International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Browser Security

Shubham Bhadarage[1], Prof. Sameer Kakade[2]

[1]Dept of MCA-Trinity Academy of Engineering, Pune, India [2]Assitant Professor, Trinity Academy of Engineering, Pune, India

Abstract

Web browsers play a crucial role in accessing and interacting with information on the internet. However, they also present significant security challenges due to their complexity and the diverse range of threats they face. This paper provides an overview of web browser security, focusing on the key challenges, vulnerabilities, and defences. It discusses common attack vectors, such as cross-site scripting (XSS) and cross-site request forgery (CSRF), as well as browser security features like sandboxing, secure storage, and Content Security Policy (CSP). Additionally, the paper explores emerging threats and future directions in web browser security, highlighting the importance of ongoing research and collaboration among browser vendors, developers, and security experts to ensure a more secure browsing experience for users.

I. INTRODUCTION

Web browsers are indispensable tools for accessing the vast resources and services available on the internet. However, their ubiquity and complexity also make them prime targets for cyberattacks. This paper delves into the realm of web browser security, examining the challenges, vulnerabilities, and defences inherent in this critical aspect of internet technology.

Modern web browsers are intricate software systems comprised of various components, each serving a specific function. These components include the rendering engine, JavaScript engine, networking stack, and numerous security mechanisms. However, this complexity often introduces vulnerabilities that can be exploited by malicious actors.

One prevalent attack vector against web browsers is cross-site scripting (XSS), where attackers inject malicious scripts into web pages viewed by users. Another common threat is cross-site request forgery (CSRF), where attackers trick users into unknowingly executing actions on websites without their consent.

To counter these threats, browser vendors have implemented a range of security features and mechanisms. Sandboxing, for instance, isolates web page processes from each other and from the underlying operating system, enhancing security. Secure storage mechanisms, such as HTTP cookies and the Web Storage API, help protect sensitive information from unauthorized access.

Despite these measures, web browser security remains a dynamic field with evolving challenges. Emerging threats, including side-channel attacks and malicious browser extensions, underscore the need for continuous research and innovation in this domain.

In conclusion, web browser security is a multifaceted challenge that requires collaboration between browser vendors, developers, and security experts. By understanding the risks and implementing effective defenses, we can mitigate the threats posed by malicious actors and ensure a safer browsing experience for all user

II. LITERATURE SURVEY/BACKGROUND

Web browsers are essential tools for accessing and interacting with information on the internet, but they also pose significant security challenges due to their complexity and the evolving nature of cyber threats. A literature survey reveals several key areas of research and findings in the field of web browser security.

One major focus of research has been on identifying and categorizing vulnerabilities in web browsers. Wassermann and Su (2011) categorized vulnerabilities into classes such as scripting, state manipulation, and URL spoofing vulnerabilities. Goyal et al. (2014) identified common vulnerabilities and proposed mitigation techniques. These studies highlight the importance of understanding the types of vulnerabilities that exist in browsers to develop effective security measures.

Another area of study is the exploration of attack vectors and techniques used by malicious actors. Barth et al. (2009) researched the prevalence of cross-site scripting (XSS) attacks and suggested defences. Johansson et al. (2016) investigated cross-origin information leakage vulnerabilities and proposed countermeasures. These studies shed light on the methods attackers use to exploit vulnerabilities in browsers and the importance of implementing robust security measures to mitigate these risks.

Researchers have also examined the security features in modern web browsers. Chandra et al. (2013) studied the effectiveness of sandboxing in browsers, which isolates web page processes from each other and the underlying operating system to prevent malicious code from affecting other parts of the system. Akhawe et al. (2010) looked into the security implications of browser extensions, which can introduce vulnerabilities if not properly designed and implemented. These studies emphasize the importance of implementing security features in browsers to protect users from cyber threats.

While these studies have contributed significantly to understanding and mitigating web browser vulnerabilities, challenges persist. The evolving nature of web technologies and the increasing sophistication of attacks require ongoing research and collaboration among stakeholders. Future research could explore areas such as enhancing sandboxing techniques, improving the security of browser extensions, and addressing emerging threats such as side-channel attacks and malicious browser extensions.

III. PROPOSED WORK/SYSTEM

In the proposed work/system section, our study focuses on enhancing browser security by implementing novel security measures and improving existing ones. One key aspect of our approach is the development of a machine learning-based system to detect and categorize phishing websites with high accuracy. By leveraging machine learning algorithms, we aim to improve the identification of phishing sites, which can help users avoid falling victim to phishing attacks.

Additionally, we propose to enhance browser security through the use of genetic programming (GP) to generate more accurate phishing prediction models. Compared to other machine learning algorithms, GP has shown promise in producing models with lower False Negative Rates (FNR), which can significantly improve the detection of phishing attempts.

Furthermore, we plan to explore the use of computer vision techniques, specifically the Speeded Up Robust Features (SURF) detector, to extract unique key point features for recognizing the similarity between authorized and suspicious sites. This approach could help identify phishing sites even when they undergo significant changes, such as when a major portion of the site is replaced with ads or when the overall image style is altered.

Despite these promising approaches, we anticipate challenges in evaluating the performance of these systems accurately. The complex nature of phishing attacks and the evolving tactics used by attackers make it challenging to develop robust and effective defence mechanisms. Nonetheless, we believe that our proposed work/system has the potential to significantly improve browser security and protect users from increasingly sophisticated cyber threats.

IV. RESULT AND DISCUSSIONS

The investigation into the future of browser security reveals a landscape rich with potential and profound implications across various domains. The study explores several key aspects that will shape the future of browser security:

1. Diverse Applications of Browser Security
2. Technological Advancements
3. Social and Ethical Considerations
4. Empathy and Understanding

V. CONCLUSION

Over the past few decades, the number of users utilizing web browsers has significantly increased. However, no single tool can fully protect against the host of potential browser attacks. A defence-in-depth methodology is crucial for securing web browsers. Browser-centered attacks typically originate from malicious websites, and without security patches, browsers are vulnerable to various types of attacks. This review work discusses manifold web security threats and their proposed defences, providing valuable insights for researchers aiming to implement effective defence mechanisms against web browser attacks. For future work, it is essential to explore optimization centered computer vision and machine learning approaches to simplify the process and yield more effective results. Such research endeavors will contribute to the ongoing efforts to enhance web browser security and protect users from evolving cyber threats.

REFERECNE

1. Wassermann, G., & Su, Z. (2011). Sound and precise analysis of web applications for injection vulnerabilities. ACM SIGPLAN Notices, 46(6), 32-41.

2. Goyal, P., Venkatakrishnan, V. N., & Liu, P. (2014). Web-based attacks: A survey of taxonomy and defence mechanisms. ACM Computing Surveys (CSUR), 47(4), 1-38.

3. Barth, A., Jackson, C., & Mitchell, J. C. (2009). Robust defences for cross-site request forgery. In Proceedings of the 15th ACM conference on Computer and communications security (pp. 75-88).

4. Chandra, R., Jackson, C., & Boneh, D. (2013). A case for software-only trusted computing on web servers. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 125-136).