Volume 3, Issue 12 December 2025 **ISSN (E):** 2938-3757

TYPES OF ATTACKS ON WEBSITES AND METHODS OF THEIR PREVENTION

Tuxtanazarov Dilmurod Solijonovich
Associate Professor, PhD, International Islamic
Academy of Uzbekistan, Tashkent, Uzbekistan

Abstract
This article discusses various types of attacks on websites. The most common types of cyberattacks observed today and the causes of such attacks are analyzed. Information is provided on major attacks such as Distributed Denial of Service (DDoS), SQL injection, Man-in-the-Middle attacks, Cross-Site Scripting (XSS), and DNS attacks. In addition, the causes of attacks on websites and recommendations for their prevention are presented.

Keywords: Website, Internet, DDoS, SQL injection, Cross-site scripting, attack, information security, vulnerabilities, data.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

Introduction

Nowadays, it is very easy to obtain information on how to compromise computer networks and carry out various cybercrimes. Printed materials describing technologies for committing computer crimes are freely distributed. Website attacks refer to malicious actions or tactics used to compromise website security with the aim of disrupting normal operation, stealing confidential information, or gaining unauthorized access to website databases. Such attacks are typically carried out by hackers, cybercriminals, or other malicious actors who exploit vulnerabilities in website code, architecture, or infrastructure.

Common types of website attacks include DDoS attacks, SQL injection attacks, XSS attacks, phishing attacks, malware attacks, brute-force attacks, Man-in-the-Middle attacks, and others. Website owners are generally advised to take preventive and mitigation measures, such as regularly updating software, implementing security protocols, and increasing user awareness.

An attacker can discredit an entire network by disrupting the operation of one of its components. Modern telecommunication technologies have enabled local networks to connect to global networks such as the Internet. The rapid development of the Internet has made security a critical issue, requiring security mechanisms for all networks and systems connected to it, regardless of the type of data being processed.

In the early stages of network technology development, the damage caused by viruses and other cyberattacks was relatively minor, as the global economy was not highly dependent on information technologies. Today, however, due to the continuous increase in cyberattacks and the growing dependence of businesses on electronic information exchange, even minor attacks can result in significant financial losses.

Protecting networks from unauthorized access, data misuse, modification, and loss has become a pressing issue. Enterprises, organizations, and government institutions that rely on network-

Licensed under a Creative Commons Attribution 4.0 International License.

based operations must pay serious attention to network security before connecting to networks for data exchange.

Network security is ensured by implementing various tools, methods, and measures aimed at protecting transmitted, stored, and processed information in a reliable and systematic manner. Security tools must be capable of quickly detecting threats and responding appropriately. Network security threats can be categorized into several groups[1]:

- Eavesdropping and data manipulation during transmission;
- Denial-of-Service (DoS);
- Port scanning.

Eavesdropping and data manipulation attacks can be carried out through telephone communication lines, instant messaging over the Internet, videoconferencing, and fax transmissions, allowing attackers to secretly intercept, alter, or block information. Various network analysis protocols can be used to carry out such attacks. Malicious software can convert digital audio encoded using CODEC standards into high-quality but large-sized audio files (e.g., WAV format).

