GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 12, Issue 9 September (2024)

# THREATS APPLIED IN THE NATIONAL SEGMENT OF THE INTERNET NETWORK

Gafurov Sh. A.
Independent Researcher of Tashkent University of Information
Technologies named after Muhammad al-Khwarizmi

## ABSTRACT

In this article Threats and attacks directed at domains located in the national segment of the Internet network , levels of threats to web resources, existing vulnerabilities in web applications, and the interaction between an attack made as a result of this vulnerability and its possible consequences are presented.

**Keywords** : security , electronic government , eGov system , cyber attacks, web resources, national segment, threat.

## INTRODUCTION

Security requirements are not always followed in their development due to the fact that the developers of every website or web resource placed in the national segment of the Internet do not have the necessary knowledge and skills. That is why it is recommended by experts to test every website that is developed. The continuous research of many specialized enterprises and organizations shows that the majority of web applications have a high level of vulnerability risk, which is a risk not only for the website itself, but also for the information security activities of the organizations that provide the hosting service and the domain where the website is located. also increases the level.

Network threats and attacks on web applications are usually the first step in breaking the networks of large companies, and false information and advertisements on official sites about the owner of information are the main tools in information warfare. The vast majority of web applications, not just on the national segment of the internet, but on the entire internet, are vulnerable web applications, and today's widespread distributed denial-of-service (DDoS) attacks can compromise the usability of web applications. It does not take much time to break. If the special services of the provider working at the network level and the devices used to protect the traffic do not provide protection, then the attacker who made the attack will have the opportunity to control the user's actions in the web applications and send special resource-rich requests to the site. As a result, even a small amount of traffic can cause the site to crash completely.

Securing the electronic government (eGov) system is a critical issue. ( “Electronic government is an electronic document exchange system of public administration based on the automation of the entire complex of state-level management processes and the significant improvement of the efficiency of public administration and the reduction of social communication for each member of society. The creation of electronic government is the management of documents and their processing implies the construction of a nationwide networked system of collective management, which implements the solution of the full range of tasks related to the processes ). Why was the security of the eGov system considered an important issue? The main reason for this is that all interactive public services provided in eGov services are provided online, and the national segment of the Internet network (".UZ") serves as a single platform for this.

As we know, the presentation of e-government projects through an unprotected Internet channel causes a number of problems. That is why many countries do not have a single government infrastructure that supports information flow control, authentication, confidentiality and integrity. In addition, the public key infrastructure (Public Key Infrastructure - PKI) used in electronic commerce cannot be used in eGov without a thorough analysis. All organizations want to integrate information from their websites into the e-government system, but cannot achieve this due to the lack of security requirements in the developed web applications. Countries all over the world pay a lot of attention to the security of their national e-government system. While the credibility assessment for trade is based on monetary issues, national segment infrastructure is considered to be related to important issues of community and privacy.

Based on the above, before presenting the general threats to security in the national segment of the Internet network, it is necessary to state a number of performance characteristics of the typical components of the eGov system that distinguish them from others.

1. Difficulties in implementing software and hardware unification. In some cases, there is a custom development that runs on a specific software-hardware environment. This makes it difficult to monitor web applications in the national segment of the Internet network and reduces the level of reliability.

2. The need to protect personal data of customers. This requirement is one of the first requirements for developers of web resources that will be integrated into the eGov system. At the same time, the data should be open for static processing and analysis by appropriate services. In this case, personal information about the user is required to be securely protected.

3. It is required that the usability and integrity of the open data used based on the types of services related to the user is ensured.

4. Agreed standards - business and some other requirements of state and municipal organizations, as well as individual individuals, in the development of a set of profiles common to users, only in general view, by use by service providers. ra is required to meet general safety requirements.

Web resources located in the national segment of the Internet can have local networks that aggregate various information and computing resources with access to the global Internet. Through these channels, it is possible to interact with other collective access centers, as well as eGov's data storage and reservation centers. Effective protection of eGov resources cannot be achieved without a detailed classification that facilitates the identification and countermeasures of potential threats to eGov resources.

