

Exp No : 2

Web and Mobile Security

# Student Name: ANIKET KUMAR UID: 20BCS5306

**Branch:** CSE **Section/Group:** 20BCS\_WM-703 / B

# Semester: 5th Date of Performance:06/09/2022 Subject Name: Web and mobile Security Lab Subject Code: 20CSP-338

1. **Aim/Overview of the practical:**

Design a method to simulate the html injection and cross site scripting to exploit the attackers.

# Task to be done/ Which logistics used:

Objective: To analyse Http traffic.

Software/Hardware Requirements:

Windows 7 & above version

Wireshark Packet Sniffer and Packet Capture Library Microsoft Word. Win Zip as necessary

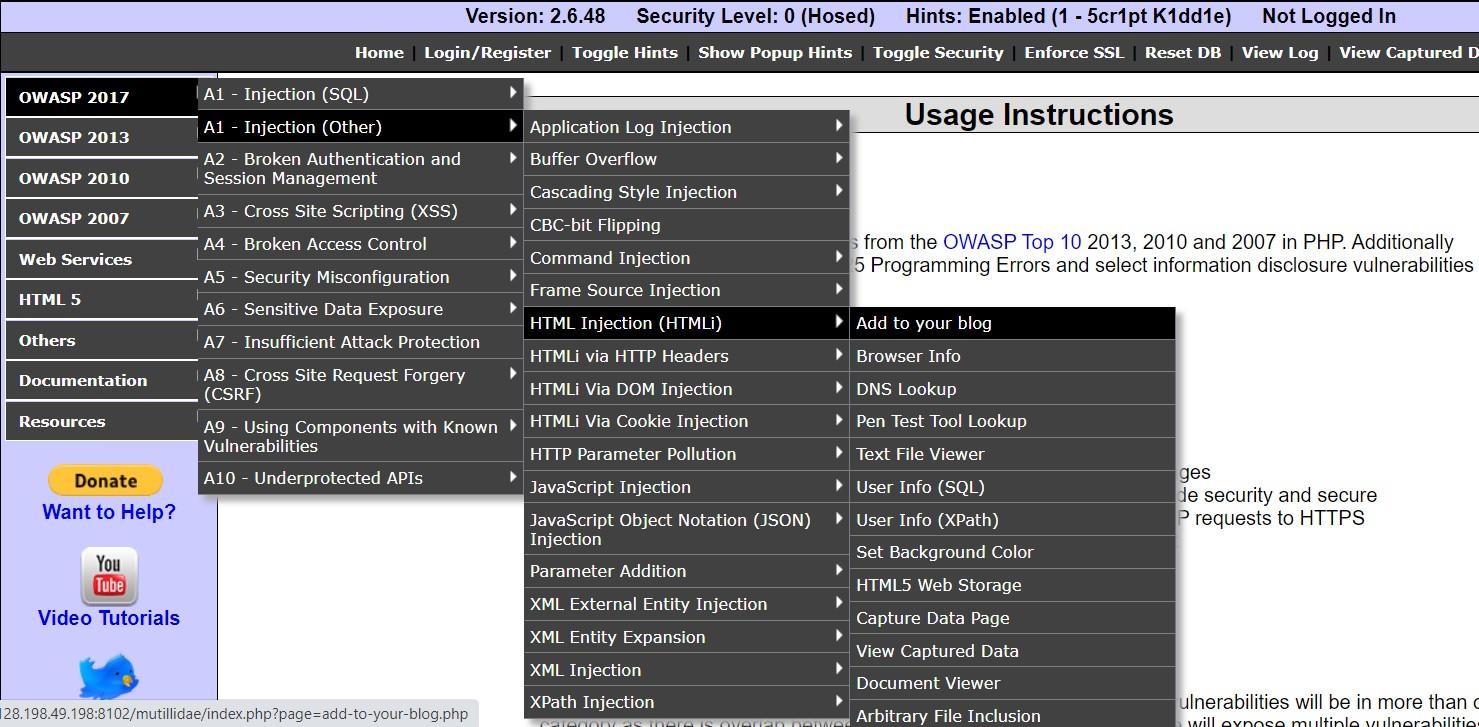
# Result/Output/Writing Summary:

*HTML Injection*

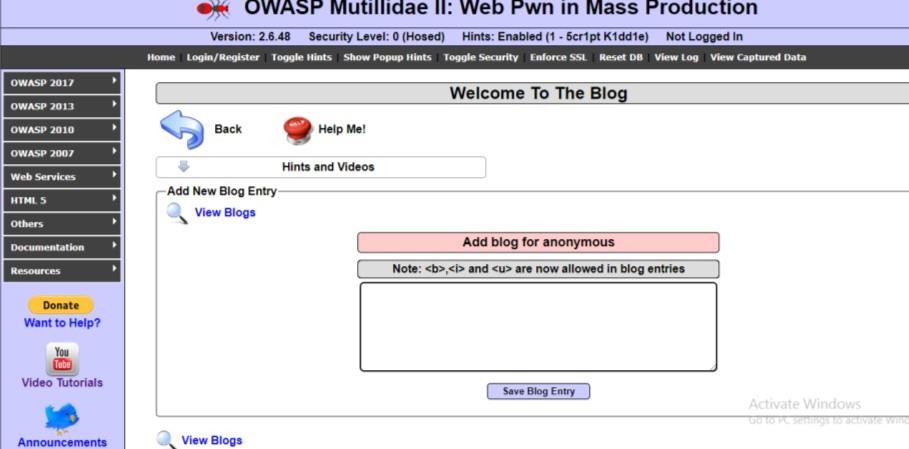
1. Open website : **OWASP Mutillidae II: Web Pwn in Mass Production**

(URL: http://128.198.49.198:8102/mutillidae/index.php?page=documentation/usageinstructions.php)

1. Now, we’ll be redirected to the web page which is suffering from an **HTML Injection vulnerability** which allows the user to submit his entry in the blog.
2. On the left hand side, click on OWASP 2017🡪A1-injection(others)🡪HTML injection.



1. Welcome to blog window will appear on the screen. Now, let’s try to inject malicious code. Enter the HTML code inside the given text area in order to set up the HTML attack.

