ANALYSIS OF THREATS TO WEBSITES AND THEIR PROTECTION

Mahkamov Anvarjon Abdujabborovich
International Islamic Academy of Uzbekistan
“Modern information and communication
Technologies” department, associate professor, PhD
mahkamovanvar2020@gmail.com
Tuhtanazarov Dilmurod Solijonovich
International Islamic Academy of Uzbekistan
“Modern information and communication
Technologies” department, associate professor, PhD
dtuxtanazarov@gmail.com

Annotation. The article presents the current threats to websites and ways to protect them, outlining measures to ensure information security. It emphasizes the implementation of modern technologies to protect communication networks, software products, information systems, and resources. Additionally, it discusses the development of technical infrastructure to further enhance the protection of information resources.

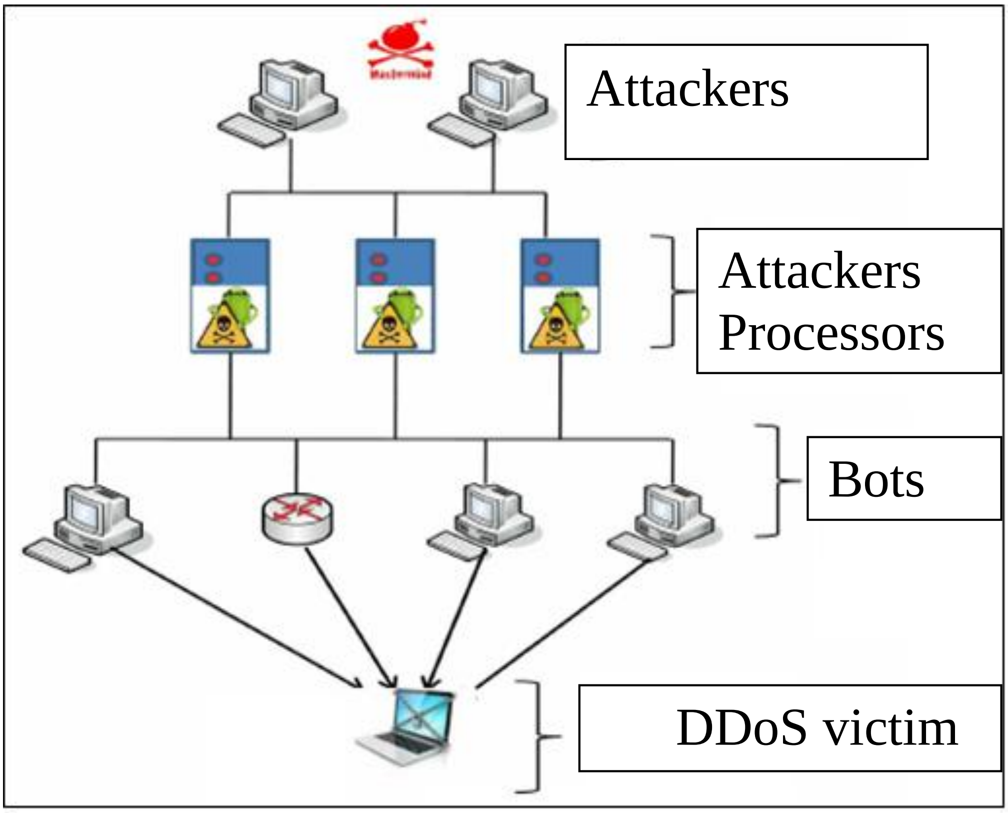
Keywords: Websites, threats, analysis, cyber threats, security, information resources.

Introduction. Most modern information systems are created in the form of websites. Therefore, special attention must be given to ensuring the security of websites.

Developers may not always pay special attention to the complete protection and security of the websites they create. Every website, in one way or another, can be subjected to hacker attacks, potentially compromising information security. Taking this into account, ensuring the security of websites is of great importance.

Websites can be highly diverse: digital libraries, social networks, web portals of various educational institutions, online stores, official websites of various organizations, banks, and more.

