**Experiment-2**

**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: Window 7 and above version**

**Tools to be used:**

OWASP Mutillidae II: Web Pwn in Mass Production

XSS game site

## Introduction:

[**Acunetix**](https://www.acunetix.com/web-vulnerability-scanner/?utm_medium=3rdparty&utm_source=softwaretestinghelp&utm_campaign=cross-site-scripting) 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.

Acunetix offers specialized technologies that let you detect more and fix faster

**Reading Material (add reference links along with material):**

## Html Injection

* The attacker finds the vulnerable web application.
* The attacker sends the modified URL to the user by any means, usually via email. This URL has text injected.
* By clicking on the URL user is navigated to the attackers webpage, looks like legitimate one.
* User asked the information like username, password, card pins etc.
* This information gets transferred to the attackers server.

for example

**www.testing.com/siteAdcontent?divMessage=**<h1>Click Here!!</h1> It is possible to modify it as −

* **www.testing.com/siteAdcontent?divMessage=**<hack><h1>Do not Click!!</h1><hack>

**Cross Site Scripting(XSS)**

* It happens whenever an application takes untrusted data and sends it to the client browser without validation. This allows attackers to execute malacious scripts in the victim's browser which can result in user sessions hijack, defacing web sites or redirect the user to malicious sites.

**Types of XSS**

* Stored XSS - Stored XSS also known as persistent XSS occurs when user input is stored on the target server such as database/message forum/comment field etc. Then the victim is able to retrieve the stored data from the web application.
* Reflected XSS - Reflected XSS also known as non persistent XSS occurs when user input is immediately returned by a web application in an error message/search result or the input provided by the user as part of the request and without permanently storing the user provided data.
* DOM Based XSS –This type of attack occurs when the DOM environment is being changed, but the client-side code does not change. When the DOM environment is being modified in the victim’s browser, then the client side code executes differently

<https://www.veracode.com/security/xss>

[HTML Injection Tutorial: Types & Prevention with Examples (softwaretestinghelp.com)](https://www.softwaretestinghelp.com/html-injection-tutorial/)

