

## **Experiment – 2**

**NAME: Lipakshi**

**SUBJECT NAME: WMS Lab**

**UID: 20BCS5082  
338**

**SUBJECT CODE: 20CSP-**

**SECTION: 20BCS WM\_607-B**

### **Aim:**

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

### **Objective:**

To test HTML and XSS Injection

### **Software/Hardware Requirements:**

Windows 7 & above version.

### **Tools to be used:**

1. OWASP Mutillidae II: Web Pwn in Mass Production
2. XSS game site
3. Notepad
4. Acunetix Vulnerability Scanner

## **Introduction:**

**Acunetix** is a web application security scanner that gives you a 360-degree view of the organization's security. This end-to-end web security scanner can identify over 7000 vulnerabilities like XSS and misconfigurations. It has capabilities for scanning all pages, web apps, complex web applications, etc.

## **Steps/Method/Coding:**

### **HTML Injection**

1. Open the link in your browser

[http://128.198.49.198:8102/mutillidae/index.php?page=home.php&pop\\_UpNotificationCode=HPH0](http://128.198.49.198:8102/mutillidae/index.php?page=home.php&pop_UpNotificationCode=HPH0).

OR

Open OWASP Multilidae II: Web Pwn in Mass Production by typing in browser.

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 as shown in the screenshot.

2. Now, let us try to inject malicious code. Enter the HTML code inside the given text area in order to set up the HTML attack.
3. 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 will 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

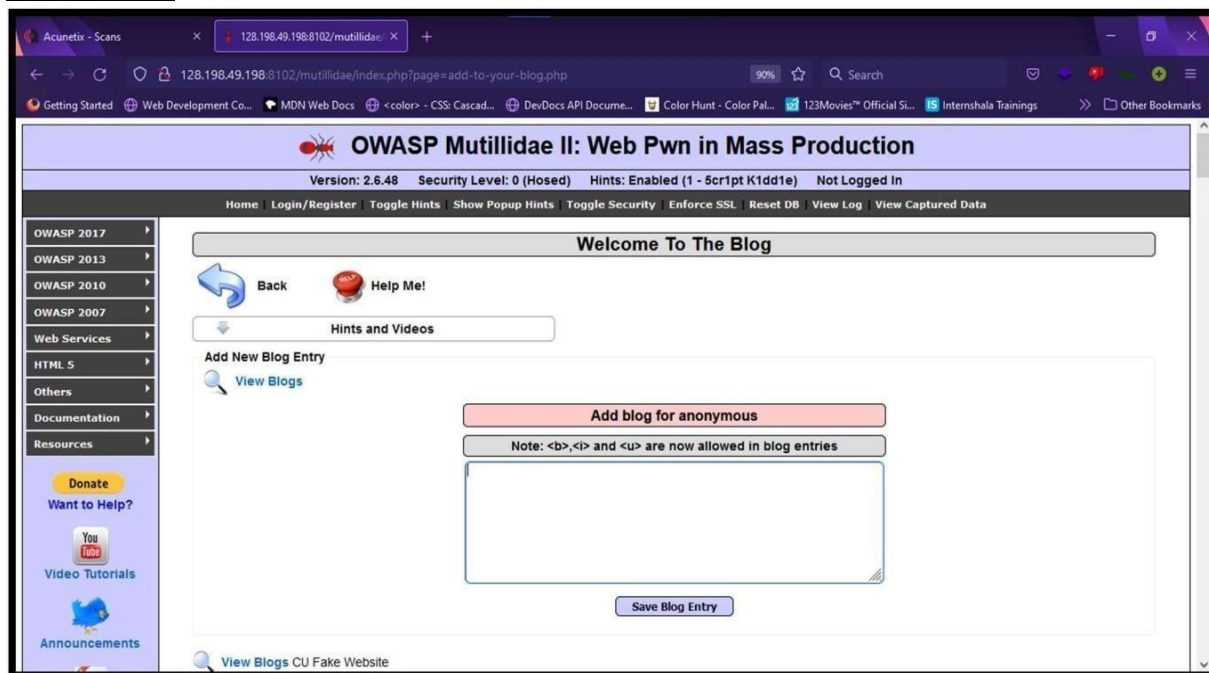
2. If the search field is vulnerable, when the user enters any script, then it will be executed.


Consider, a user enters a very simple script as shown below:

```
<script>alert(' XSS attack')</script>
```

3. Then after clicking on the “**Search**” button, the entered script will be executed. This just shows the vulnerability of the XSS attack. However, a more harmful script may be typed as well.