First and foremost, attention should be given to the security of the web server. This is because it is responsible for receiving and processing HTTP requests from clients to the website. It ensures the operation of many websites worldwide, is accountable for essential services, and stores users’ personal data.



1.1-figure. Stages of a DDoS attack execution [1]

The need to protect servers is one of the most important tasks for any organization. Even during the early days of websites, hackers launched attacks on important organizations' websites, such as Citibank in the United States (1994). As a result, $12 million was stolen, and NATO, the CIA, and the Department of Justice also became victims.

In recent years, a large number of cyberattacks have been carried out. This is because such content can "generate" large amounts of money or obtain and alter information that could impact significant events for a country. A noteworthy aspect is that the geographic location of the server has no effect on its protection. Attacks can be launched from any access point. This is due to the fact that web servers are designed for data transmission between users, making them inherently open. As a result, they are vulnerable to numerous weaknesses. For example, an attacker could modify the code of an HTTP server or database server, or even alter the web pages themselves, changing their original functionality.

Today, the most common actions of offenders in cyberattacks are frequently observed:

- ➢ Posting incorrect information on a website;
- ➢ Unauthorized access to servers where valuable data is stored;

[1] Developed by the author

- Attacking the database of bank cardholders. This involves stealing information about the primary bank cardholders' account numbers, names, surnames, and contact details, then attempting to gain access to large amounts of money;
- Developing viruses capable of easily compromising passwords, subsequently deploying these viruses, and storing or utilizing the stolen information.
- Launching attacks on the websites of governmental institutions in various countries.
- Disseminating viruses that significantly slow down Internet speeds, with some cases leading to the complete disconnection of certain regions from the network.
- Conducting DDoS (Distributed Denial-of-Service) attacks aimed at overwhelming networks with excessive requests.
- Gaining unauthorized access to information related to SecurID technology, which is used to ensure the security of corporate computer networks.

According to estimates, every third website is controlled by unauthorized individuals. This is an unpleasant and concerning fact for web developers.

Statistical data indicates that large companies suffer the most damage compared to others.

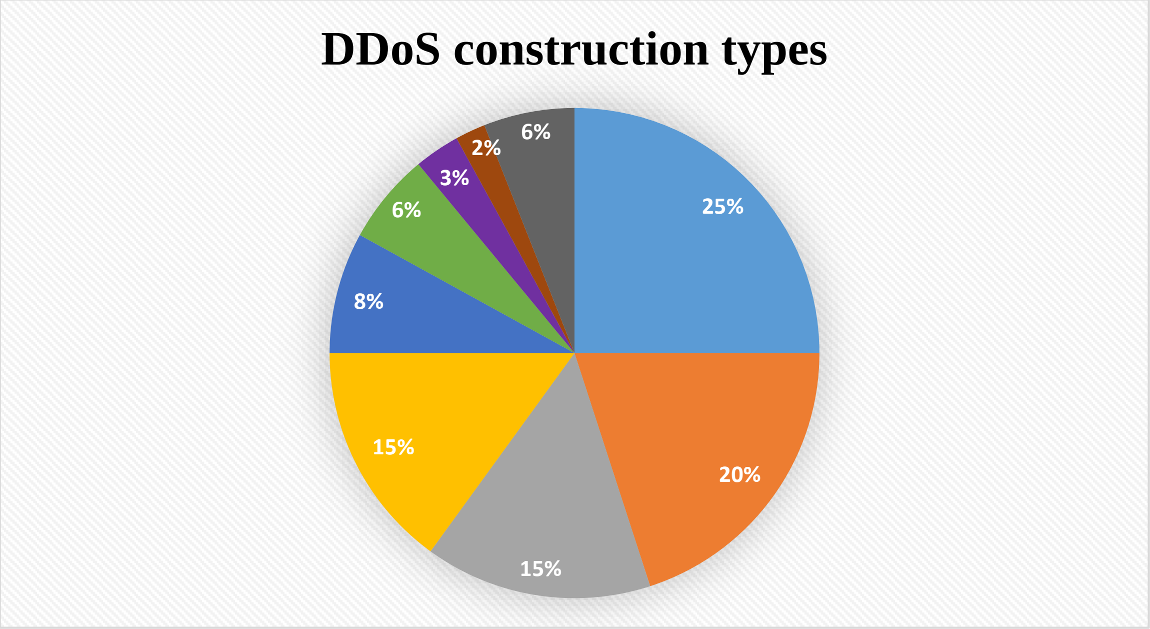


Figure 1.2. Proportion of Victims Subjected to DDoS Attacks[2]