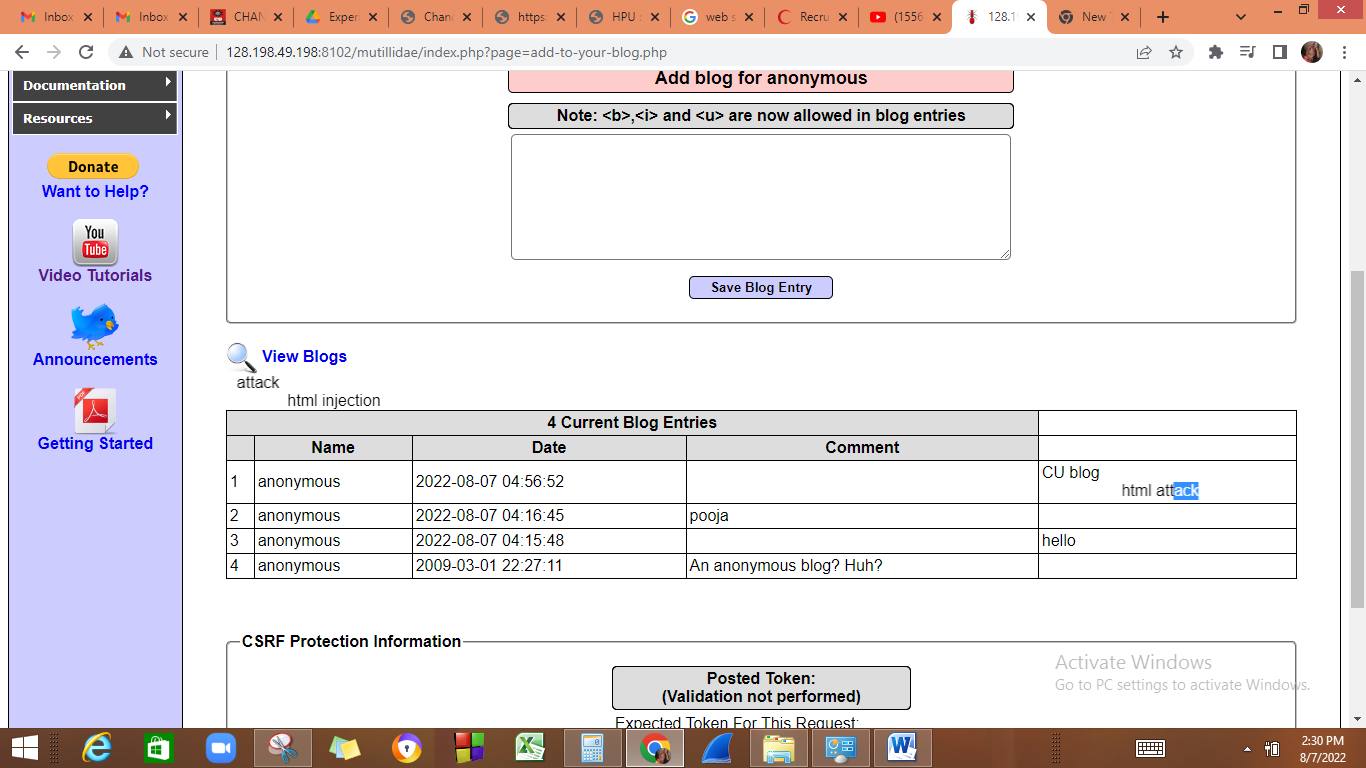
**Steps/Method/Coding:**

**HTML Injection**

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

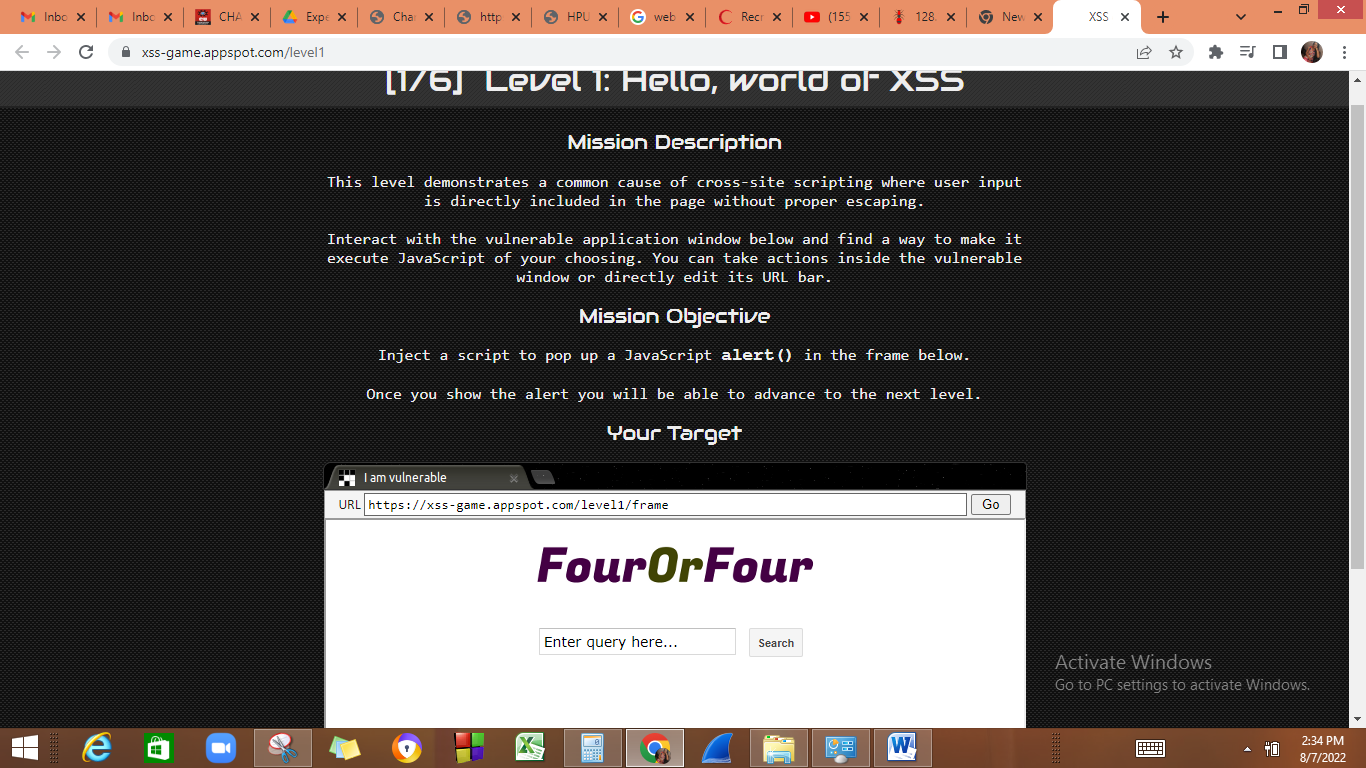
(URL: http://128.198.49.198:8102/mutillidae/index.php?page=documentation/usage-instructions.php)

