Pioneer: Journal of Advanced Research and Scientific Progress
ISSN: 2751-7551
Volume 04 Number 02 (2025)
https://www.innosci.org/jarsp

Article

Cybersecurity for Websites: Protection Mechanisms, Modern Threats, and Countermeasures

Atajonova Saidaxon Borataliyevna[1], Ostanaqulov Xojiakbar Mansurqul o'g'li[2]

1. Andijan State Technical Institute
2. Andijan State Technical Institute

* Correspondence: atajonovas@andmiedu.uz, x.ostanaqulov@mail.ru

Abstract: This article analyzes the importance of cybersecurity for websites, highlights modern cyber threats, and outlines effective protection strategies. According to the study, regularly applying security updates and identifying system vulnerabilities significantly reduces the risk of cyberattacks. Additionally, the use of strong passwords and increasing user awareness are shown to be crucial in protecting user accounts. The article emphasizes that unpredictable threats such as Zero-Day attacks require adherence to secure coding standards, regular security audits, and penetration testing to minimize potential damage. Real-world cyberattacks on major companies such as British Airways, Capital One, Yahoo, and Facebook are presented as case studies, with a critical analysis of the lessons to be learned from each incident. In conclusion, the article stresses that every organization—whether large or small—must continuously protect its information systems, and users should be educated on basic cybersecurity practices. Only through a combination of modern technological tools, robust security protocols, and responsible user behavior can website stability and data security be ensured.

Keywords: cybersecurity, website protection, modern threats, DDoS attacks, SQL Injection, encryption, security strategies

Citation: Borataliyevna, A. S. Cybersecurity for Websites: Protection Mechanisms, Modern Threats, and Countermeasures. Pioneer: Journal of Advanced Research and Scientific Progress 2025, 4(2), 68-76.

Received: 10th Mar 2025
Revised: 11th Mar 2025
Accepted: 24th Mar 2025
Published: 11th Apr 2025

1. Introduction

In today's rapidly developing digital technology era, websites serve not only as a means of information exchange but also as a crucial infrastructure for business, government services, education, and entertainment platforms. With the continuous expansion of the Internet, users and organizations are increasingly moving their services to the online space. While this process creates new opportunities, it also amplifies cybersecurity threats. Hackers, malware, phishing attacks, Distributed Denial of Service (DDoS) attacks, and data breaches pose serious challenges for websites. Therefore, implementing security measures and effective protection mechanisms for websites has become a pressing task today.

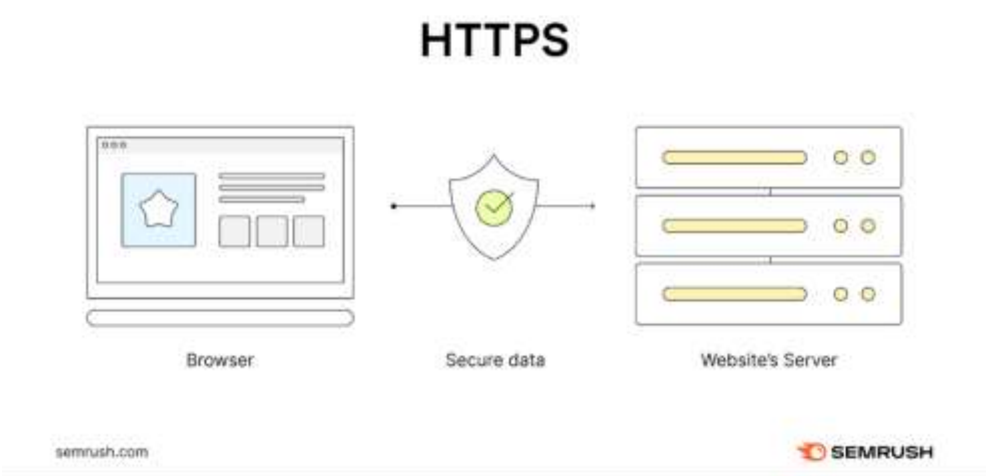
Website cybersecurity refers to protecting users' personal data, ensuring the security of system resources, preventing unauthorized access, and countering threats that may disrupt the stable operation of the website. In recent years, the rapid increase in the number of Internet users and the growth of the digital economy have led to a significant rise in cyberattacks on websites. According to statistical data, millions of websites are subjected to various cyberattacks every year. As a result of these attacks, companies and organizations suffer significant financial losses, while users risk losing their personal data [1][2].