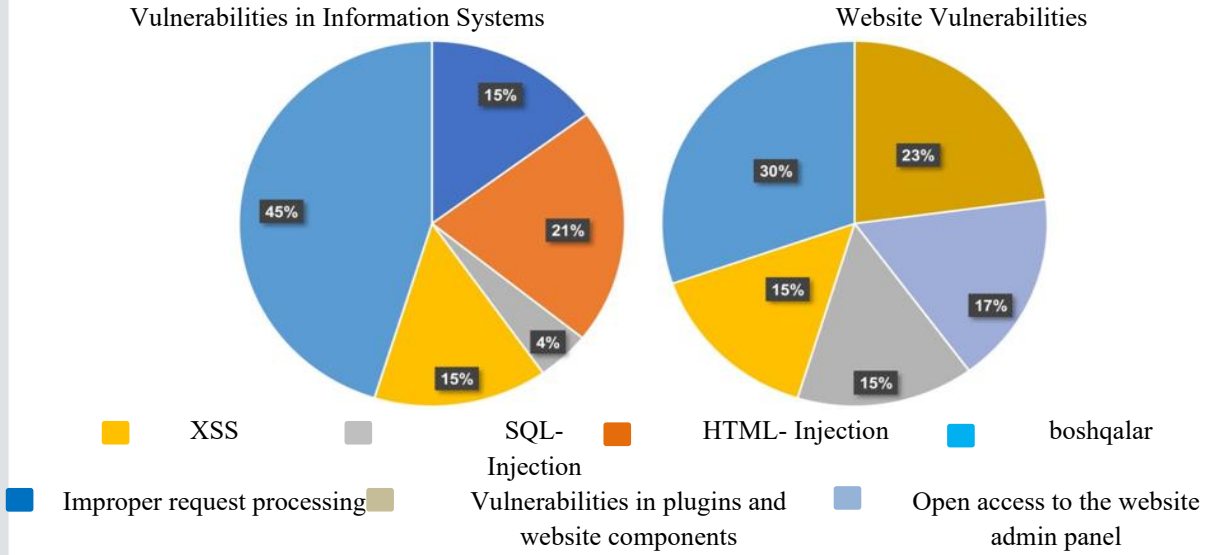

Figure 1. Analysis of more than 1.3 million cyberattacks in the national Internet segment in 2024 [2]

Website attacks are numerous, and some can cause severe damage. DDoS Attacks: A Distributed Denial of Service (DDoS) attack involves one or more attackers using a large number of devices to simultaneously send massive amounts of traffic to servers or websites, attempting to exhaust network resources required for normal operation. These attacks may be carried out for personal, corporate, political, or social motives.

To mitigate DDoS attacks, multiple security mechanisms are essential, including firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and DDoS mitigation systems. Organizations providing network services must continuously enhance their security measures to ensure network protection.

[1] https://azkurs.org/mavzu-tarmoq-xavfsizligiga-zamonaviy-tahdidlar.html
[2] https://www.google.com/url?sa=i&url=https%3A%2F%2Fkun.uz%2Fuz%2Fnews%2F2022%2F03%2F02%

Licensed under a Creative Commons Attribution 4.0 International License.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4

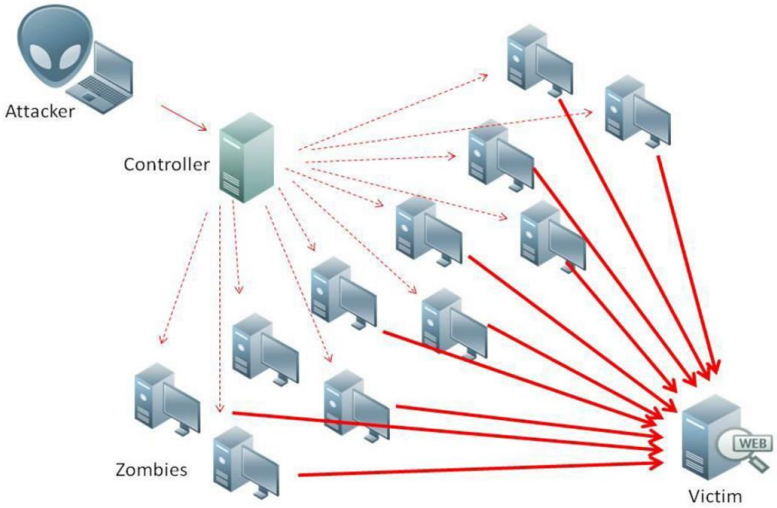

Figure 2. DDoS attack illustration.

To prevent DDoS attacks, networks should implement additional measures such as access control, traffic filtering, request validation, and real-time attack notifications.

Malware Attacks: Malware refers to malicious software or files that can be installed on a computer or network without the user's consent, aiming to damage systems, steal personal data, delete information, or compromise network security.

Malware is often difficult to detect because it is commonly bundled with seemingly legitimate software or files. It may also spread through downloaded files, emphasizing the need to scan files obtained from the Internet.

Malware comes in various forms, including viruses, trojans, rootkits, spyware, and ransomware.

Figure 3. Malware attack.

Many malware types exploit vulnerabilities in operating systems, browsers, or applications to steal user data. To protect against malware, systems and applications must be regularly updated, and users should avoid downloading files from suspicious sources such as unknown emails or untrusted websites.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4
Licensed under a Creative Commons Attribution 4.0 International License.

SQL Injection Attacks: SQL injection is a common attack technique targeting websites or networks. In such attacks, hackers manipulate SQL queries to gain unauthorized access to databases or modify stored data. SQL injection can allow attackers to retrieve sensitive information such as usernames, passwords, credit card details, or business-related data, posing serious security risks.

