**Web and Mobile Security**

**EXPERIMENT-2**

**Student’s Name: Kanishk Soni UID: 20BCS9398**

**Section/Group: 20BCS\_WM\_707\_B Subject Code: 20CSP-338**

**Subject Name: WMS\_Lab Date of performance: 11/08/2022**

**Branch: B.E. CSE Semester: 5th**

**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

**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.

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

**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>

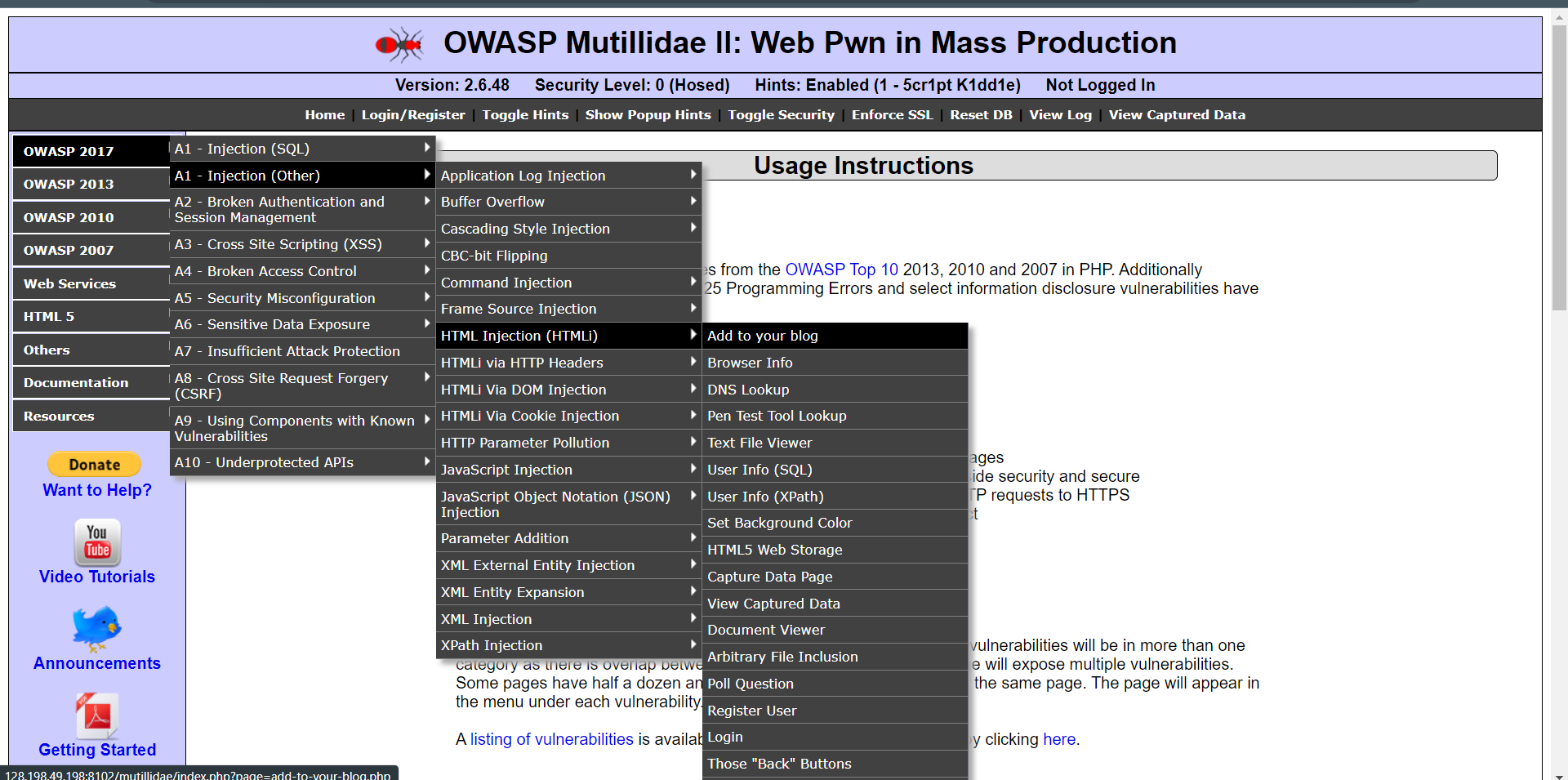
**Cross Site Scripting(XSS)**

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

