IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, July 2024

The Cross-Site Scripting (XSS) Attack: A Comprehensive Review

Prof. Jayanthkumar A Rathod[1], Darshan S Gowda[2], Kartik M[3], Paresh Talekar[4], Nagaraj Daddi[5], Ashwini Bhairanallikar[6], Gousiya G[7]
Professor, Department of Computer Science and Design[1]
Students, Department of Computer Science and Design[2,3,4,5,6,7]
Alva's Institute of Engineering and Technology, Mijar, Moodabidiri, India
jayantkumarrathod@gmail.com,darshansgowda20042004@gmail.com, kartikmyageri84@gmail.com , pareshtalekar2@gmail.com, nagraj973143@gmail.com, 4al22cg006@gmail.com,4al22cg020@gmail.com

Abstract:. *Cross-site scripting (XSS) is a critical threat to web applications, involving the insertion of malicious code to compromise user trust and extract sensitive information. This paper presents a comprehensive review of various XSS attack types, including Reflected, Persistent, DOM-based, Blind XSS, and Self-XSS. It discusses prevention and remediation strategies such as secure development practices, data assessment, content filtering, encoding, and the use of web application firewalls and security tools like Cloudflare and Zscaler. Despite advancements, XSS vulnerabilities persist due to inadequate security measures during development. The paper emphasizes the need for robust security plans and introduces Sanctum's App-Scan as an example of an effective security measure. Lastly, it underscores the importance of understanding and addressing the diverse forms of XSS attacks to ensure comprehensive internet security*

Keywords: Cross-site scripting; web security; web applications; XSS attacks; mobile

DOI: 10.48175/IJARSCT-19230