# SECURITY ISSUES IN WEB SYSTEMS

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

**Abstract**:
Nowadays, along with the rapid development of Internet technologies, ensuring the security of web systems has become one of the urgent problems. This article analyzes the main security threats encountered in web systems and the reasons for their occurrence. In particular, types of attacks such as Malware, Phishing, DDOS attacks, Botnet, SQL injection, XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery) are analyzed.

**Keywords**: malware, phishing, DDOS, botnet , SQL injection , XSS, CSRF, insider threats, zero-day exploits, data breaches, untrusted APIs .

Web systems have become an integral part of our daily lives, providing us with convenient access to information, services, and communication. However, the increasing reliance on web systems also exposes them to various threats that can compromise their security, integrity, and availability. Understanding these threats is essential for individuals and organizations to effectively protect their web systems. Some common threats to web systems include:
Malware - Malicious software, including viruses, worms, ransomware, and spyware, poses a serious threat to web systems. Malware can damage websites and users' devices, leading to data corruption, unauthorized access, or financial loss. A malware attack refers to the malicious infiltration of a computer system, network, or device with the intent of causing damage, stealing confidential information, or disrupting normal operations. Malware, short for malicious software, is designed by cybercriminals to exploit vulnerabilities in software, hardware, or human behavior. There are different types of malware attacks, each with a specific purpose and method of execution. Some common forms of malware include viruses, worms, Trojans, ransomware , spyware, adware, and rootkits. This malware can spread through infected email attachments, malicious websites, corrupted software downloads, or even USB drives.
Once malware has successfully infiltrated a system, it can cause serious damage. Some common consequences of a malware attack include:
data theft;
financial loss;
system failure;
creating a botnet;

invasion of privacy.

Phishing attacks are attacks that attempt to trick users into revealing sensitive information, such as usernames, passwords, or credit card information, by impersonating legitimate websites or organizations. These attacks often use social engineering techniques and can lead to identity theft or financial fraud. In this type of attack, attackers attempt to trick individuals or organizations into revealing sensitive information, such as login credentials, credit card numbers, or personal information. Phishing attacks typically involve the use of fraudulent emails, text messages, or websites that impersonate legitimate entities, such as banks, social media platforms, or online retailers.