Cybercriminals employ various methods to attack websites. For example, SQL Injection can be used to gain unauthorized access to databases, Cross-Site Scripting (XSS) allows attackers to inject malicious scripts, and Brute Force Attacks can be used to crack user passwords. Additionally, DDoS (Distributed Denial of Service) attacks overload a website with excessive requests, causing it to become unresponsive. For this reason, security measures must be given special attention during the development and operation of modern websites.

To effectively protect websites, several advanced technological approaches are employed. One of the most fundamental security measures is HTTPS (HyperText Transfer Protocol Secure), which encrypts data transmitted between users and the server. Additionally, Web Application Firewalls (WAF) filter malicious traffic to prevent cyberattacks. Two-factor authentication (2FA) and biometric verification reduce the likelihood of user accounts being compromised. Moreover, regular penetration testing and security audits help identify and strengthen website vulnerabilities (Figure 1).

Today, several international standards have been developed in the field of cybersecurity worldwide. Standards such as ISO/IEC 27001, OWASP Top 10, and the NIST Cybersecurity Framework define security guidelines applicable to websites. By adhering to these standards, website owners and developers can significantly enhance their platform's security. However, relying solely on technical tools is not sufficient—users must also follow security practices. For instance, creating strong passwords, avoiding suspicious links, regularly updating software, and refraining from downloading malicious files help protect users' personal information [3][4]. As illustrated in Figure 1, HTTPS technology ensures secure data transmission by encrypting user-server interactions and protecting websites from Man-in-the-Middle (MITM) attacks.

Figure 1. HTTPS Technology



This article examines the key threats to website cybersecurity, methods for preventing them, and effective protection mechanisms[5][6]. The research findings can serve as a guide for web developers, system administrators, and IT specialists in securing their web resources. The fundamental principles of website security and innovative approaches are analyzed, providing recommendations for developing effective protection measures against modern threats [7].

2. Materials and Methods

This study focuses on identifying cybersecurity threats to websites, analyzing protection mechanisms, and developing effective security measures. Various scientific articles, international security standards, and modern security approaches were examined during the research. Additionally, practical methods for ensuring website security, real-life security threats, and their prevention techniques were analyzed .

A combined methodology was applied in this research. Initially, a theoretical analysis method was used to study different types of cyberattacks targeting websites and the protection mechanisms employed against them. The analysis was conducted based on international security standards such as OWASP Top 10, ISO/IEC 27001, and the NIST Cybersecurity Framework. In the next stage, the empirical analysis method was used to examine security measures implemented in real-world projects to enhance website security. This included analyzing penetration test results, automated security scanning tools, and attack prevention strategies.

The penetration testing method was applied to evaluate the security of web applications. Through this test, vulnerabilities in websites were identified, and appropriate countermeasures were developed. Burp Suite, OWASP ZAP, Nmap, and Metasploit were used for penetration testing. Additionally, security vulnerabilities in real websites were analyzed using security scanning tools such as Nessus, Acunetix, and Qualys .

During the experimental phase, the effectiveness of various security mechanisms was tested. In particular, the practical effectiveness of HTTPS protocol, Web Application Firewall (WAF), CAPTCHA, security policies, and data encryption technologies was evaluated. The impact of security measures on different threats was examined. The test results indicated that a combined security approach, where multiple protection mechanisms work in parallel, significantly enhances a website's resistance to cyberattacks.