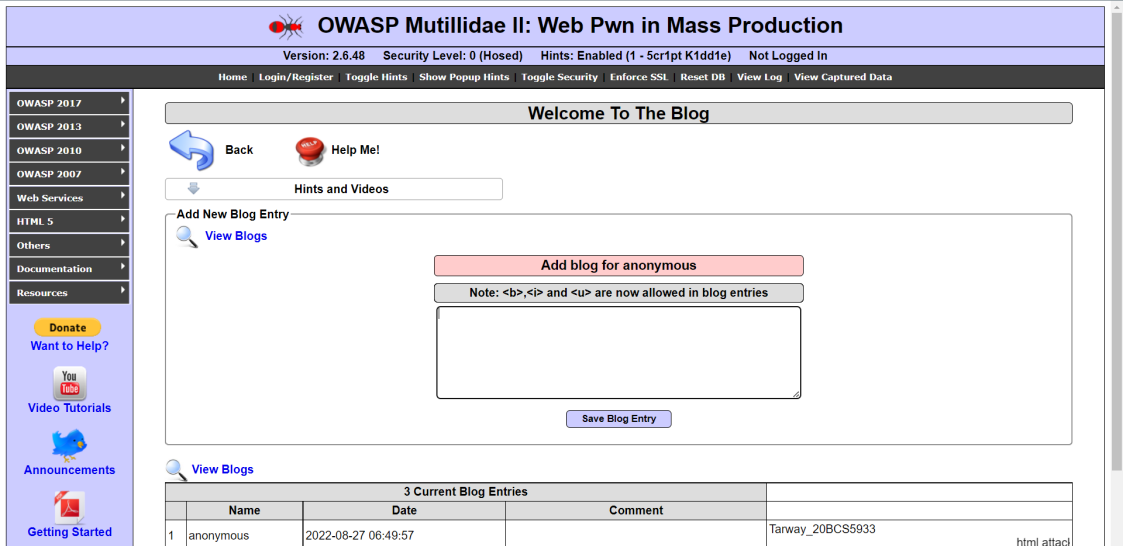
**Steps/Method/Coding:**

**HTML Injection**

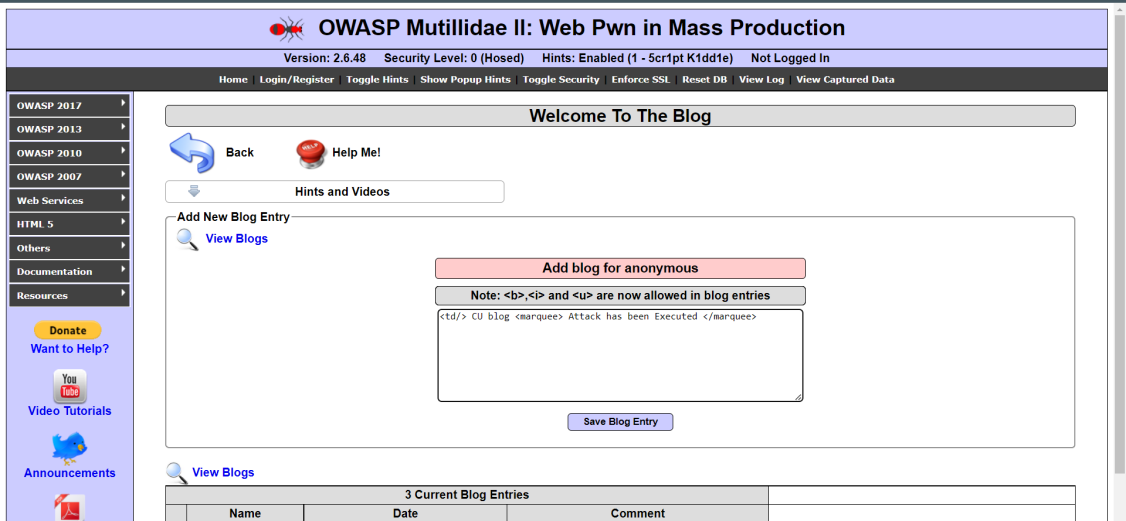
1. Open website : OWASP Mutillidae II: Web Pwn in Mass Production (URL: http://128.198.49.198:8102/mutillidae/index.php?page=documentation/usage-instructions.php)
2. Now, we’ll be redirected to the web page which is suffering from an HTML Injection vulnerability which allows the user to submit his entry in the blog.
3. On the left hand side, click on OWASP 2017🡪A1-injection(others)🡪HTML injection🡪Add to your blog screenshot)