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🡪Add to your blog (check screenshot)
3. 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.
4. For example injected code is : **<td/> CU blog <marquee> html attack </marquee>** then save blog entry
5. 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)

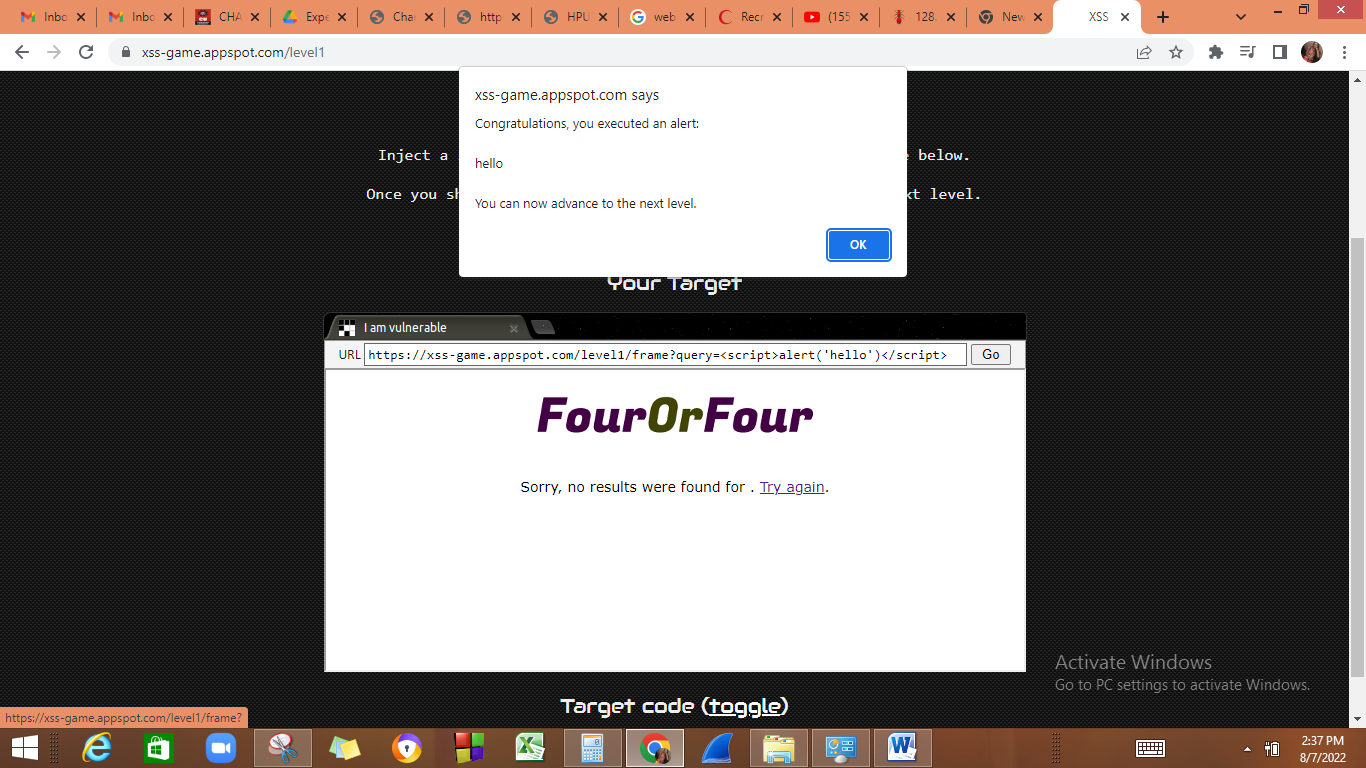


1. If the search field is vulnerable, when the user enters any script, then it will be executed. Consider, a user enters a very simple script as shown below:

**<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.



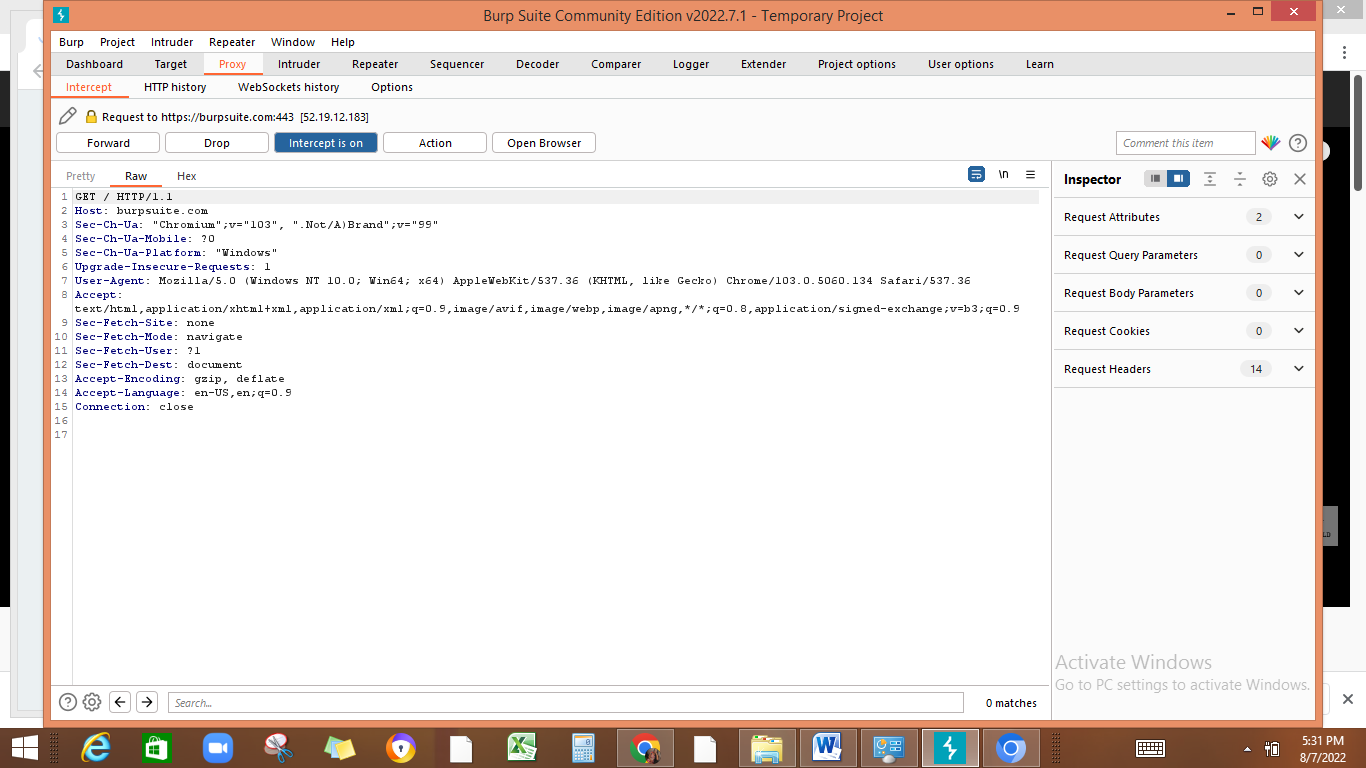
**Learning outcome:**

We have learned what HTML injection is 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.

**Burpsuite**

**Download Link**

[**https://portswigger.net/burp/communitydownload**](https://portswigger.net/burp/communitydownload)



1. Proxy> intercept on->open browser-> type any URL like burpsuite.com🡪forward (to open that page on browser)

Preconfigured browsers are there. So we can fetch a request and modify it and then can send to server.