MECHANISMS FOR PROTECTION AGAINST ATTACKS IN WEB SYSTEMS

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

Abstract

The main information security threats encountered in the framework of modern web systems architecture and effective protection mechanisms against them are analyzed. With the widespread popularity of web applications, the issue of ensuring their security level has become one of the pressing problems. The article examines the main mechanisms used to increase the level of protection of web applications, including firewalls, IDS, IPS systems, SSL/TLS protocols, web application firewalls, access control, security monitoring and incident response systems.

Keywords : firewall , IDPS , SSL/TLS , WAF , XSS, SQL injection, access control, Security patching and updating, Security monitoring and incident response.

Several mechanisms can be implemented to protect web systems from threats. These mechanisms aim to prevent unauthorized access, data corruption, and other malicious actions. There are several general methods that can be used to protect web systems from threats.

Firewalls act as a barrier between a trusted internal network and an untrusted external network, such as the Internet. They monitor and control incoming and outgoing network traffic based on predefined security rules. By filtering potentially malicious traffic and blocking unauthorized access attempts, firewalls help protect web systems from external threats.

Intrusion Detection and Prevention Systems (IDPS): IDPS are security systems that monitor network traffic for suspicious activity or specific attack patterns. They can detect and prevent various types of attacks, including malware infections, unauthorized access attempts, and denial-of-service (DoS) attacks. IDPS can be configured to automatically respond to detected threats by blocking or mitigating them.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Encryption: SSL/TLS encryption protocols provide secure communication over the internet by encrypting data transmitted between a web server and a client browser. This helps protect sensitive information such as login credentials, payment information, and personal information from being intercepted or modified by attackers.

Web Application Firewalls (WAFs): WAFs are specifically designed to protect web applications from a variety of attacks, including SQL injection, cross-site scripting (XSS), and remote file injection. WAFs analyze incoming HTTP requests and apply security rules to block

or filter out malicious traffic. They can also provide additional protection against specific vulnerabilities in web applications.

IDS/IPS (Intrusion Detection System) is the process of monitoring network traffic and analyzing it for signs of possible intrusions, such as exploit attempts and events that could be threats to your network. Intrusion prevention, on the other hand, is the process of performing intrusion detection and then stopping the detected events, usually by dropping packets or terminating sessions. These security measures intrusion detection systems (Intrusion Detection Systems-IDS) and Intrusion prevention systems (IPS) are part of the network security measures taken to detect and stop intrusions.

Access Control: Implementing strong access controls is essential for securing web systems. This includes implementing strong passwords, implementing role-based access controls, and regularly reviewing and revoking unnecessary privileges. By ensuring that only authorized individuals have access to sensitive resources and functions, the risk of unauthorized access and data breaches can be significantly reduced.

Security Patching and Updates: Regular updates and patches for web applications, operating systems, and other software components are essential to ensure the security of web systems. Software vendors often release updates to address known vulnerabilities and security flaws. By applying these updates promptly, web systems can be protected from the latest threats.

Security Monitoring and Incident Response: Implementing a robust security monitoring system allows you to detect and respond to security incidents in real time. This includes monitoring system logs, network traffic, and user activity for any signs of suspicious or malicious behavior. Having an incident response plan ensures that security incidents are promptly detected, prevented, and mitigated to minimize potential damage.

User awareness and education: Educating users about security best practices, such as avoiding suspicious links and attachments, using strong passwords, and being cautious when sharing sensitive information, is essential to protecting web systems. Users should be aware of common threats such as phishing attacks and know how to report any suspicious activity or potential security incidents.

By implementing these mechanisms and following secure practices, web systems can be better protected from a wide range of threats. However, it is important to note that no security measure is foolproof, and a layered defense approach should be adopted to address multiple attack vectors and adapt to evolving threats. Regular security assessments and audits should be conducted to identify potential vulnerabilities or weaknesses in the system.

To protect against malware attacks, individuals and organizations should follow the following best practices:

- keep software up to date;
- use reputable security software;
- Be careful with email attachments and downloads;
- enable firewalls;
- training employees or users;
- Back up your data regularly;
- implement strong passwords and multi-factor authentication;

By following these preventive measures and remaining vigilant, individuals and organizations can reduce the risk of falling victim to malware attacks and protect their valuable data and systems.