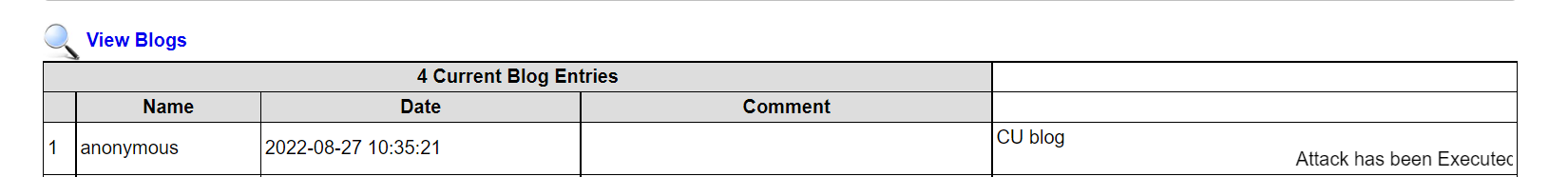
1. Welcome to blog window will appear on the screen. Now, let’s try to inject malicious code. Enter the HTML code inside the given text area in order to set up the HTML attack.



1. For example injected code is : <td/> CU blog <marquee> Attack has been Executed </marquee> then save blog entry.

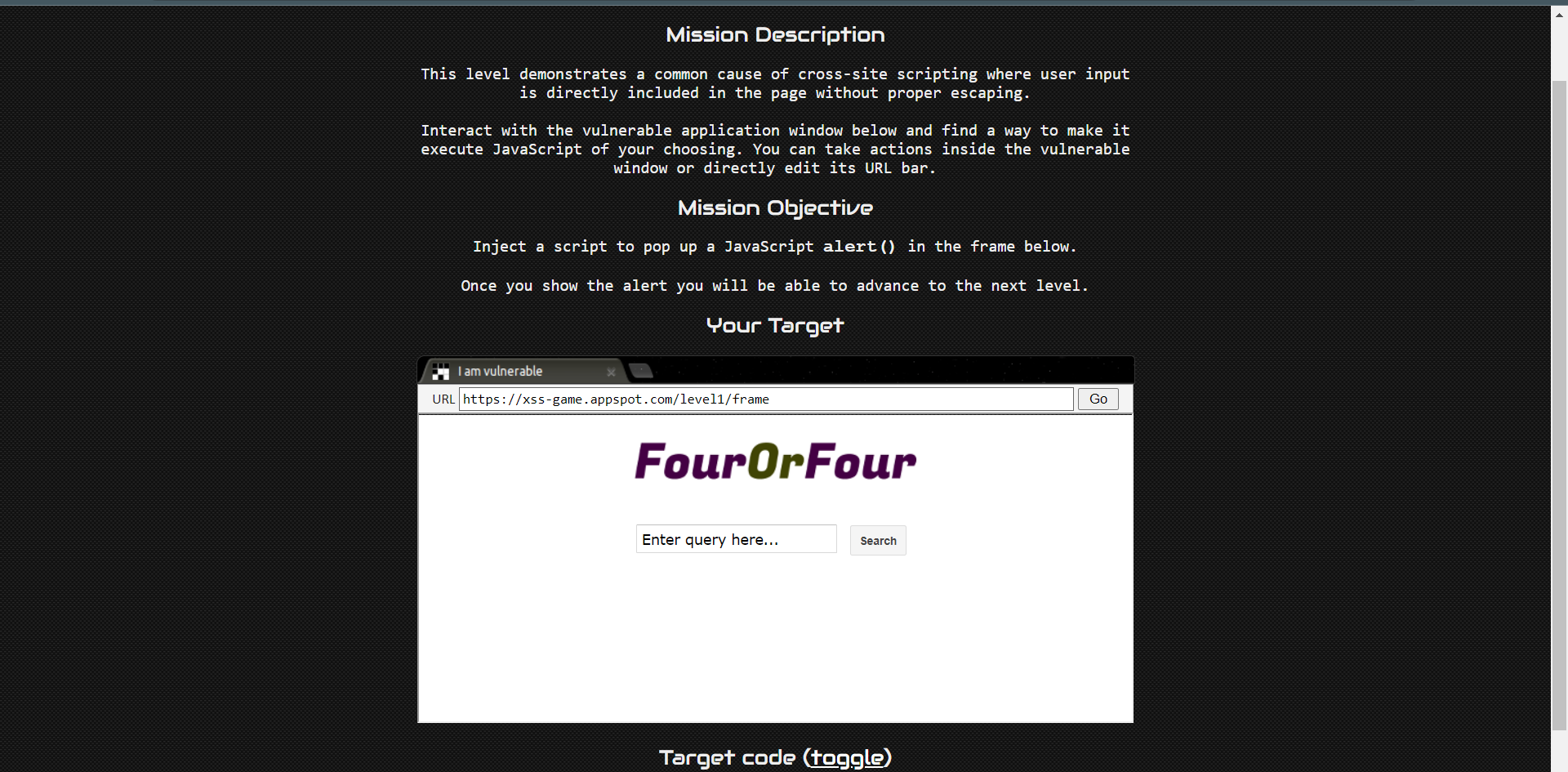


1. That html code is thus now into the application’s web server, which gets rendered every time whenever the victim visits this malicious page, he’ll always have this code which looks official to him



