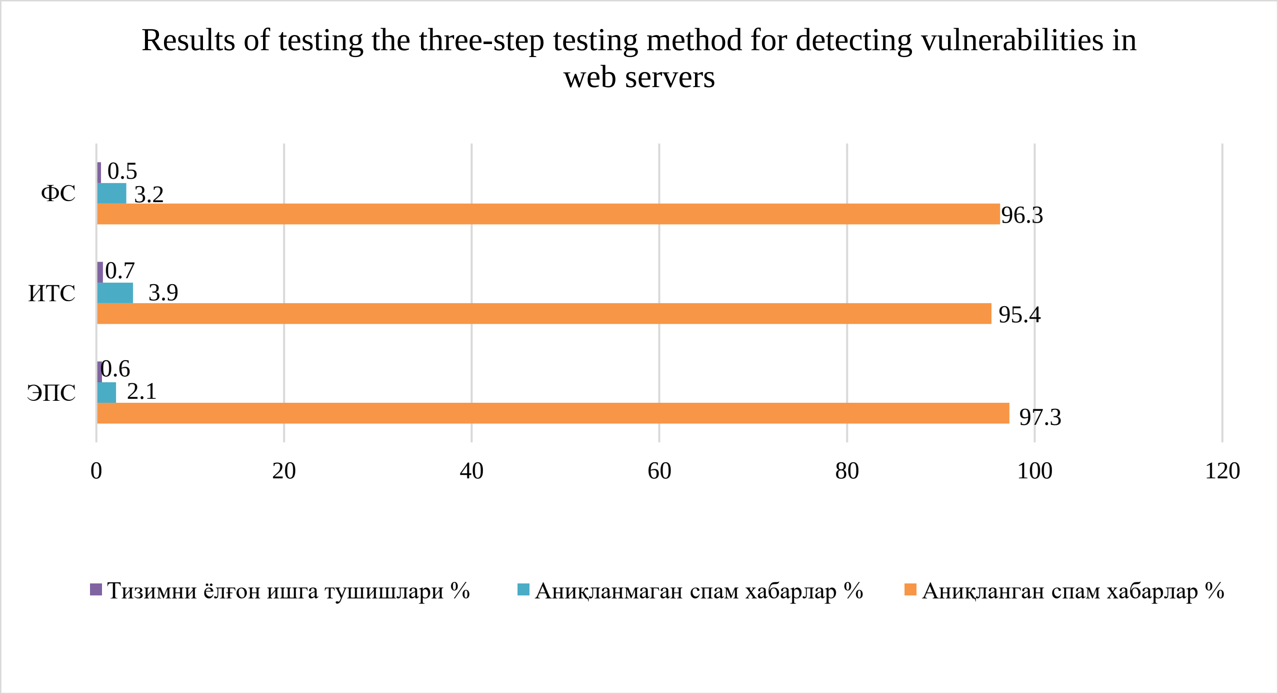
Today, the number of network attacks against websites, portals and internal information exchange systems of every organization is increasing day by day. The main reason for this is undetected vulnerabilities in the system.

Analytical data are provided 4 times a year by organizations that provide provider services and by organizations that produce software and hardware used to ensure information security (Kaspersky, Risk Watch, OWASP, Positive Technologies, etc.). According to the results of the analysis, the main problem is related to vulnerabilities, and it was found that vulnerabilities exist in almost half of the analyzed systems. For example, a total of 13,434 errors of various degrees were detected in all applications, and 1,412 samples of malicious code were recorded on the pages of vulnerable systems. The percentage of sites compromised by malware distributors was 1.7%. These data were obtained as a result of attacks carried out within one quarter. Each of these vulnerable sites has server-side command execution vulnerabilities that have been confirmed to be exploitable to compromise the system. The probability that an automatic scanner will detect a bug in a web application is about 35% and can be increased to 80% with detailed expert analysis. The most common mistakes made by web application developers are cross-site scripting and SQL Injection vulnerabilities, accounting for more than 19% and 17% of all identified vulnerabilities, respectively.

Table 1 shows the test results of the three-step testing method for detecting vulnerabilities in developed web servers.

Table 1 Test results of a three-step testing method for detecting vulnerabilities in servers. These include: injection vulnerabilities (IZ), business logic vulnerabilities (BMZ), session management vulnerabilities (SBZ).