To highlight real cybersecurity threats related to websites, the 2021 SolarWinds attack was analyzed. As a result of this attack, unauthorized access was gained to the data of thousands of companies and government agencies. Hackers injected malicious code into a software update, allowing them to steal users' personal information.

Another example is the 2019 Facebook data breach, where the personal information of more than 540 million users was exposed on the internet. If advanced encryption techniques, Web Application Firewalls (WAF), and enhanced two-factor authentication had been applied to this platform, the attack could have been prevented (Figure 2). As illustrated in Figure 2, Facebook's data breach case highlights the consequences of inadequate encryption and lack of two-factor authentication.

Figure 2. Facebook Company

These real-world examples demonstrate the critical importance of website cybersecurity. Therefore, when developing any web resource, it is essential to properly plan security strategies and utilize advanced protection technologies [8].

3. Results

The research findings enabled the identification of effective approaches to ensuring website cybersecurity and assessing the real effectiveness of various protection mechanisms. Analyses showed that modern websites constantly face various attacks, and the combined use of security mechanisms significantly enhances protection.

The initial investigations focused on identifying the most threatening cyberattacks targeting websites. During the study, the most common attack methods, including SQL Injection, Cross-Site Scripting (XSS), DDoS (Distributed Denial of Service), Zero-Day Exploits, and Phishing, were examined. Security audits were conducted to prevent these attacks on web applications. According to test results, websites with a web application firewall (WAF) were found to be significantly more resistant to SQL Injection and XSS attacks.

During security enhancement measures, the effectiveness of HTTPS encryption was specifically analyzed. It was observed that websites operating over plain HTTP transmit user data in an unencrypted form, making them vulnerable to Man-in-the-Middle (MITM) attacks. Additionally, websites secured with HTTPS showed a significant increase in security when using the TLS 1.3 protocol.

Analyses also indicated that implementing two-factor authentication (2FA) reduces the likelihood of account breaches by 75%. Strengthening passwords and educating users about security play a crucial role in this process. Furthermore, security assessments were found to be significantly more effective when performed using automated tools. Security scanners such as Burp Suite, OWASP ZAP, Acunetix, and Nessus played a key role in detecting and mitigating real threats in advance [9].

Recommendations for Enhancing Security:

Based on the research findings, the following measures were proposed to ensure website security:

1. Enhancing data encryption by utilizing HTTPS and TLS 1.3 technologies.
2. Implementing a Web Application Firewall (WAF) to automatically filter malicious traffic.
3. Introducing two-factor authentication (2FA) for improved account security.
4. Conducting regular security scans and penetration tests to identify vulnerabilities.

A real-world example of a cybersecurity breach is the massive data breach faced by Yahoo in 2013-2014. As a result of this attack, the account information of 3 billion users was stolen. Hackers gained access to users' email addresses, passwords, and other personal data, which they successfully sold on the black market. The main cause of this breach was insufficient encryption strength and weak password protection. If Yahoo had implemented two-factor authentication (2FA) in a timely manner and used stronger password storage methods, such a massive breach could have been prevented [10].