**XSS Attack**

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

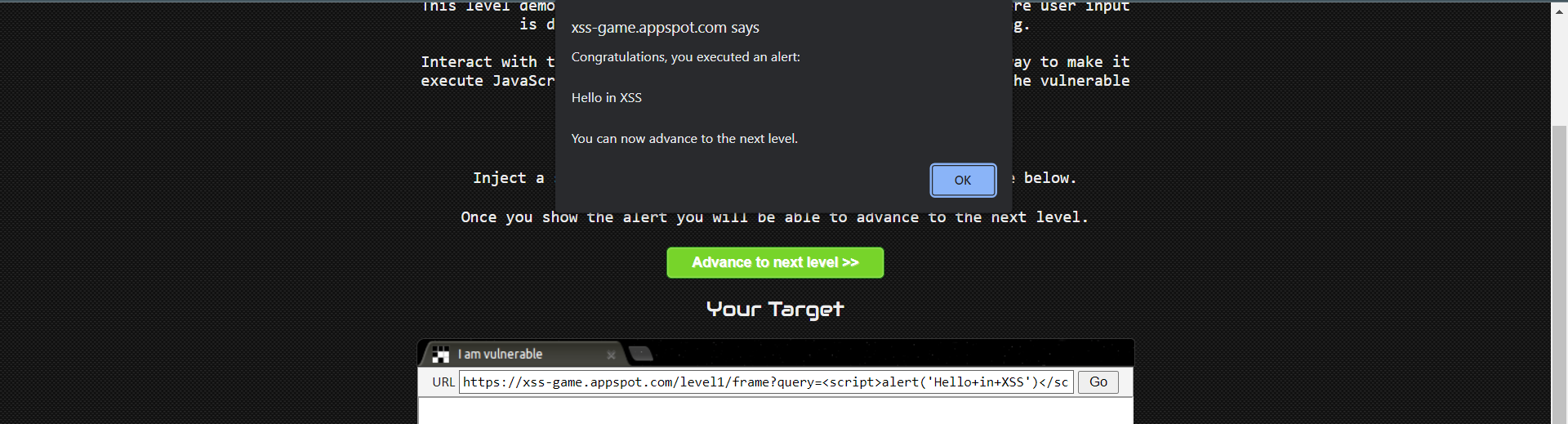


1. If the search field is vulnerable, when the user enters any script, then it will be executed. Consider, a user enters a very simple script as shown below

**<script>alert('Hello in XSS')</script>**

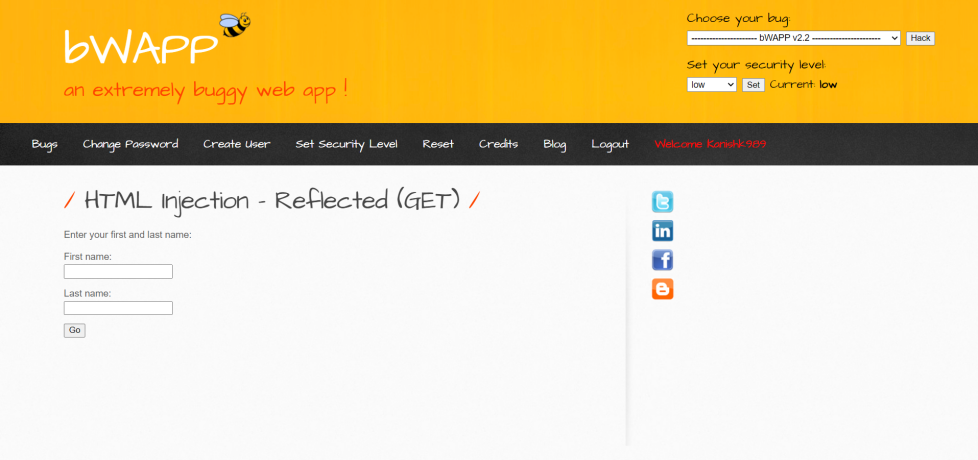


1. Then after clicking on the “Search” button, the entered script will be executed. The script typed into the search field gets executed. This just shows the vulnerability of the XSS attack