Types of vulnerabilities	Total number of vulnerabilities	Identified vulnerabilities %	Undetected vulnerabilities %	False activation of the system %
IZ	23	97,9	1,5	0,6
BMZ	11	96,4	2,8	0,8
SBZ	16	98,1	1,2	0,7



1 – picture. Results of testing a three-step testing method for detecting vulnerabilities in web servers

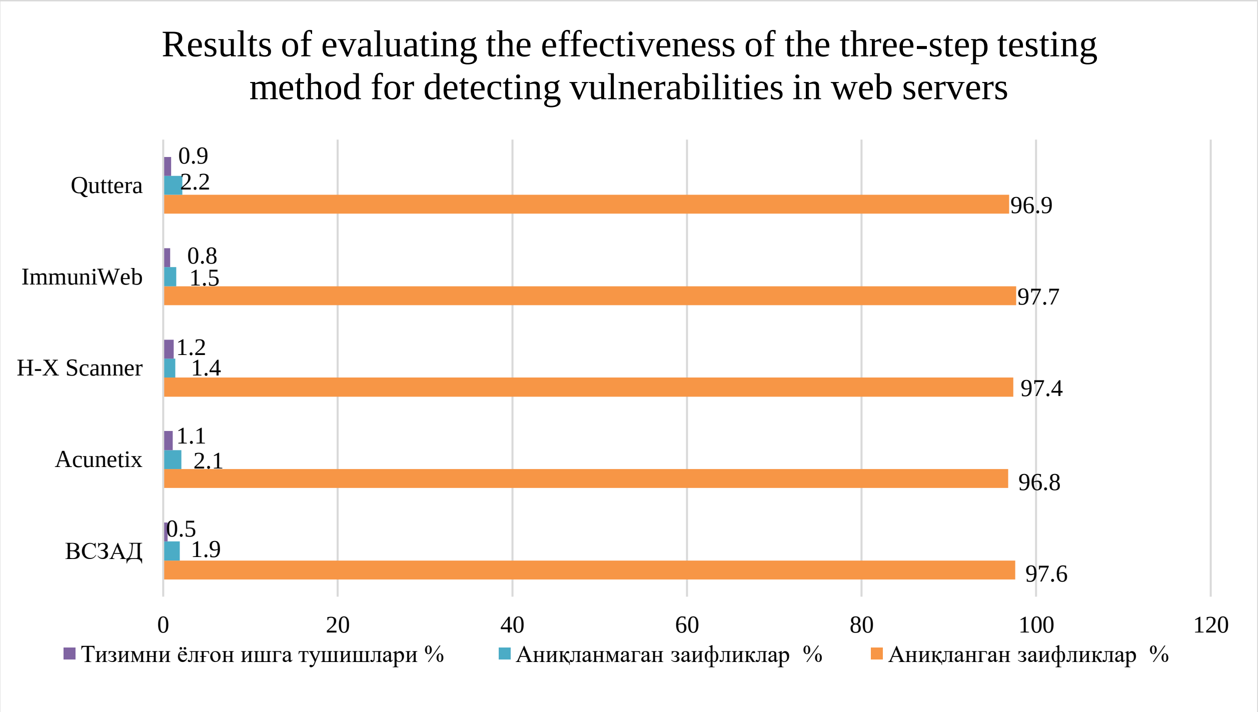
Table 2 shows the results of comparing systems based on the three-step testing method for detecting vulnerabilities in web servers with the effectiveness of other vulnerability detection systems.

Table 2

Results of evaluating the effectiveness of the three-step testing method for detecting vulnerabilities in web servers

In this case, the Web Server Vulnerability Detection Program (VSZAD).

Vulnerability detection programs	Total vulnerabilities	Identified vulnerabilities %	Undetected vulnerabilities %	False activation of the system %
VSZAD	26	97,6	1,9	0,5
Acunetix	26	96,8	2,1	1,1
H-X Scanner	26	97,4	1,4	1,2
ImmuniWeb	26	97,7	1,5	0,8
Quttera	26	96,9	2,2	0.9



2 – picture. Results of evaluating the effectiveness of the three-step testing method for detecting vulnerabilities in web servers

3 – table

Results of evaluating the effectiveness of the VITE method for detecting network attacks In this case, the program for protecting data on the web server from network attacks (VSMTHHD)

Network attack detection programs	Total number of network attacks	Detected attacks %	Undetected attacks %	False activation of the system %
VSMTHHD	163469	97,9	1,5	0,6
S-Terra	163469	95,9	2,3	1,8
AirSnare	163469	96,8	1,8	1,4
Network Olympus	163469	97,1	1,6	1,3
Nagios	163469	95,4	2,7	1.9