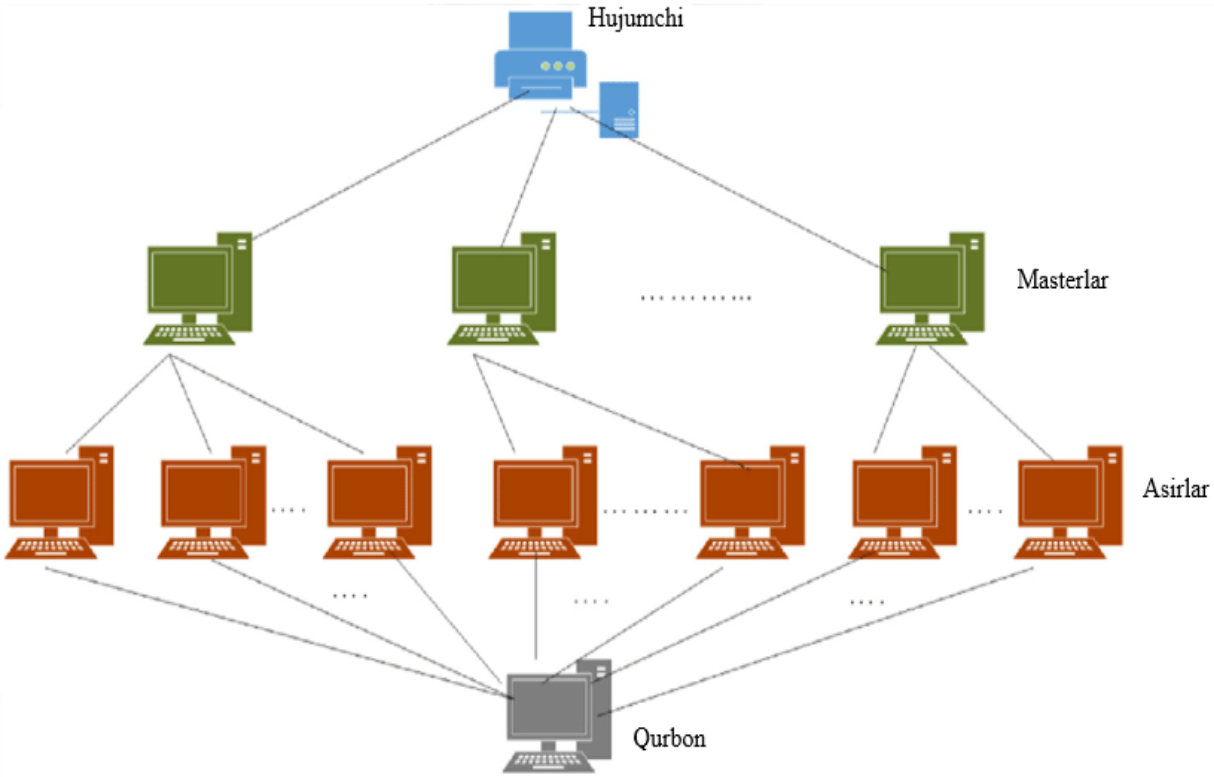


Figure 1. Appearance of a DDOS attack

Distributed denial-of-service attacks – DDOS attacks aim to flood a web system's resources with a large volume of traffic from multiple sources. This can lead to service disruptions, making the web system unavailable to legitimate users.

Botnet creation - Malware can turn infected devices into part of a botnet - a network of compromised computers controlled by a hacker. These botnets are often used for large-scale cyberattacks, such as Distributed Denial of Service (DDoS) attacks that take down targeted websites or networks.