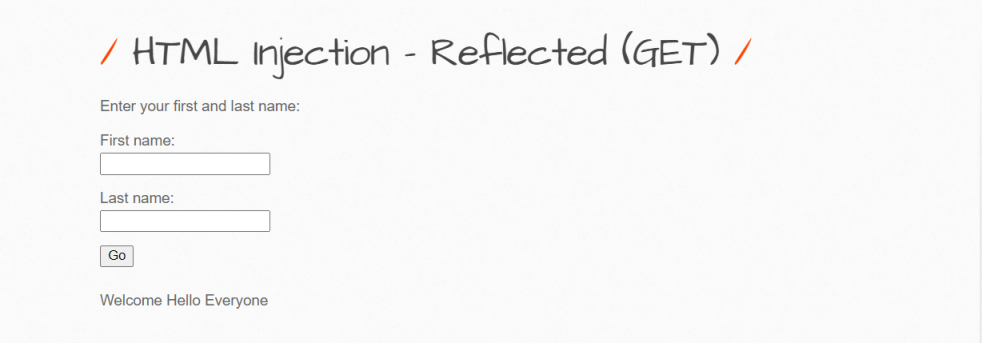


**HTML injection**

1. Open bwapp login page and login with default credentials given on the page.
2. Then you will see a page with this url :https://bwapp.hakhub.net/portal.php
3. Choose your bug(**HTML reflected GET**) on the top right corner and click on Hack.(low level)



1. Write anything in both input tags, it will reflect as output.

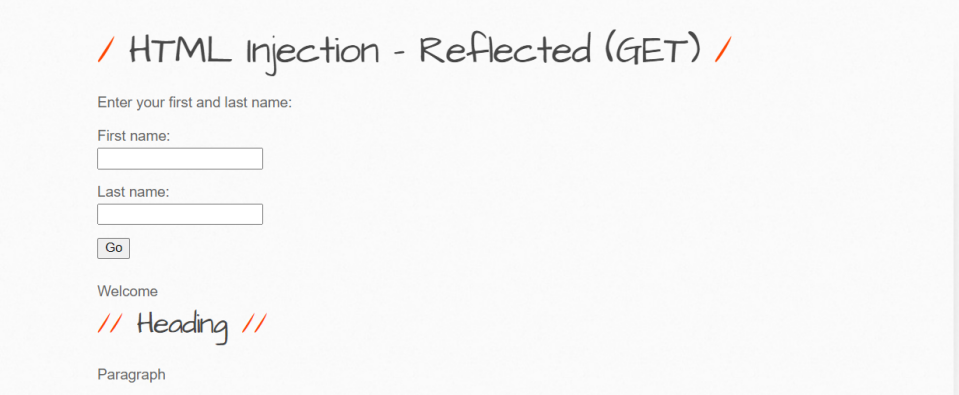


1. Now enter input with any html tag. E.g.

In 1st input field: <h1> Heading </h1>

In 2nd: <p>Paragraph</p>

Do vice versa and then fill both fields with html code



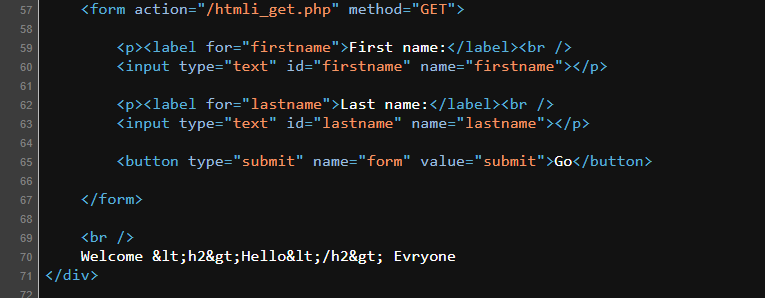
Both input fields are vulnerable with html attack.

