Artificial Intelligence Review (2023) 56:12725–12769
https://doi.org/10.1007/s10462-023-10433-3

Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review

Jasleen Kaur[1] · Urvashi Garg[1] · Gourav Bathla[2]

Published online: 23 March 2023

Abstract

With the rising demand for E-commerce, Social Networking websites, it has become essential to develop security protocols over the World Wide Web that can provide security and privacy to Internet users all over the globe. Several traditional encryption techniques and attack detection protocols can secure the data transmitted over public networks. However, hackers can effortlessly exploit them to acquire access to the users' sensitive information such as user ID, session ID, cookies, passwords, bank account details, contact numbers, private PINs, database information, etc. Researchers have continuously innovated new techniques to build a secure and robust system that cannot be easily hacked and manipulated. Still, there is much scope for novelty to provide security against contemporary techniques used by intruders. The motivation of this survey is to observe the recent developments in Cross-Site Scripting attacks and techniques used by researchers to secure confidential information. Cross-Site Scripting (XSS) has been recognized as one of the top 10 online application security risks by the Open Web Application Security Project (OWASP) for decades. Therefore, dealing with this security flaw in web applications has become essential to avoid further personal and financial damage to Internet users and business organizations. There is a need for an extensive survey of recent XSS attack detection techniques that can provide the right direction to researchers and security professionals. We present a complete overview of recent machine learning and neural network-based XSS attack detection techniques in this paper, covering deep neural networks, decision trees, web-log-based detection models, and many more. This paper also highlights the research gaps that must be addressed while designing attack detection models. Further, challenges researchers face during the development of recent techniques are also discussed. Finally, future directions are provided to reflect on new concepts that can be used in forthcoming research works to improve XSS attack detection techniques.

Keywords Web vulnerabilities · Cyber-attacks · Web-security · Machine learning · XSS attack · Deep learning · Neural networks

✉ Gourav Bathla
gouravbathla@gmail.com

Extended author information available on the last page of the article