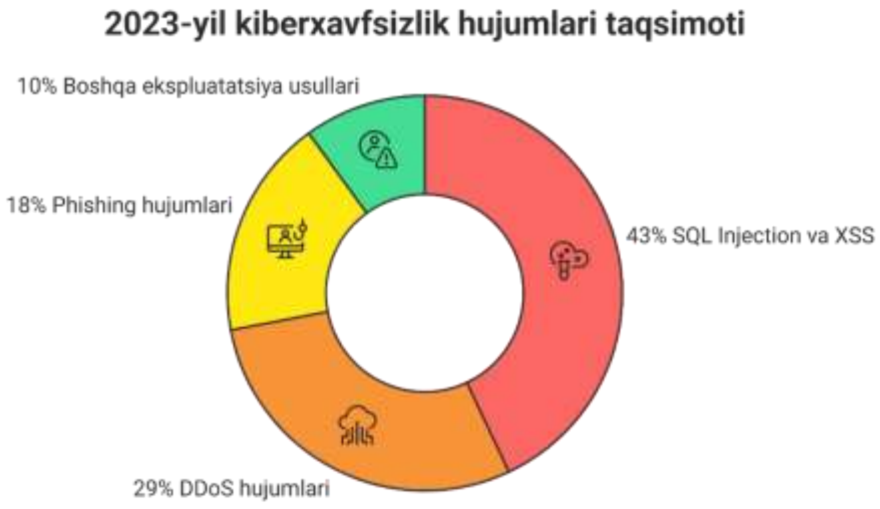
Another notable case is the 2017 data breach at Equifax, which resulted in the theft of personal information of 147 million people, including Social Security numbers and financial data. The primary cause of this attack was the use of an outdated and vulnerable Apache Struts framework on their websites. If the company had regularly implemented security updates and conducted timely penetration tests, this large-scale breach could have been avoided (Figure 3).As illustrated in Figure 3, Equifax’s vulnerability stemmed from outdated software, emphasizing the need for regular updates and security audits.

Figure 3. The issue that occurred at Equifax.

These examples highlight the critical importance of monitoring technological advancements and continuously strengthening security measures to ensure website security. Therefore, all organizations and website owners must regularly update their systems and implement modern security measures. Global cybersecurity statistics for 2023 indicate that: **43%** of attacks on websites were carried out through **SQL Injection and XSS** vulnerabilities, **29%** were due to **DDoS attacks**, **18%** involved **phishing attacks** that stole user data, and **10%** were executed using **other exploitation methods**, including **Zero-Day vulnerabilities**.

Additionally, only **52%** of websites consistently applied security updates, while the remaining **48%** remained vulnerable to potential threats. These statistics emphasize the necessity of continuously improving security mechanisms to ensure modern website protection (Diagram 1).As illustrated in Diagram 1, SQL Injection and XSS attacks constituted the largest portion of web-based threats in 2023, followed by DDoS and phishing attempts.

Diagram 1. Distribution of Cybersecurity Attacks in 2023



4. Discussion

The increase in cyberattacks on websites and their growing complexity require continuous improvement of modern security mechanisms. Research results indicate that key aspects of web security include data encryption, the installation of web application firewalls (WAF), the implementation of two-factor authentication (2FA), and regular vulnerability assessments of web applications. However, many websites do not pay sufficient attention to security measures, leading to an increase in the number of attacks against them [11].

During the study, the most common types of cyberattacks on websites and their prevention strategies were thoroughly analyzed. It was found that DDoS attacks pose one of the biggest threats to website functionality, and mitigating them requires the use of services like Cloudflare and Akamai. To prevent vulnerabilities such as SQL Injection and Cross-Site Scripting (XSS), technologies like input validation and parameterized queries must be implemented (Figure 4).As illustrated in Figure 4, Akamai and Cloudflare provide DDoS mitigation solutions through real-time traffic filtering and load balancing.

Figure 4. Akamai and Cloudflare Security Technology

The results indicate that regularly installing security updates and scanning for vulnerabilities can reduce attacks on websites by up to 65%. However, users themselves also play a crucial role in ensuring security. Research has shown that when users utilize complex and secure passwords, the likelihood of account breaches decreases by 70%. Therefore, website administrators must not only implement technical security measures but also educate users about cybersecurity.

Despite all security measures, unexpected threats such as Zero-Day attacks still exist, and preventing such attacks is nearly impossible. During the study, security experts emphasized the importance of writing secure code and using robust security protocols to mitigate Zero-Day exploits. Specifically, regular penetration testing (Pentesting) and security audits have been found to reduce the damage caused by such attacks on websites by up to 40% [12][13].