According to international experience, the US federal standard FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems" (Minimum Security Requirements for Federal Information and Information Systems) prevents unauthorized access, tampering, opening, modification and service through an information system. defines a "threat" as an existing situation or event that has the potential to adversely affect the organization's activities by means of refusal to show. It also requires identifying the potential source of the threat in order to effectively use the known vulnerability of the information system. Accordingly, threats to web resources located in the national segment of the Internet network are implemented at four levels. Organization of communications in the environment of the national segment of the Internet network is mostly based on a set of TCP/IP protocols that ensure compatibility between different computers.

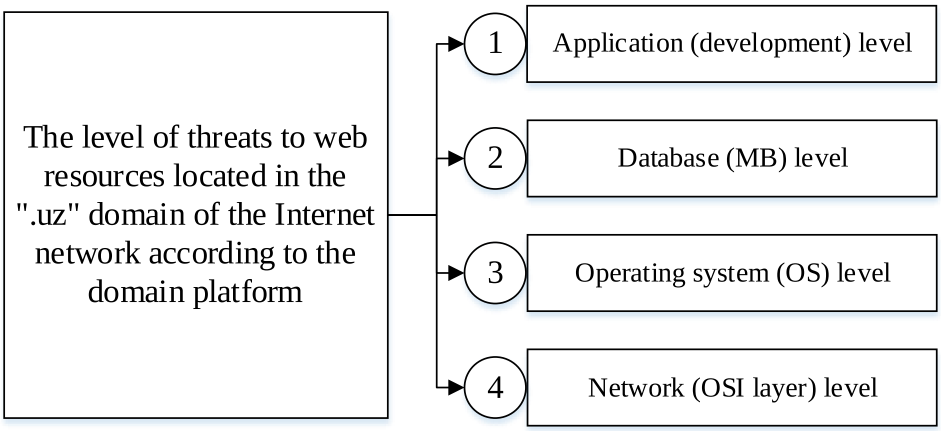
The level of threats to web resources located in the ".uz" domain of the Internet network according to the domain platform
1
Application (development) level
2
Database (MB) level
3
Operating system (OS) level
4
Network (OSI layer) level

Figure 1. The level of threats to web resources located in the national segment of the Internet network according to the domain platform

This set of protocols has become the standard for inter-network communication due to its ability to use the resources of the Internet global network and easy adaptation. However, the widespread adoption of the TCP/IP protocol stack has also exposed its weaknesses. Therefore, such situations occur in distributed systems, especially for remote attacks, because their components usually use open data transmission channels, and the attacker can modify (change) the transmitted traffic, not just passively monitor the transmitted data. will also be possible.

It can be said that the complexity of detecting a remote attack and the relative simplicity of the attack (due to the excess functionality of modern systems) have brought this type of illegal activity to the first place in terms of the level of danger. According to the above domain platform, web resources located in the national segment of the Internet network are proposed as the level of threats, on the other hand, the response to the services provided at these levels is also the reason, because at what level the threat is implemented and not protected against. service failures at this level are:

- the level of applications (developments) (application software) responds to interaction with the user and controls usability;
- the database level (MBD) is responsible for data storage and processing and integrates with the database management system;
- the level of the operating system (OS) is responsible for servicing MBD and application programs (it is necessary to pay attention to the type of OS used by the user);
- the network level corresponds to the interaction of web application nodes located on a national segment of a distributed Internet network.

Voluntary attack by attackers is carried out by activating one or another vulnerability existing in the national segment of the Internet network. This allows successful information attacks located in the “.uz” domain of the Internet network. All actions that can be used to disrupt the performance of web applications located in the ".uz" domain of the Internet network also indicate the absence of protective measures that allow an attacker to perform actions that lead to a disruption of system performance. Improperly configured security policy, lack of certain information security tools or errors in the software used allow an attack to be carried out using vulnerabilities. Based on this, it can be said that the relationship between the existing vulnerability in web applications located in the national segment of the Internet network and the attack made as a result of this vulnerability and its possible consequences is as follows.