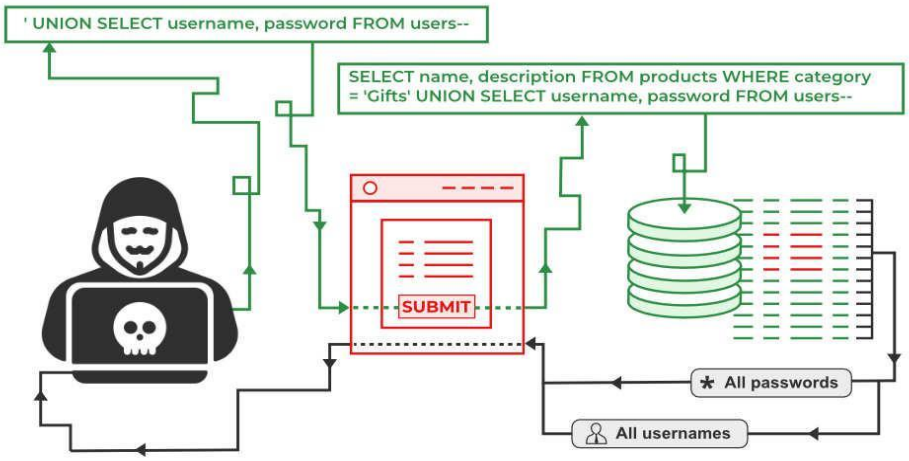

Figure 4. SQL injection attack.

To prevent SQL injection attacks, input validation, secure query handling, regular updates of servers and applications, and proper database access controls are essential.

Cross-Site Scripting (XSS) Attacks: Cross-Site Scripting (XSS) is one of the most frequently encountered web attacks. Attackers inject malicious scripts into websites to steal user data or manipulate website content. XSS attacks may compromise user credentials and disrupt website functionality.

Mitigation measures include input sanitization, proper data validation, output encoding, detection of unauthorized scripts, and restricting direct user input where necessary.

Phishing Attacks: Phishing attacks aim to obtain confidential information such as bank card details, passwords, or personal data via email, phone calls, SMS, or fraudulent websites. Attackers impersonate trusted organizations to deceive users.

Users should verify official URLs and email addresses and avoid clicking suspicious links or downloading attachments. Phishing sites often lack proper security certificates and request sensitive personal information.

Man-in-the-Middle (MITM) Attacks: Man-in-the-Middle attacks involve intercepting and manipulating Internet traffic between users and websites. Attackers can steal sensitive information such as usernames, passwords, email addresses, and banking details.

Using SSL/TLS certificates, accessing websites via direct URLs, and avoiding unsecured networks can help mitigate MITM attacks.

DNS Attacks: DNS attacks exploit vulnerabilities in the Domain Name System, which translates human-readable domain names into machine-readable IP addresses. Since organizations often cannot directly control DNS traffic between remote clients and DNS

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4
Licensed under a Creative Commons Attribution 4.0 International License.

servers, DNS attacks have become a relatively easy method for cybercriminals to disrupt networks.

Security Scanning Tools: Several specialized tools exist to verify whether operating system parameters are correctly configured and unchanged. Examples include ASET for Solaris, KSA for NetWare and Windows NT, and SSS for Unix systems.

SSS (System Security Scanner) program. This program is designed to check the security status of computers running the Unix operating system and identify external and internal vulnerabilities in the operating system. In addition, it can check access rights, file ownership rights, network resource configuration, authentication programs, and more.

The program has the following capabilities:

- Configuration check, i.e. checking the configuration to prevent unauthorized access. This includes configuration files, operating system version, access rights, user accounts and passwords;
- Checking for dangerous changes in the system. It is used to search for changes that have occurred in the system as a result of unauthorized access. Such changes include changes to the amount of memory occupied by the following files, changes to access rights or the information in the file, changes to user access parameters to the resources, as well as unauthorized transfers of files to other external computers;
- User interface usability. This interface not only provides convenient work with the program, but also generates reports on the work performed;
- remote scanning. It provides the ability to scan computers on the network and encrypt data during communication;

generates complete reports on the work performed.

References

1. E. Jordan and A. Becker, Princeton officials broke into Yale online admissions http://www.yaledailynews.com/article.asp?AID= 19454, July 25, 2002.
2. Prof. Marwan Dwairy 2010, Journal of Child and Family Studies
3. Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef Concordia University, Montreal, Canada
4.https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.geeksforgeeks.org%2Fsql-injection%2F&psig=AOvVaw3aayeeMTmsmkkWe- E
5.https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.alliantcybersecurity.com%2Fdifferent-types-malware-attacks-

Licensed under a Creative Commons Attribution 4.0 International License.

Web of Technology: Multidimensional Research Journal
webofjournals.com/index.php/4