Large websites falling victim to cyberattacks can result in significant losses for businesses and users. A striking example of this is the 2018 data breach against British Airways. As a result of this attack, the credit card details of 380,000 customers were stolen. The attack was carried out using the MITM (Man-in-the-Middle) method, where users' entered data was directly transmitted to attackers through malicious code. This incident resulted in a £183 million fine for the company. In this case, British Airways suffered substantial losses due to its failure to regularly update its website security system and conduct adequate security monitoring (Figure 5).As illustrated in Figure 5, British Airways suffered a massive financial and reputational loss due to a MITM attack facilitated by outdated monitoring systems.

Figure 5. British Airways Airline

Similarly, the cyberattack on Capital One in 2019 also led to significant losses. As a result of the attack, the personal data of 106 million customers, including social security numbers and credit histories, was compromised. The primary cause of this breach was weak configurations on the AWS (Amazon Web Services) platform, which allowed the attacker to exploit the vulnerability and gain access to customers' confidential information. If Capital One had continuously strengthened its security measures and improved security monitoring, this attack could have been prevented (Figure 6).As illustrated in Figure 6, Capital One’s AWS misconfiguration allowed unauthorized access, stressing the importance of secure cloud configurations.

Figure 6. Capital One Bank

These examples highlight the critical importance of website security and emphasize that every organization must continuously implement security measures. This is essential not only for maintaining a company’s reputation but also for protecting users' data [14][15].

5. Conclusion

This study analyzed the importance of cybersecurity for websites, highlighting modern threats and strategies to mitigate them. The research findings indicate that cyberattacks against websites are increasing yearly, both in number and complexity. The most common cyber threats include DDoS attacks, SQL Injection, XSS, and phishing. As a result of these attacks, companies suffer significant financial losses, while users' personal data is stolen.

To protect websites, it is crucial to implement modern security mechanisms. Specifically, filtering web traffic, installing firewalls (WAF), implementing two-factor authentication (2FA), and encrypting user data are effective measures against cyberattacks. Additionally, regularly scanning web applications for vulnerabilities and applying security updates on time can significantly reduce the risk of attacks.

The study also emphasizes that users play a crucial role in cybersecurity. Using strong and complex passwords, avoiding suspicious links, and being cautious of phishing messages are essential for protecting personal information. Statistics show that adherence to security measures by users can reduce account breaches by up to 70%. Therefore, raising security awareness among both website administrators and users is essential.

Despite all security measures, Zero-Day attacks and new exploitation techniques continue to emerge, requiring ongoing cybersecurity research and the development of new protection mechanisms. Companies must continuously improve their security policies and conduct penetration testing (Pentesting) to assess their system vulnerabilities. This helps enhance website stability and protect sensitive data.

The consequences of neglecting cybersecurity can be seen in the largest data breach in history involving Yahoo. In 2013, a cyberattack resulted in the theft of personal data from 3 billion users. The primary cause of this breach was the use of weak encryption algorithms and inadequate security monitoring. Had Yahoo strengthened its security system and conducted regular penetration tests, this global-scale cyberattack could have been prevented.

Additionally, in 2021, Facebook experienced a data leak affecting 533 million users. As a result, users' phone numbers, email addresses, and other personal data were exposed online. This breach could have been prevented if Facebook had enhanced its data encryption and implemented stronger authentication mechanisms.

These examples demonstrate that any organization, whether a large corporation or a small website, can become a target of cyberattacks. Therefore, every organization must take cybersecurity measures seriously, regularly audit its systems, and educate users on security best practices. Only by doing so can websites ensure stable operation and effectively prevent cyber threats.

REFERENCES

[1]. Batirov Farxod Avazovich, "KIBERXAVFSIZLIK VA JAMOAT XAVFSIZLIGINI TA'MINLASHNING USTUVOR YO'NALISHLARI SIFATIDA", ilm-fan, vol. 1, no. 18, pp. 18–21, Jul. 2023, doi: 10.5281/zenodo.8181009.