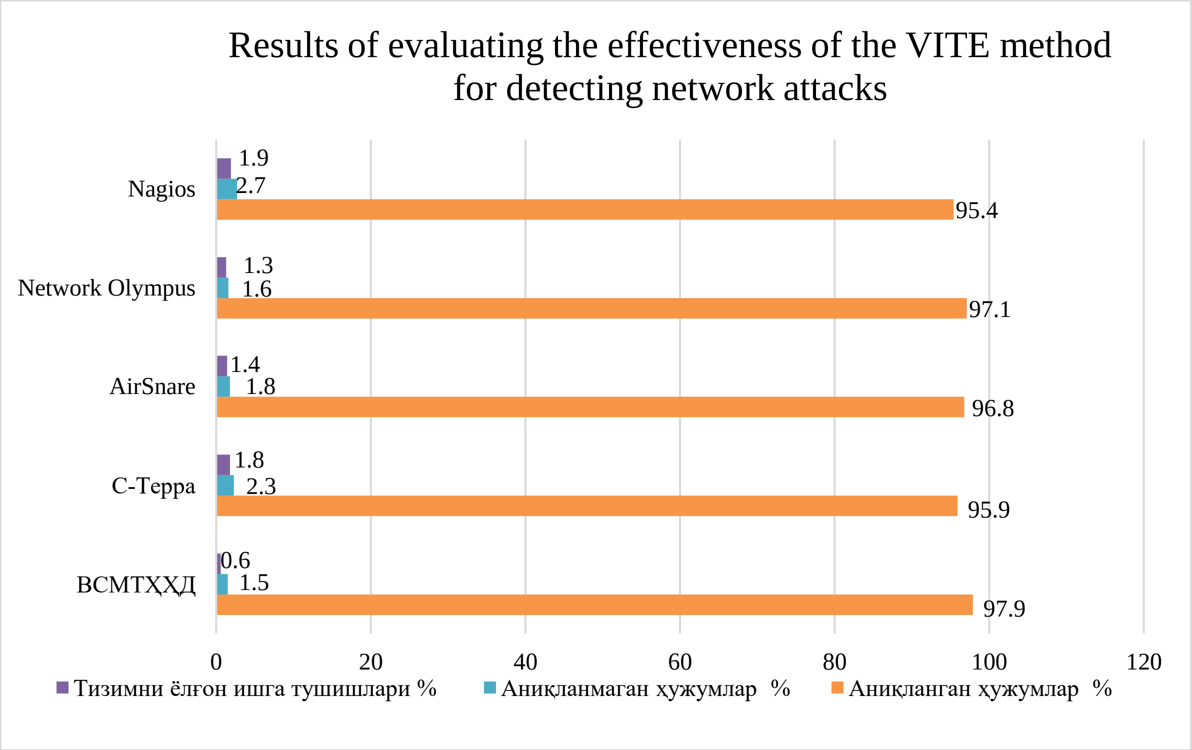


Figure 3 Results of evaluating the effectiveness of the VITE method of network attack detection

Summary

As can be seen from the above-mentioned tables, the test results of the software tool developed based on the method of detecting vulnerabilities in web servers and the methods of detecting network attacks against data on the web server are more detectable than the software tools used in practice, and the system's isolation is higher. then showed that the startup status is low.

References

1. Ibrohimov Azizbek Ravshonbek ugli, Detection method for “denial of service” attacks on web applications, Shemical technology. control and management, 2020, №4(94), p. 75-81.
2. Beijing Rising cyber security technology Co., Ltd. Rising 2020 China cyber security report. Information security research 2021;7(2):102-109.
3. Xu Cheng. Research on cyber attack prevention methods for enterprise information security. Journal of the chinese academy of electronic science 2020; 15(5):483-487.
4. Ibroximov A.R., Korxonadagi axborot tizimida axborotlarni himoyalash jarayonlarini avtomatlashtirish, Ict in education: Challenges and solutions, International conference, Tashkent, May 20, 2021–B. 81-83.
5. Sherzod Rajaboyevich Gulomov, Nasrullayev Nurbek Bakhtiyorovich, Method for security monitoring and special filtering traffic mode in info communication systems,

2016 International Conference on Information Science and Communications Technologies (ICISCT), 2016.

6. Xamdamov Rustam Xamdamovich, Ibrohimov Aziz Ravshanbek o'g'li, & Haydarov Elshod Dilshod o'g'li. (2022). Logistik regressiya asosida tasniflash masalalarini yechish. research and education, 1(9), 162–171. https://doi.org/10.5281/zenodo.7443501
7. Rustam Kh. Khamdamov, Komil F. Kerimov, Methods of Blocking Vulnerabilities of XSS Type Based on the Service Oriented Architecture // Journal of Automation and Information Sciences DOI: 10.1615/JAutomatInfScien.v51.i12.30 New York, USA 12,2019. –pp.18-24. Scopus (https://www.scopus.com/sourceid/25497)