When creating a new website, developers can either use existing platforms, specifically CMS (Content Management Systems), or build everything from scratch. However, small companies often prefer to use pre-made tools.

[2] https://mgl.gogo.mn/newsn/images/ck/2014/05/15/08-094156-553024301.jpeg

Key Functions of a CMS:

- Providing content creation tools and facilitating collaboration on content;
- Managing content: including storage, version control, access control, document workflow management, and more;
- Publishing content: enabling seamless and efficient distribution;
- Presenting information in a user-friendly format for search and navigation.

CMS platforms typically have vulnerabilities that can be found online. Each year, more new CMS updates are released, but with these updates, new weaknesses also emerge.

- The most popular methods for protecting CMS platforms from various attacks include:
- Protection Against XSS Injections: Implementing security measures to prevent cross-site scripting attacks by sanitizing and validating user inputs.
- Hiding Excess Information: Limiting the exposure of system and platform details to reduce the attack surface.
- Mandatory Use of SSL: Enforcing HTTPS to secure data transmission between the server and users.
- Protecting Root Files: Securing critical configuration files (e.g., .htaccess, wp-config.php) from unauthorized access.
- Preventing Spammers and Bots: Utilizing CAPTCHA, honeypots, or other anti-spam mechanisms.
- Using Plugins to Block Malicious URL Requests: Installing and configuring plugins to detect and block harmful requests.
- Preventing Directory Browsing on the Server: Disabling directory listing to restrict unauthorized users from viewing server directories.

There are several protection technologies available to ensure data confidentiality, including:

- WEP Protocol: Enables encryption of transmitted data using the RC4 algorithm. However, due to numerous vulnerabilities, it is easily compromised by hackers. Recognizing this, the WPA (Wi-Fi Protected Access) standard was introduced in 2003 as a more secure alternative.
- WPA2 Protocol: Adopted in June 2004 and mandatory for all certified Wi-Fi devices starting March 13, 2006. WPA2 operates in two authentication modes: Personal and Enterprise. This protocol prevents key reuse, making it significantly more secure than its predecessors.
- MAC Address Filtering: Supported by all modern access points, this feature effectively enhances network security. Filtering can be implemented in three ways:

- The access point allows connections from any MAC address.
- The access point permits connections only from MAC addresses listed in a trusted list.
- The access point denies connections from MAC addresses included in a “blacklist”.
- SSID Hiding: Provides a mode for concealing the network's identifier, adding an extra layer of security by making the network less visible to unauthorized users.

Protecting websites is one of the most critical tasks for web developers. Failure to prioritize this can lead to significant financial and political losses.

It is well-known that no security software can provide complete protection against cyber threats. Identifying potential issues in advance helps prepare and plan measures to address them before they arise.

Here are some critical issues to consider:

Depending on your requirements, you may need to install multiple software programs to meet all your cybersecurity needs. For example, installing an antivirus program does not protect against hacking attacks, as it is not a firewall.

Another important issue is that the convenience provided by software products can both benefit and pose risks. Systems and websites can be easily breached, allowing unauthorized users to alter data.

As cybercrime tactics evolve, software products designed to ensure information security must be continuously updated and improved. The latest trends in software development play a crucial role in this area.

Continuous Assessment of Risk and Trust (CARTA) is a new approach for ongoing, regular evaluation of users. Essentially, this process uses real-time risk and trust assessment within an IT environment. For example, if a user has a minimal risk of privilege abuse, they may be granted extended access rights. This method is focused on enabling companies to make informed decisions regarding their security posture.

