Alyson Hall

CYB333

May 26, 2020

Course Project

XXS Vulnerability Scanner

Project Plan:

For this project, I plan on building an XXS vulnerability scanner. Cross-site scripting is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable web application. The attacker aims to execute scripts in the victim's web browser by including malicious code in a normal web page. These flaws that allow these types of attacks are quite widespread in web applications that has user input. So, for the goal for this project is to look for vulnerabilities that could cause XXS or make it easier for an attacker to use XXS attack against the system. Another goal for this project is to be aware of this type of attack and learn how to detect the XSS vulnerabilities. The expected outcome for this project is to run a scan for a website and see if the outcome is true or not. If it is “true”, then there should be no vulnerabilities in the system for the website. I first started out the process by making a function to get all the forms from the HTML content of any web page. Then, I made a function to return a list of forms as soup objects and made a way to extract every form details and attributes. Then, after I get the form details, I set up another function to submit any given form. Finally, after we extract the form information, we cannot scan for XSS vulnerabilities.

Green = 1st step

Blue = 2nd step

Orange = 3rd step

Yellow = 4th step

<https://github.com/alyhalll/XSSscan.git>

A screenshot of a cell phone

Description automatically generated

A screenshot of text

Description automatically generated