World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:16, No:02, 2022

Ontology for Cross-Site-Scripting (XSS) Attack in Cybersecurity

Authors : Jean Rosemond Dora, Karol Nemoga

Abstract : In this work, we tackle a frequent problem that frequently occurs in the cybersecurity field which is the exploitation of websites by XSS attacks, which are nowadays considered a complicated attack. These types of attacks aim to execute malicious scripts in a web browser of the client by including code in a legitimate web page. A serious matter is when a website accepts the “user-input” option. Attackers can exploit the web application (if vulnerable), and then steal sensitive data (session cookies, passwords, credit cards, etc.) from the server and/or from the client. However, the difficulty of the exploitation varies from website to website. Our focus is on the usage of ontology in cybersecurity against XSS attacks, on the importance of the ontology, and its core meaning for cybersecurity. We explain how a vulnerable website can be exploited, and how different JavaScript payloads can be used to detect vulnerabilities. We also enumerate some tools to use for an efficient analysis. We present detailed reasoning on what can be done to improve the security of a website in order to resist attacks, and we provide supportive examples. Then, we apply an ontology model against XSS attacks to strengthen the protection of a web application. However, we note that the existence of ontology does not improve the security itself, but it has to be properly used and should require a maximum of security layers to be taken into account.

Keywords : cybersecurity, web application vulnerabilities, cyber threats, ontology model
Conference Title : ICCT 2022 : International Conference on Cybersecurity and Threats
Conference Location : Paris, France
Conference Dates : February 17-18, 2022