A customized security policy allows for proactive preparation against potential threats. It provides organizations with more effective solutions, as the approaches are tailored to meet their specific needs.

In 2018 alone, 21 incidents were reported where major businesses and corporations, including Facebook, British Airways, T-Mobile, Cathay Pacific, and Marriott Hotels, experienced security breaches, compromising millions of user accounts and customer personal information. Yahoo reported a breach involving data from 1.5 billion accounts. This suggests that even global corporations with the strongest cybersecurity measures are not immune to attacks.

Kaspersky Lab blocked nearly 800 million attacks originating from online sources across 194 countries.

In the first quarter of 2018, the same cybersecurity company, Kaspersky, detected 1.3 million malicious installation packages downloaded to mobile devices.

It was identified that there were over 282 million unique URLs flagged as malicious. Additionally, more than 200,000 computers were compromised by malware designed to steal money through online access to bank accounts. [1-5].

In today's digital world, where financial transactions are conducted online, critical data is stored in the cloud, and connected devices are not only linked to the internet but also to each other, the need for defense and protection tools is paramount. One might think that small businesses don't attract hackers' attention, but in reality, hackers often target the most vulnerable. It has been found that 43% of cyberattacks are aimed at small businesses. It is crucial to seriously consider investing in a robust cybersecurity program that can proactively implement preventative measures and protect systems, devices, and the most valuable data.

Conclusion. In conclusion, due to the ongoing cyberattacks on websites (and considering that all malicious actions are punishable by law), developers must prioritize security during the creation process. There are many methods for protecting websites, but regardless of their effectiveness, vulnerabilities must be regularly checked. Therefore, the key advice for website developers and administrators is to repeatedly assess and verify the reliability and security of their websites.

Used literature

1. Fazilov, S. X., Mahkamov, A. A., & Jumayev, T. S. (2018). Algorithm for extraction of identification features in ear recognition. Информатика: проблемы, методология, технологии, 3-7.
2. Mahkamov, A. A., Jumayev, T. S., Tuhtanazarov, D. S., & Dadamuxamedov, A. I. (2024). Using AdaBoost to improve the performance of simple classifiers. In Artificial Intelligence, Blockchain, Computing and Security Volume 2 (pp. 755-760). CRC Press.
3. Zhumaev, T.S., Mirzaev, N.S., & Makhkamov, A.S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27),
4. Маҳкамов, А. А., & Инадуллаев, Х.Ў.Ў. (2021). Сравнительный анализ биометрических систем в обеспечении информационной безопасности. Universum: технические науки, (12-1 (93)), 32-37.
5. Махкамов А. А. Алгоритмы идентификации личности человека по изображению ушных раковин //Исследования технических наук. – 2015. – №. 4. – С. 28-32.
6. Tuhtanazarov, D., Xodjayeva, M., Jumayev, T., & Mahkamov, A. (2022, June). Computational algorithm and program for determining the indicators of wells

based on processing of information of oil fields. In AIP Conference Proceedings (Vol. 2432, No. 1, p. 060021). AIP Publishing LLC.

7. Zhumaev, T. S., Mirzaev, N. S., & Makhkamov, A. S. (2015). Algorithms for segmentation of color images based on the selection of strongly coupled elements. Studies of Technical Sciences,(4), 22(27), 4.
8. Жумаев, Т. С., Мирзаев, Н. С., & Махкамов, А. С. (2015). Алгоритмы сегментации цветных изображений, основанные на выделение сильносвязанных элементов. Исследования технических наук, (4), 22-27.
9. Махкамов, А. А., & Дадамухамедов, А. И. (2022). Алгоритм выделения области ушных раковин при распознавании личности. Universum: технические науки, (5-1 (98)), 14-17.
10. Махкамов, А. А. (2015). Алгоритмы идентификации личности человека по изображению ушных раковин. Исследования технических наук, (4), 28-32.