1. Check same with medium level attack. Admin has applied some security measures on website.

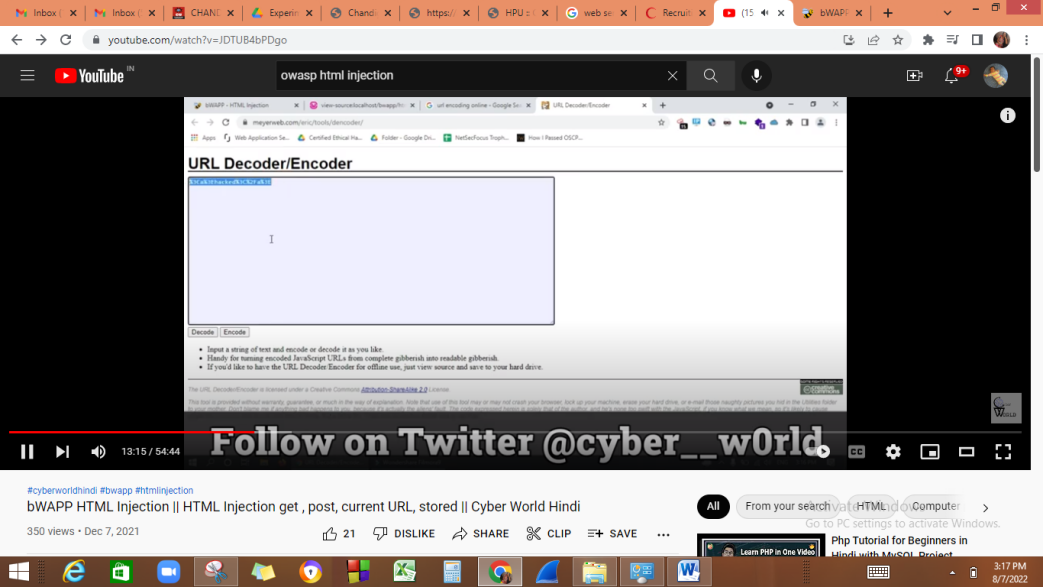
Click on go then check. Here tag is not executed successfully. Check with another tags also like <a> etc. Same result will appear.



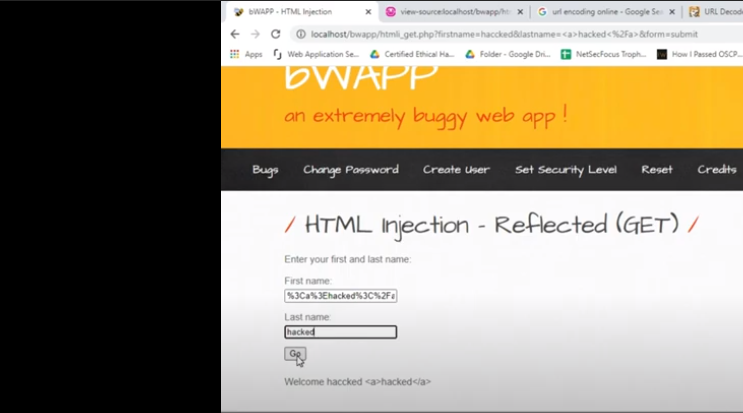
1. Right click on page and view source code. Check HTML reflected get code part. Angular brackets are encoded with lt and gt. This is url encoding. Check in browser URL also.

;

1. To bypass it, we will encode the input data that we are entering in input fields. Search url encoding online on google and encode it.

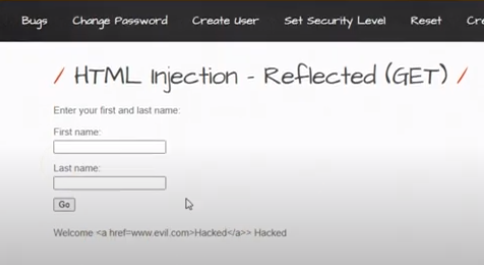


1. Inject encoded code in input fields. It will be executed.

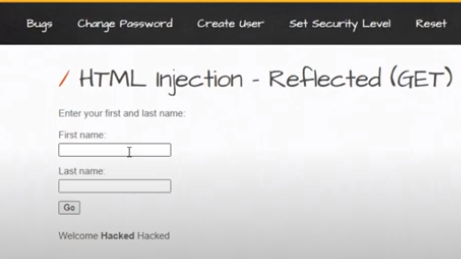




1. Let’s check for another tag. As it is not running so encode it and try again. It will be executed. A link will show for a corresponding input field in which you will enter <a> tag code.

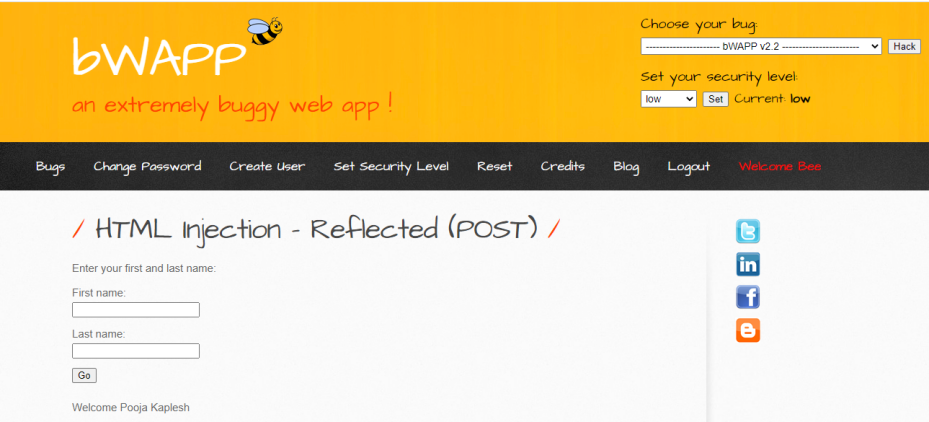


After encoding: Hacked is displayed as a link. Repeat and Check for both input fields.