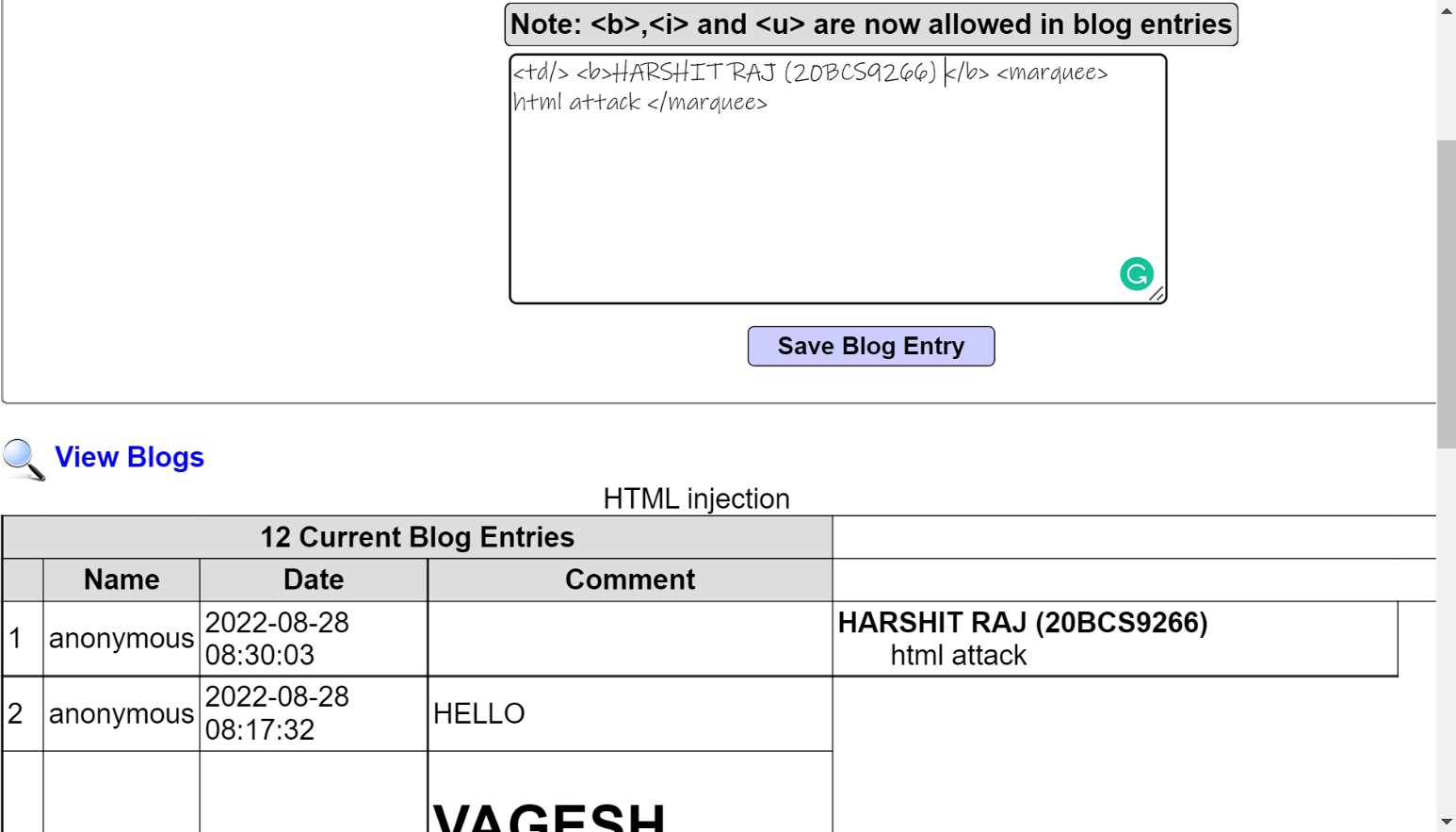


|  |
| --- |
| **5.** For example injected code is : **<td/> CU blog <marquee> html attack </marquee>** |
| then save blog entry |



|  |
| --- |
|  |
| 6. That html code is thus now into the application’s web server, which gets rendered every |
| time whenever the victim visits this malicious page, he’ll always have this code which |
| looks official to him. |

## XSS attack

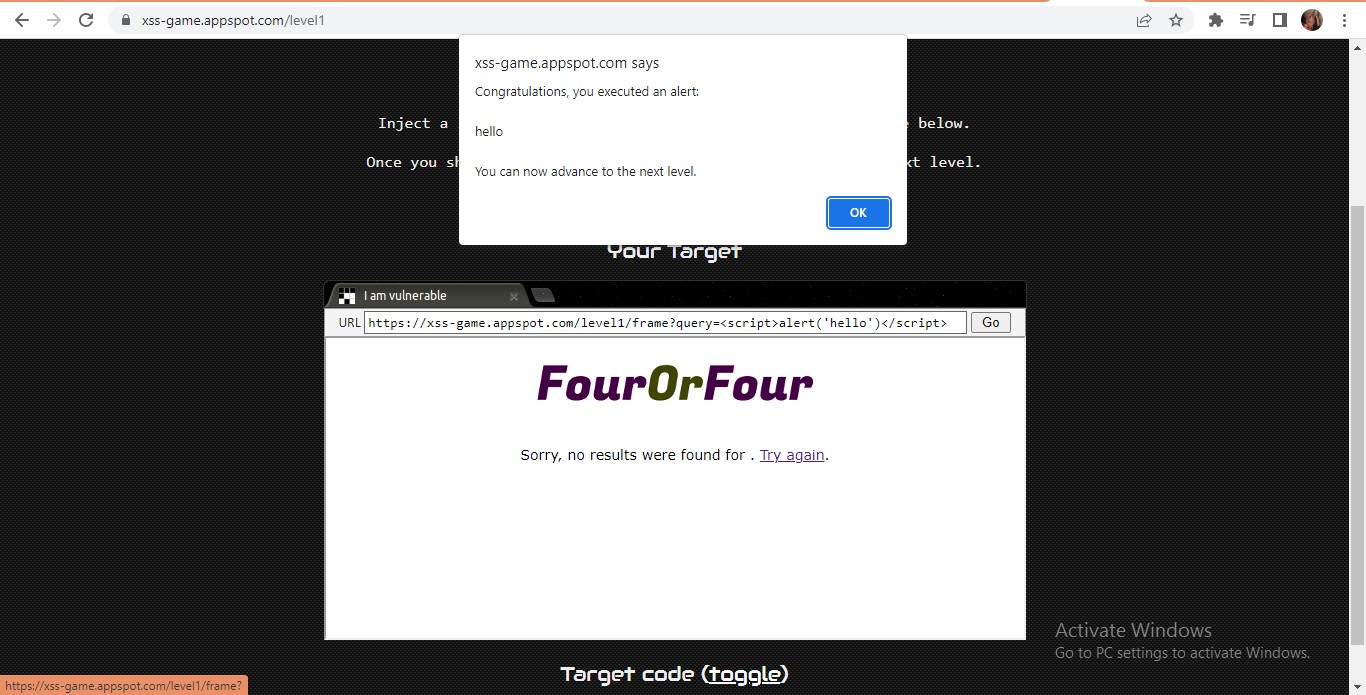


* 1. Open the link <https://xss-game.appspot.com/level1>(or Google XSS game website).



* 1. If the search field is vulnerable, when the user enters any script, then it will be executed. Consider, a user enters a very simple script as shown below:

## <script>alert(‘ Hello)</script>



* 1. 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.



# Learning outcomes (What I have learnt):

## We have learned what HTML injection is and XSS injection .

* + 1. **An overview of how these attacks are constructed and applied to real system.**

## If the app or website lacks proper data sanitization, the malicious link executes the attacker's chosen code on the user's system.

**Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):**

|  |  |  |  |
| --- | --- | --- | --- |
| Sr. No. | Parameters | Marks Obtained | Maximum Marks |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
|  |  |  |  |