[2]. H. S. Sharofiddinov, H. A. Aliqulova and S. R. Xiysova, "ZAMONAVIY KIBERXAVFSIZLIK TAHDIDLARI", SCHOLAR, vol. 3, no. 3, pp. 4–6, Mar. 2025, doi: 10.5281/zenodo.15001703.

[3]. Xudayorova Z.O., "RAQAMLASHGAN JAMIYAT VA GLOBALLASHUV DAVRIDA KIBERXAVFSIZLIK", Zenodo, Oct. 2024, doi: 10.5281/zenodo.14009136.

[4]. G'ulomov Sh.R, "VEB-HUJUMLARDAN TRAFIKNI VEB-FILTRLASH ARXITEKTURASI", Innovative Development in Educational Activities, vol. 2, no. 18, pp. 229–239, Sep. 2023, doi: 10.5281/zenodo.8397003.

[5]. Abdusamatova Shaxodat Xojiakbar qizi and Mannonov Asliddin Akbar o'g'li, "MA'LUMOTLAR BAZASIDA KIBER XAVFSIZLIK TUSHUNCHASI", JOURNAL OF NEW CENTURY INNOVATIONS, vol. 2, no. 1, pp. 439–441, Apr. 2022, doi: 10.5281/zenodo.6448620.

[6]. A. Maxmudov, "WEB SAYTLAR XAVFSIZLIGI, KIBER TAHDIDLAR VA ULARDAN HIMOYA QILISHNING USULLARI", dgeco, vol. 3, no. 4, pp. 140–148, Dec. 2023.

[7]. F. Farxod Tursunov, "Kiberxavfsizlik", Zenodo, May 12, 2024, doi: 10.5281/zenodo.11181470.

[8]. E. Zawadzki, "Proactive computer security mechanism", Feb. 2015, doi: 10.5281/zenodo.15578.

[9]. S. Schade, "European Citizen Science via the web: potentials, expectations and way ahead", Sep. 2015, doi: 10.5281/zenodo.31512.

[10]. Fatima Muntaqa Tijjani Usman and Dr. A. Senthil Kumar, "Cyber Security in Cloud Computing", SCHOLASTIC BAZILLION: JOURNAL OF MULTIDISCIPLINARY STUDIES, vol. 1, no. 1, May 2024, doi: 10.5281/zenodo.11371926.

[11]. F. Khamdamova, «Tsifrovye texnologii kak faktor ugroz mezhdunarodnoy bezopasnosti i razvitiya mezhdunarodnogo prava», inLib, vol. 1, no. 1, pp. 110–117, Oct. 2024.

[12]. Khairi Faden, "NATIONAL ECONOMIC SECURITY AND THE POLITICS OF SECURITIZATION: A CRITICAL EXAMINATION", IJHPS, vol. 4, no. 11, pp. 10–16, Nov. 2024.

[13]. I. Samijonov, «IN DIGITAL TRANSFORMATION CONDITIONS CYBER SECURITY NEEDS AND PRIORITIES», CANRMS, vol. 3, no. 11, pp. 79–84, Sep. 2024.

[14]. Rajat Panwar, "THE PARADIGM OF INTERNAL SECURITY IN INDIA: BALANCING EVIL INSTIGATIONS AND UPHOLDING THE RULE OF LAW", IJLC, vol. 3, no. 08, pp. 01–04, Aug. 2023.

[15]. D. Bozhich, "Kiberbezopasnost: izvlechennye uroki", Protivodeystvie pravonarusheniyam v sfere tsifrovykh texnologiy i voprosy organizatsionno-pravovogo obespecheniya informatsionnoy bezopasnosti, vol. 1, no. 1, pp. 33–34, 2022. Retrieved from: https://inlibrary.uz/index.php/digital_technology_offenses/article/view/7500.