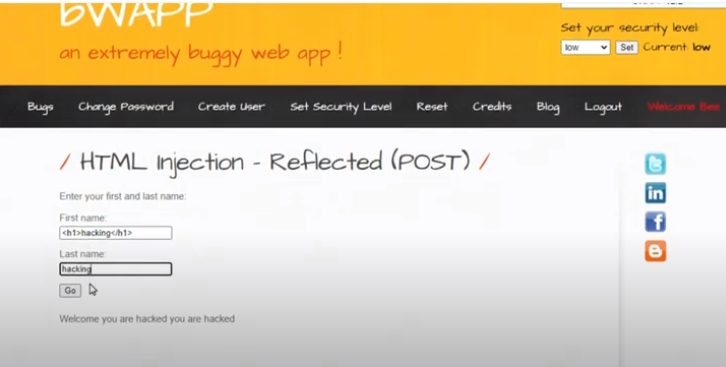


**HTML Injection-Reflected (POST)**

1. Login to bwapp and select HTML Reflected (POST) and click on Hack.



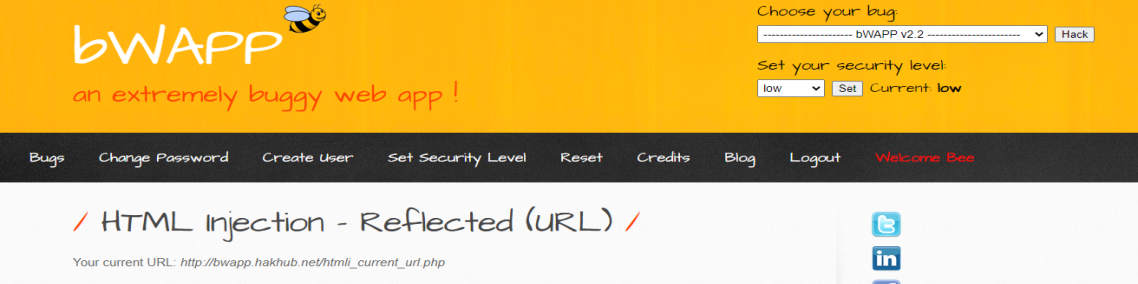
1. No parameters are shown in URL in POST method. Repeat same steps here as we have done in GET method and check all the cases.



If single encoding is not enough for bypassing the security then we can encode text twice.

**HTML Injection-Reflected (URL)**

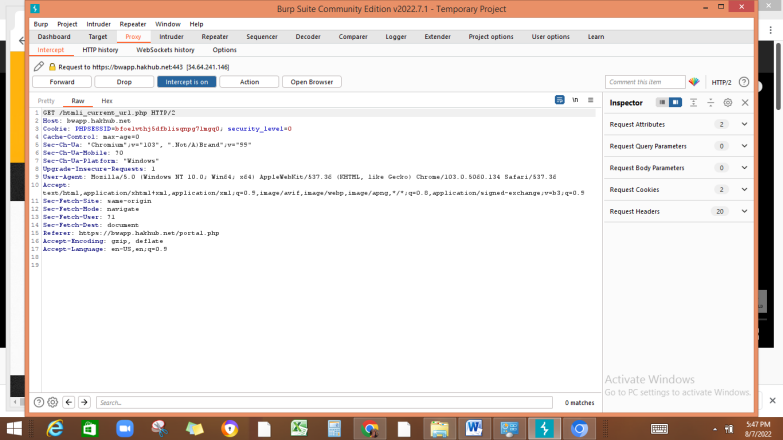
1. Choose you bug as HTML Injection-Reflected (URL).