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

Input validation and output encoding: Implement strong input validation mechanisms to ensure that user-provided data is properly sanitized and validated. Additionally, use output encoding techniques to prevent the execution of malicious scripts in users' browsers.

Content Security Policy (CSP): Implement a CSP that defines the trusted content sources and scripts that a web page can load. This helps mitigate the impact of XSS attacks by restricting the execution of malicious scripts.

Regular security updates: Keep your web applications, frameworks, and plugins up-to-date with the latest security patches. This helps address known vulnerabilities that attackers can exploit.

Web Application Firewalls (WAF): Implement a WAF that can detect and block XSS attempts. A WAF can analyze incoming requests and block requests that contain suspicious or malicious scripts.

Security testing and code reviews: Conduct regular security testing, including vulnerability assessments and penetration testing, to identify and address potential XSS vulnerabilities. Also, review your code to ensure that secure coding practices are being followed.

By implementing these preventive measures, individuals and organizations can significantly reduce the risk of XSS attacks and protect their web applications and users' sensitive data.

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

- csrf tokens;
- samesite attribute;
- strict referrer policy;
- multi-factor authentication (mfa);
- increasing user awareness and education.

Implement CSRF tokens as part of your web application's authentication and session management processes. These tokens are unique to each user session and are included in all requests that modify data or perform sensitive operations. The server verifies the authenticity of the token before processing the request, preventing unauthorized actions.

In general, the following security measures should be taken to ensure system protection.

- regular software updates and patches to address known vulnerabilities;
- strong authentication mechanisms such as multi-factor authentication;
- encrypting sensitive data during transmission and storage;
- robust access controls and user permissions to limit unauthorized access;
- web application firewalls and intrusion detection systems to monitor and prevent attacks;
- employee training and awareness programs to educate users about potential threats and safe online practices;
- creating regular backups of important data to ensure its availability in the event of a system failure or malfunction;
- Continuous monitoring and logging of web system activity to identify.

In addition to plugins for web browsers, there are many other types of plugins, such as:

- **Audio plug-ins** : Audio plug-ins are used in digital recording studios to create specific sound effects or simulate musical instruments;
- **Graphics and video plug-ins** : Graphics programs like Photoshop use plug-ins to add new effects or support specific files;
- **Social plugins** : These plugins can be embedded on your website so that the site connects and integrates with popular social networks such as Facebook or Twitter;
- **Plug-ins for integrated development environments** : You can use plug-ins to support additional programming languages in integrated development environments (IDEs). Some IDEs, such as Microsoft Visual Studio, can be fully integrated into other programs using plug-ins;
- **Email Plugins** : Email plugins are often used to add encryption methods, tracking features, or pre-built templates to email clients;
- **CMS plugins** : Content management systems like WordPress are very popular, mainly because there are thousands of plugins available for these systems. There is a specific plugin for almost every possible feature.

List of used literature

1. Хамдамов Р.Х., Керимов К.Ф. Математический метод обнаружения XSS атак на web приложения. Доклады Республиканской научнотехнической конференции

«Современное состояние и перспективы применения информационных технологий в управлении». – Самарканд, 2019. – С.419-422.

2. Ibrohimov A.R. Veb serverlardagi axborotni tarmoq hujumlaridan himoyalash usullari, International conference Recent advances in intelligent information and communication technologies “ISPC-2022” Tashkent -2022, pp. 360-364.
3. J. Liang, W. Zhao, W. Ye Anomaly-based Web attack detection: a deep learning approach Proceedings of the 2017 VI International Conference on Network, Communication and Computing, Association for Computing Machinery, New York, NY, USA (2017), pp. 80-85.
4. H. Mac, D. Truong, L. Nguyen, H. Nguyen, H.A. Tran, D. Tran Detecting attacks on Web applications using autoencoder Proceedings of the Ninth International Symposium on Information and Communication Technology, Association for Computing Machinery, New York, NY, USA (2018), pp. 416-421.
5. Ibrohimov A.R . Tarmoq hujumlarini aniqlash usul va algoritmlari, International conference Recent advances in intelligent information and communication technologies “ISPC-2022” Tashkent -2022, pp. 352-356.