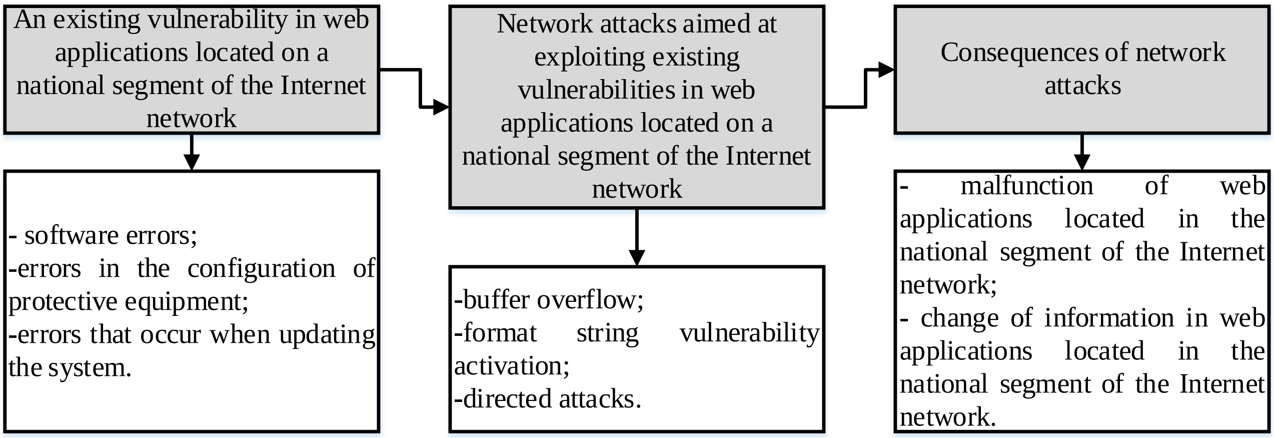
An existing vulnerability in web applications located on a national segment of the Internet network
- software errors;
-errors in the configuration of protective equipment;
-errors that occur when updating the system.
Network attacks aimed at exploiting existing vulnerabilities in web applications located on a national segment of the Internet network
-buffer overflow;
-format string vulnerability activation;
-directed attacks.
Consequences of network attacks
- malfunction of web applications located in the national segment of the Internet network;
- change of information in web applications located in the national segment of the Internet network.

Figure 2. An existing vulnerability in web applications located in a national segment of the Internet network and the relationship between an attack made as a result of this vulnerability and its possible consequences

The presence of vulnerabilities creates sufficient conditions for the emergence and implementation of various information security threats and attacks against web applications located in the “.uz” domain of the Internet network and the possible consequences of an information attack. This may lead to violations of information privacy, integrity and usability of web applications and resources located in the ".uz" domain of the Internet network .

## REFERENCES

1. Sharafaldin , A.H. Lashkari, A.A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion traffic characterization, in: ICISSP 2018 - Proc. 4th Int. Conf. Inf. Syst. Secure. Priv., 2018, pp. 108–116.
2. R. Patil, H. Dudeja, C. Modi, Designing an efficient security framework for detecting intrusions in virtual network of cloud computing, Comput. Secure. 85 (2019) 402–422.
3. C. Kh ammassi, S. Krichen, A NSGA2-LR wrapper approach for feature selection in network intrusion detection, Comput. Netw. 172 (2020), 107183, https://d o i. o rg/10.1016/jc o mnet.2020.107183
4. V. Hajisalem, S. Babaie, A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection, Comput. Netw. 136 (2018) 37–50
5. B.A. A. Al'Aziz, P. Sukarno, and A. A. Wardana, “Blacklisted IP distribution system to handle DDoS attacks on IPS Snort based on Blockchain,” Proceeding - 6th Inf. Technol. Int. Semin. ITIS 2020, pp. 41–45.