1. Open burpsuite-> intercept off open browser open bwapp website here

<https://bwapp.hakhub.net/htmli_current_url.php>

1. Proxy is automatically set on the predefined browser.



1. **Change values as:**

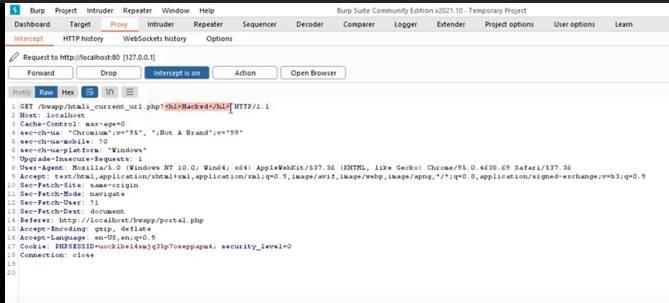
Php? <h1>hacked</h1> **//**anything after ? becomes input parameter

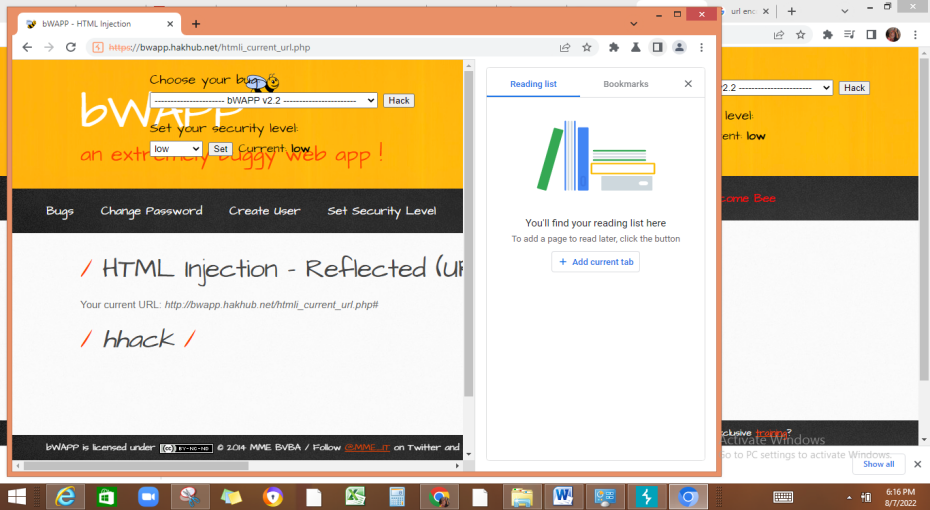
Host:evil.com

**Note: For http2, use # in place of ?**

**No need to change host name**

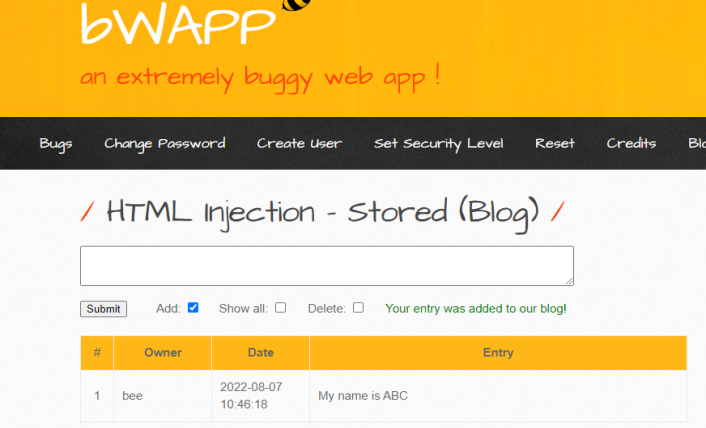
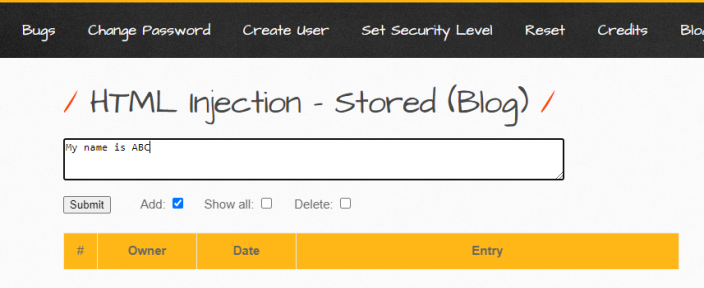
Then click on forward



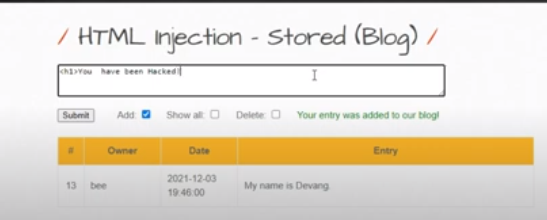


**HTML injection-Stored Blog**

1. Enter anything in input box and submit it. Entry will be stored in database



1. If attacker enters its malicious code or any link then it will be added there in database or this table. So if users access this website then they may be affected of the malicious code.
2. Enter any html code



**Learning Outcomes:**

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.