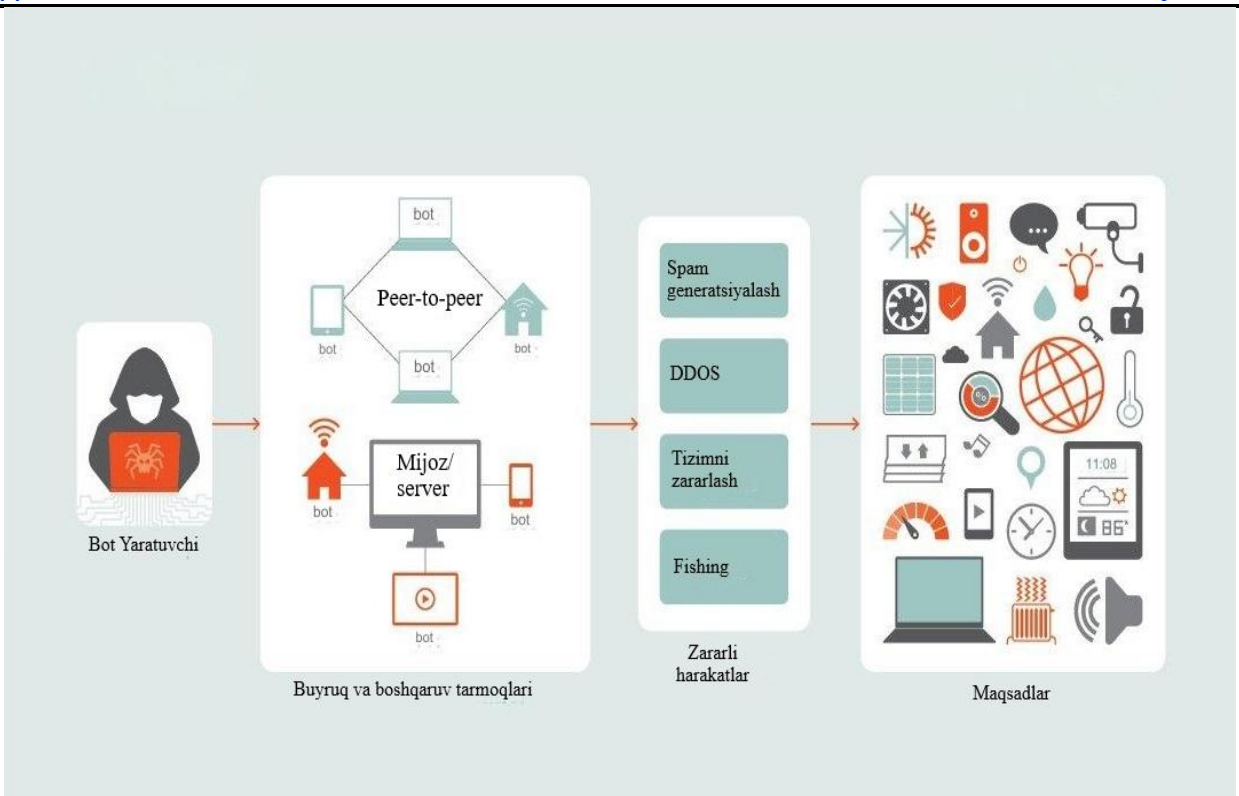


Figure 2. Botnet implementation and management architecture

SQL Injection: SQL injection attacks exploit vulnerabilities in web applications that use a database backend. Attackers inject malicious SQL commands through user input fields, which can gain unauthorized access to the database or control its contents. SQL Injection is a type of cyberattack targeting databases that exploits vulnerabilities in the application's input validation process. It involves injecting malicious SQL statements into the application's input fields, which are then executed by the database. This allows attackers to manipulate, extract, or modify data stored in the database.

The SQL Injection attack process typically includes the following steps:

- identifying vulnerable applications;
- exploiting vulnerability;
- gaining unauthorized access;

When a SQL Injection attack occurs, the consequences can be serious:

data theft;

manipulation or deletion of data;

unauthorized access to other systems.

To prevent SQL Injection attacks, individuals and organizations should take the following security measures:

Cross-Site Scripting (XSS) - XSS attacks involve injecting malicious scripts into web pages that are viewed by other users. These scripts can be used to steal sensitive information or perform actions on behalf of the victim, which can lead to data breaches or unauthorized

actions. Cross-site scripting involves injecting malicious scripts into a website or web application, which are then executed by users' browsers. This allows attackers to steal sensitive information, perform unauthorized actions on behalf of users, or compromise the website.

The XSS attack process typically includes the following steps:

- identify vulnerable applications
- inserting malicious scripts
- executing malicious scripts:

When other users visit a compromised web page or interact with an affected application, the embedded scripts are executed by their browsers. This allows attackers to steal sensitive information such as login credentials or session cookies, perform actions on behalf of users, or manipulate website content.

Cross-Site Request Forgery (CSRF) attacks trick users into performing unwanted actions on an authenticated web system. By exploiting the trust between the user and the web system, attackers can perform unauthorized transactions or change user settings. Unlike XSS attacks, which target vulnerabilities in input validation and output encoding, CSRF attacks exploit the trust built into the browser to perform unauthorized actions on behalf of the user.

The CSRF attack process typically includes the following steps:

- identifying vulnerable applications;
- creating malicious requests;
- deceiving users when completing requests;
- committing unauthorized actions.

Set the SameSite attribute on cookies to restrict the use of the SameSite attribute in first-party contexts. This prevents cookies from being sent in cross-origin requests and reduces the risk of CSRF attacks.

Insider Threats - Insider threats refer to individuals within an organization who abuse their privileges or access rights to compromise the security of web systems. This includes unauthorized access to data, sabotage, or the leakage of confidential information.

Zero-day exploits - Zero-day exploits target previously unknown vulnerabilities in web systems for which no patches or security fixes are available. Attackers exploit these vulnerabilities before developers can fix them, making it crucial for organizations to stay vigilant and update their systems regularly.

Data breaches - Web systems often store sensitive user data, including personal information, financial details, or intellectual property. Data breaches can occur for a variety of reasons, such as weak security measures, internal threats, or external attacks. These breaches can result in identity theft, financial losses, or reputational damage.

Untrusted APIs - Application Programming Interfaces (APIs) allow different systems to interact and exchange data. Untrusted APIs can be used by attackers to gain unauthorized access to sensitive data or perform unauthorized actions on connected systems.

**List of used literature**

1. Иброхимов А.Р., Корхонадаги ахборот тизимида ахборотларни ҳимоялаш жараёнларини автоматлаштириш, Ict in education: Challenges and solutions, International conference, Tashkent, May 20, 2021–B. 81-83.
2. Li Chen, Cong Tang, Junjiang He, Hui Zhao, Xiaolong Lan, Tao Li, XSS adversarial example attacks based on deep reinforcement learning, Computers & Security Volume 120, September 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. Li Peng. Practical experience on phishing email protection. Network security technology and application 2022; 1:136-137.
5. Иброҳимов А.Р. “Веб сервердаги заифликларни аниқлашнинг модификацияланган қора қути усули ва алгоритмлари” “Илмий хабарнома Физика –математика тадқиқотлари” журнали. 2021/№2(3), Андижон-2021. –Б. 81-85.