CSRF (CROSS-SITE REQUEST FORGERY) HUJUMI

АТАКА CSRF (CROSS-SITE REQUEST FORGERY)

CSRF (CROSS-SITE REQUEST FORGERY) ATTACK

Sobirjonov Behzod Qahramon o‘g‘li
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasi katta o‘qituvchisi
behzodbekqahramonovich@gmail.com
Komilov Islombek Nosirjon o‘g‘li
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalar yo‘nalishi
2-kurs talabasi
komilovislombek07.06@gmail.com

Аннотация

В данной статье проводится всесторонний анализ атаки CSRF (Cross-Site Request Forgery), которая считается одной из наиболее актуальных проблем в безопасности веб-приложений. Данный тип атаки характеризуется незаконным использованием активной сессии пользователя в системе, при котором пользователь, сам того не осознавая, вынужден отправлять вредоносные запросы. В результате могут возникнуть серьёзные риски, такие как изменение данных учётной записи, выполнение финансовых операций или других важных действий.

В ходе исследования подробно рассматриваются причины возникновения CSRF-атак, в частности недостатки процессов аутентификации и авторизации в веб-приложениях, уязвимости управления сессиями, а также случаи неправильного использования доверия пользователя. Кроме того, объясняются различные виды данной атаки и способы её реализации с примерами.

Ключевые слова: *CSRF-атака, веб-безопасность, сессия, аутентификация, авторизация, вредоносный запрос, куки, токен, доверие пользователя, кибератака*

Annotation

This article provides a comprehensive analysis of the CSRF (Cross-Site Request Forgery) attack, which is considered one of the most critical issues in web application security. This type of attack is characterized by the unauthorized use of a user’s active session in the system, where the user is tricked into unknowingly sending malicious requests. As a result, serious risks may arise, such as changing account information, performing financial transactions, or executing other important actions.

During the research, the causes of CSRF attacks are thoroughly examined, including weaknesses in authentication and authorization processes in web applications, vulnerabilities in session management, and cases of exploiting user trust. In addition, different types of this attack and methods of its execution are explained with examples.

Keywords: *CSRF attack, web security, session, authentication, authorization, malicious request, cookies, token, user trust, cyberattack*

In today’s rapidly evolving digital era, web applications have deeply penetrated almost all areas of human life. Banking services, electronic payment systems, online shopping platforms, social networks, as well as various public and private services are largely carried out through web applications. Such widespread use significantly increases the demand for information security.

One of the most common and serious threats to web application security is the CSRF (Cross-Site Request Forgery) attack. This type of attack is based on exploiting an active user session in the browser to send unauthorized requests on behalf of the user. In other words, when a user is logged into a system, an attacker can deceive them into automatically executing malicious requests. As a result, the user may unknowingly change their password, transfer money, or perform other sensitive operations.

The danger of CSRF attacks lies in the fact that they do not involve direct intrusion into the system, but rather exploit an already trusted session. Therefore, detecting and preventing such attacks can be challenging. This risk becomes even higher in web applications where authentication and session management are not properly secured.

Moreover, modern web technologies and browser cookie policies, as well as cross-site request mechanisms, can create conditions for CSRF attacks to occur. Therefore, it is crucial for developers to implement proper security measures, including the use of CSRF tokens, configuring the SameSite cookie attribute, and introducing additional request validation mechanisms.

Literature Review and Methodology

The literature review conducted on the study of CSRF (Cross-Site Request Forgery) attacks shows that this issue has remained relevant in the field of web security for many years. In scientific sources, CSRF is mainly defined as a type of attack carried out by exploiting a user’s session. According to the security recommendations provided by OWASP (Open Web Application Security Project), CSRF is recognized as one of the most common web security vulnerabilities. Furthermore, modern research highlights the connection of this attack with browser cookie policies, authentication mechanisms, and the operational principles of HTTP requests.

During the literature review, various scientific articles, cybersecurity manuals, and the OWASP Top 10 security list were studied as primary sources. These materials provide a detailed explanation of the CSRF attack mechanism, its types, and methods of protection. In particular, the use of CSRF tokens, implementation of the SameSite cookie attribute, and validation of user requests are identified as effective protective measures.

As a research methodology, both theoretical analysis and practical approaches were applied. The theoretical part involved studying existing scientific literature, online resources, and security standards. The practical part focused on analyzing how CSRF attacks occur in web applications and the mechanisms for preventing them. In addition, the attack mechanism was modeled in various testing environments by simulating malicious requests.

This approach made it possible to gain a deeper understanding of the nature of CSRF attacks, assess their level of risk, and develop effective security measures.

Results and Discussion

During the study, it was determined that CSRF (Cross-Site Request Forgery) attacks pose a serious threat to web application security. The reviewed sources and practical analyses show that this type of attack is carried out by exploiting an active user session and often goes unnoticed by the user. As a result, unauthorized requests may be sent to the system, leading to dangerous situations such as modification of account information or execution of financial transactions.

Practical analysis has shown that CSRF attacks are most effective in web applications with weak authentication and session management mechanisms. In particular, in systems where additional verification of user requests is not implemented, it becomes easier to carry out such attacks. Weaknesses in browser cookie policies and the lack of restrictions on cross-site requests also contribute to the escalation of this issue.

During the discussion, it was identified that the most effective protection methods against CSRF attacks include the use of CSRF tokens, implementation of the SameSite cookie attribute, and the introduction of mechanisms for verifying each critical request. These measures significantly reduce the possibility of unauthorized use of user sessions by attackers.

Furthermore, modern security practices indicate that applying only technical protection measures is not sufficient. Increasing user awareness of cybersecurity is also of great importance, as many attacks are carried out through social engineering techniques.

Conclusion

CSRF (Cross-Site Request Forgery) attacks are considered one of the significant cybersecurity threats to modern web application security. The conducted analyses show that this type of attack is carried out through the misuse of a user’s session, resulting in

unauthorized requests being sent to the system. This negatively affects the security of users' personal data, account information, and critical operations.

During the study, the mechanism of CSRF attacks, their causes, and their connection with vulnerabilities in web applications were examined. The results indicate that systems with poorly protected authentication and session management are more vulnerable to such attacks.

Furthermore, the use of CSRF tokens, implementation of the SameSite cookie attribute, and additional verification of user requests were identified as the most effective solutions for protecting against CSRF attacks.

References:

1. OWASP Foundation. OWASP Top 10 Web Application Security Risks. https://owasp.org
2. OWASP Foundation. Cross-Site Request Forgery (CSRF) Prevention Cheat Sheet. https://owasp.org/www-community/attacks/csrf
3. Stuttard D., Pinto M. The Web Application Hacker's Handbook. Wiley Publishing.
4. Zalewski M. The Tangled Web: A Guide to Securing Modern Web Applications. No Starch Press.
5. Mozilla Developer Network (MDN). Web Security: CSRF and SameSite Cookies. https://developer.mozilla.org
6. RFC 6265. HTTP State Management Mechanism (Cookies). IETF Standards.
7. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education.
8. Goodfellow I., et al. Web Application Security: Concepts and Practices (scientific reference materials)