Experiment: 1.2

Student Name: Yash Kumar
UID: 20BCS9256
Branch: BE-CSE
Section/Group: 616 –B
Semester: 5
Date: 31-08-22
Subject Code: 20CSP-338

Aim: Design a method to stimulate the html injection and cross site scripting to exploit the attackers.

Objective: To test HTML and XSS injection.

Software: Windows 7

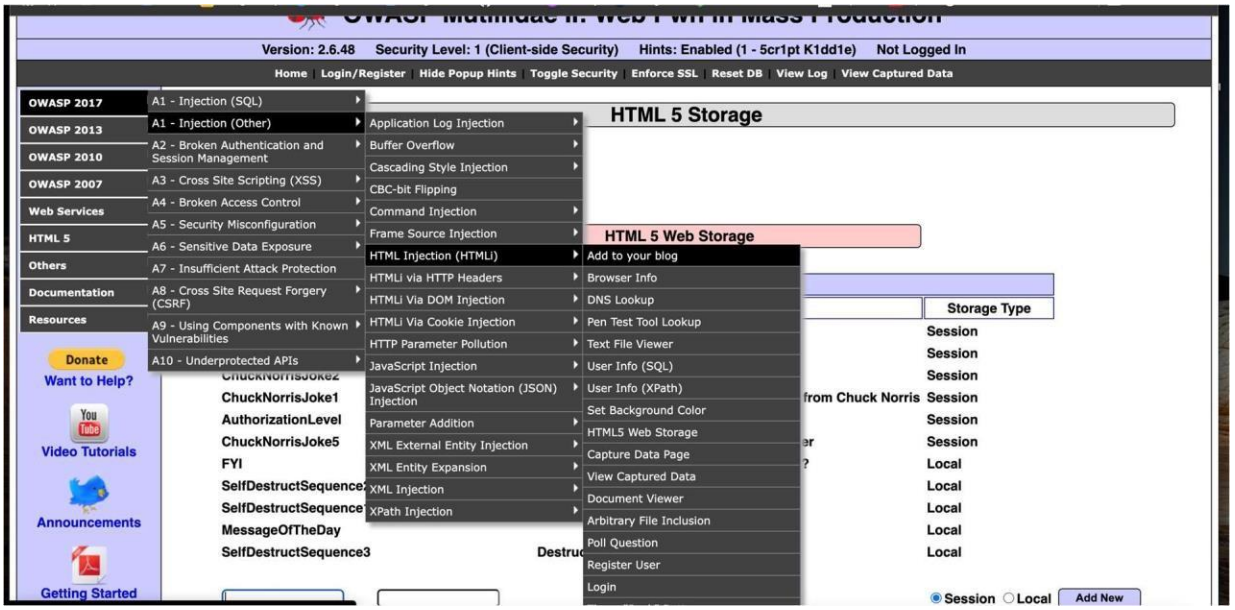
Tools to be used:

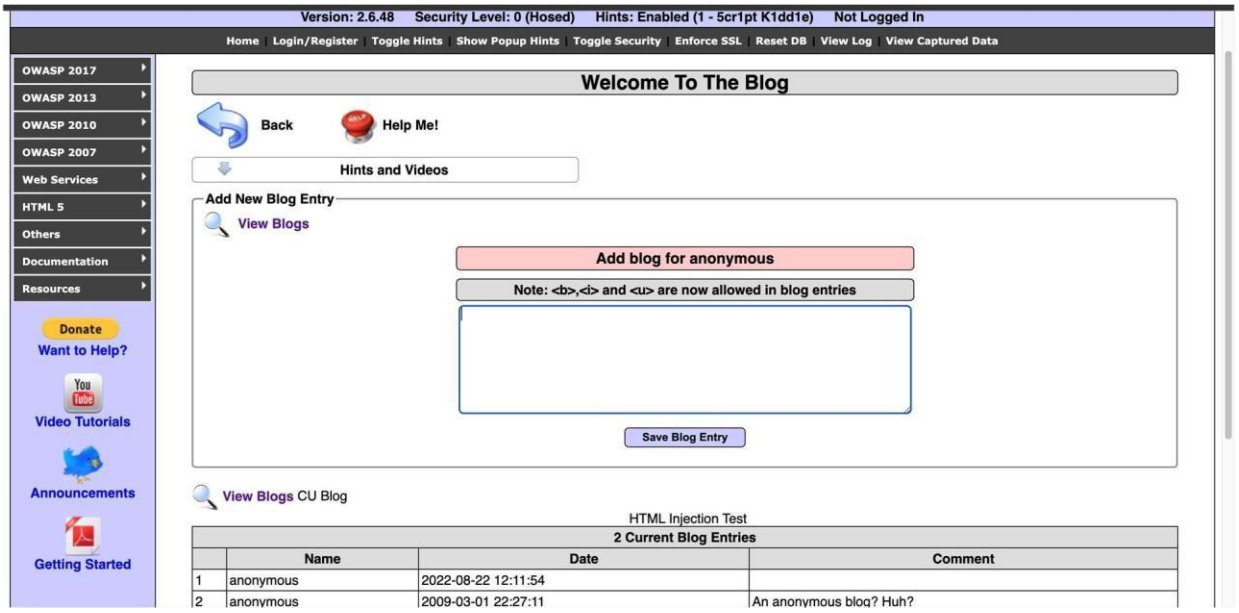
1. OSWAP Mutillidae II: Web PWN in Mass Production.
2. XSS game site.

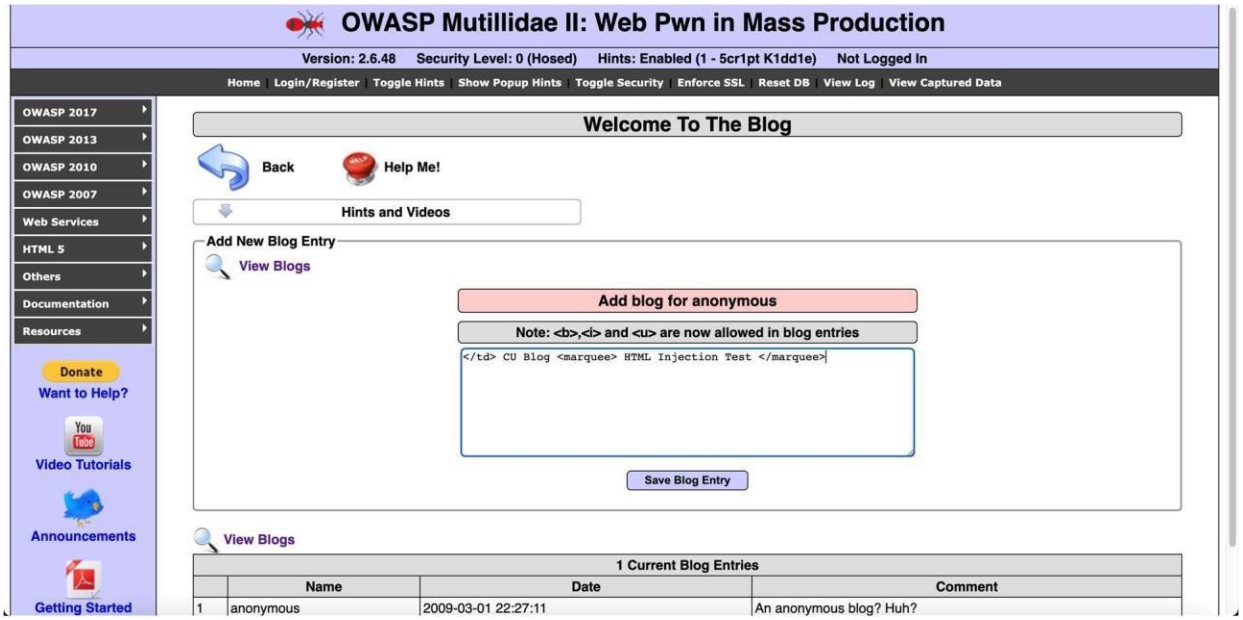
Steps to implement HTML Injection:

1. Open website: OSWAP Mutillidae II: Web Pwn in Mass Production
   Link: http://128.198.49.198:8102/mutillidae/index.php?page=add-to-your-blog.php
2. From the menu on the left open Add to your blog.
3. Enter the HTML code inside the given text area in order to set up the HTML injection attack.
4. Example: </td> CU Blog <marquee> html injection attack </marquee>.
5. The html code will now gets rendered whenever the victims visits the malicious page.

Screenshots: (HTML INJECTION)







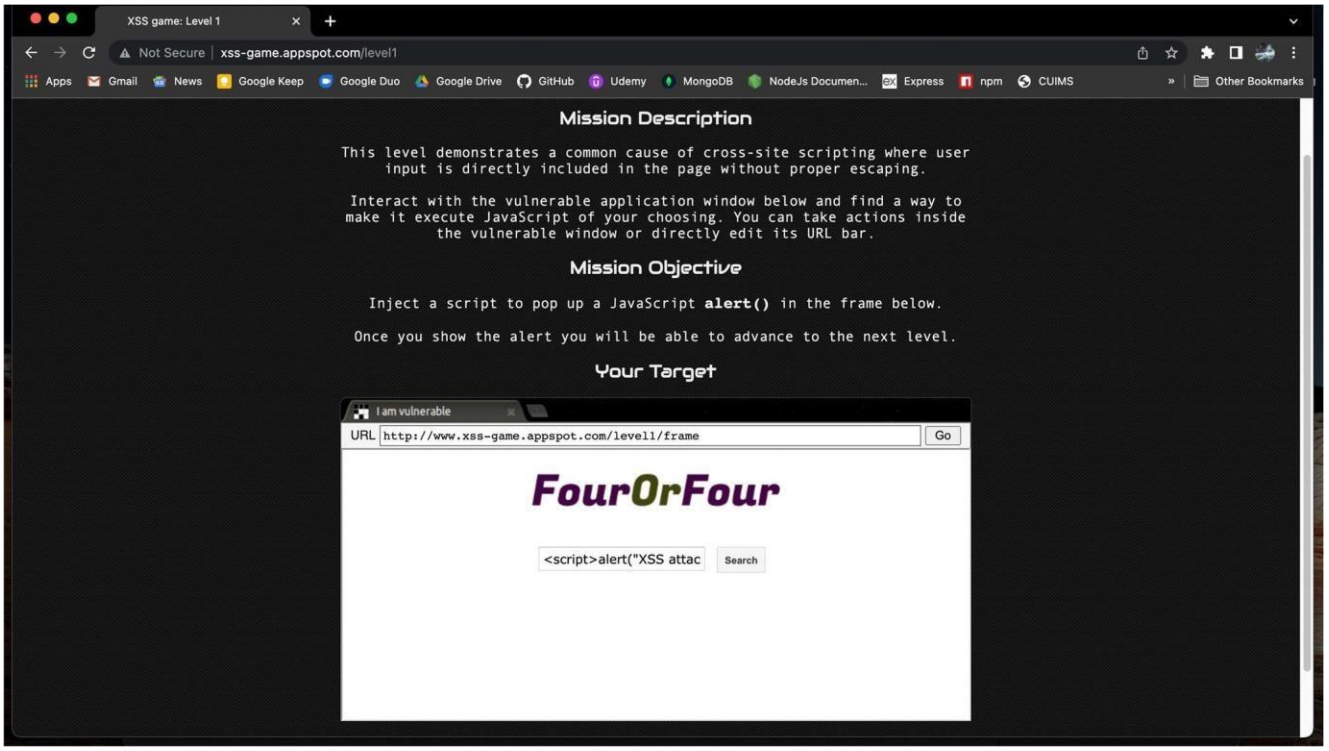
Cross-Site Scripting (XSS):