## OUTPUT:





Getting Started

CU FAKE Website

CU FAKE WEBSITE

CU FAKE Website

lalit

CU ATTACK

CU ATTACK

CU ATTACK

cu attacker

100 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2022-08-23 09:58:50	Hello my name is Shivansh Raheja My uid is 20BCSXXXX
2	anonymous	2022-08-23 09:56:44	Hello
3	anonymous	2022-08-23 09:56:16	
4	anonymous	2022-08-23 09:52:23	Greetings of the day to everyone, Myself Shivansh Raheja

Acunetix - Scans

128.198.49.198:8102/mutillidae/ X XSS game: Level 1

https://xss-game.appspot.com/level1

**[1/6] Level 1: Hello, world of XSS**

### Mission Description

This level demonstrates a common cause of cross-site scripting where user input is directly included in the page without proper escaping.

Interact with the vulnerable application window below and find a way to make it execute JavaScript of your choosing. You can take actions inside the vulnerable window or directly edit its URL bar.

### Mission Objective

Inject a script to pop up a JavaScript `alert()` in the frame below.

Once you show the alert you will be able to advance to the next level.

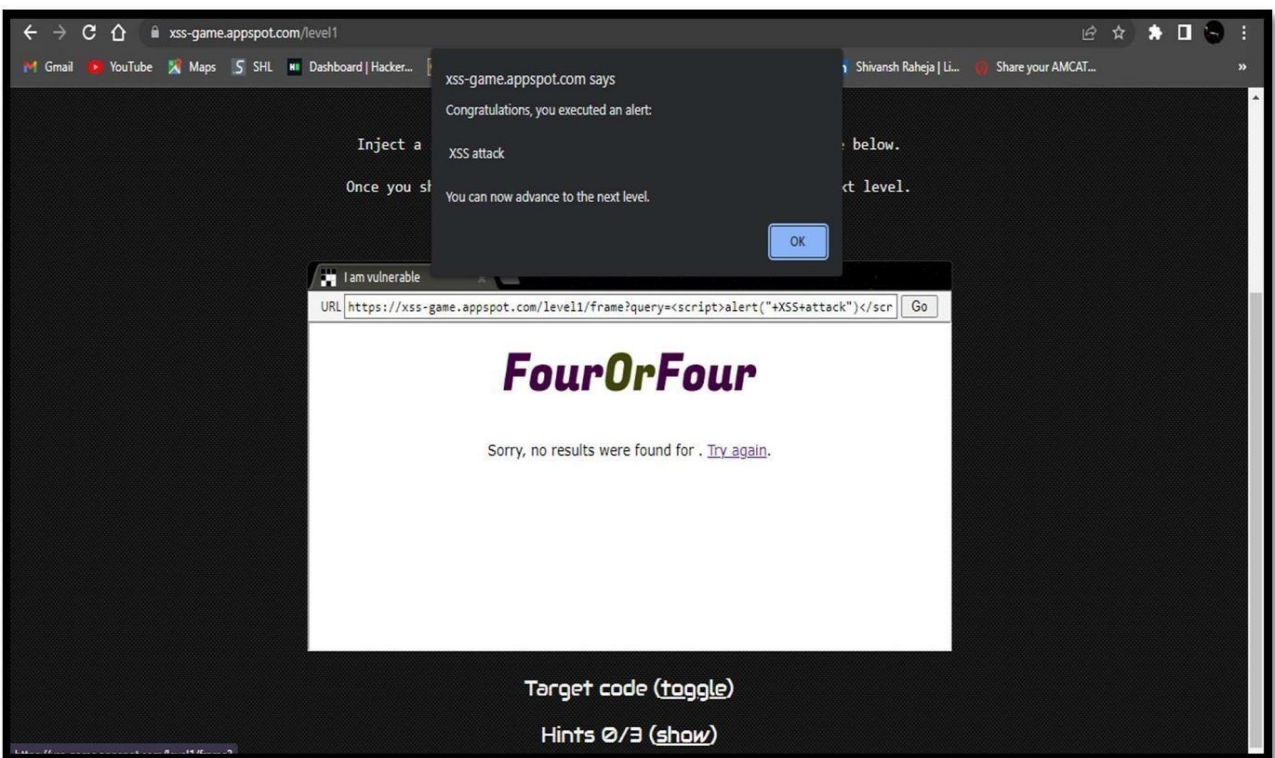
### Your Target

I am vulnerable

URL [object Object] Go

**FourOrFour**

Enter query here... Search



### **Learning Outcomes:**

We learn what is html injection and xss injection. 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. As a result, the attacker can steal the user's active session cookie and can be the harmful for the website.