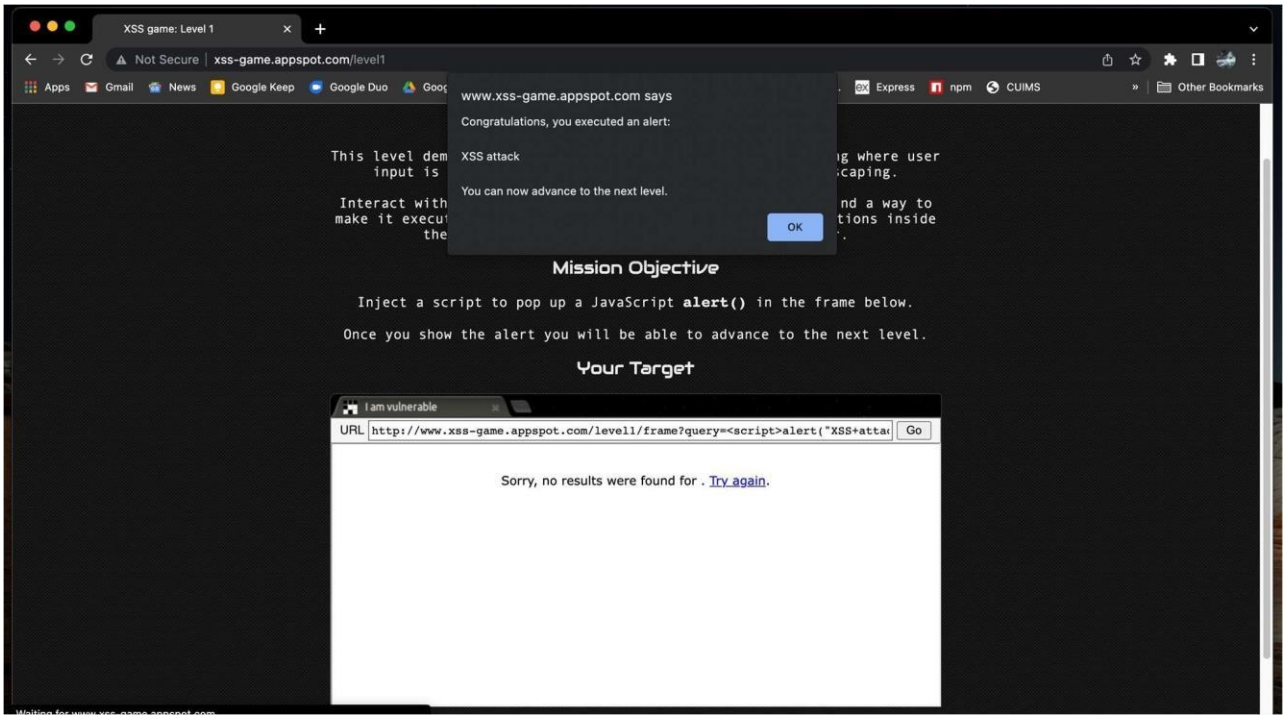
Steps to implement XSS:

1. Open the link: http://www.xss-game.appspot.com/level1
2. If the search field vulnerable, when the user enters any script, then it will be executed. Consider, a user enters a very simple script.
3. Then after clicking on the "Search" button, the entered script will be executed. The script typed into the search field gets executed. This just shows the vulnerability of the XSS attack.

Screenshots:

Cross-Site Scripting (XSS):





Learning Outcomes:

- I learned about HTML injection and XSS injection.
- Got an overview of how these attacks are constructed and applied to real system. If the app or website lacks proper data sanitization, the malicious links executes the attacker's chosen code on the user's system.
- Got to know about the difference in HTML injection and XSS injection.
- HTML injection attack is closely related to cross-site scripting (XSS). HTML injection uses HTML to deface the page. XSS, as the name implies, injects JavaScript into the page. Both attacks exploit insufficient validation of user input.