**Worksheet-2**

**Student Name:-** Pushpraj Roy **UID:-** 20BCS9866

**Branch:-** BE- CSE **Section/Group:-** WM\_617 “A”

**Subject Code:-** 20CSP-338 **Semester:-** 5th **Subject Name:-** Web and Mobile Security Lab

**Aim:** Design a method to simulate the html injection to exploit the attackers.

**Software/Hardware Requirements:** Windows 7 & above version

**Tools to be used:**

1. Bwapp or bugg web application

2. Microsoft Word

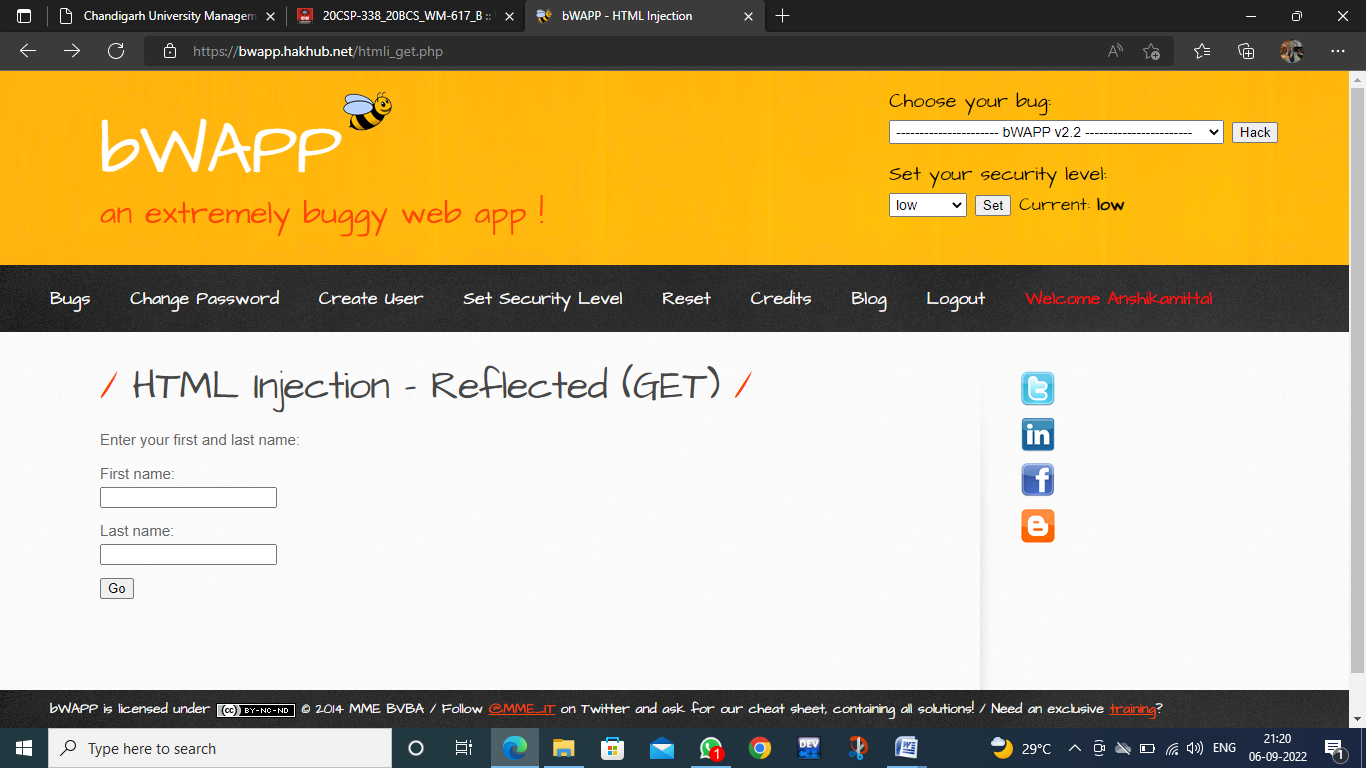
**Introduction:** Html injection is also known as a cross-site scripting. It is a security vulnerability that allows an attacker to inject html code into web pages that are viewed by other users. It can steal the data from the user.

Bwapp or a bugg web application is a free and open source application that helps security enthusiast developers and students to discover and prevent web vulnerabilities.

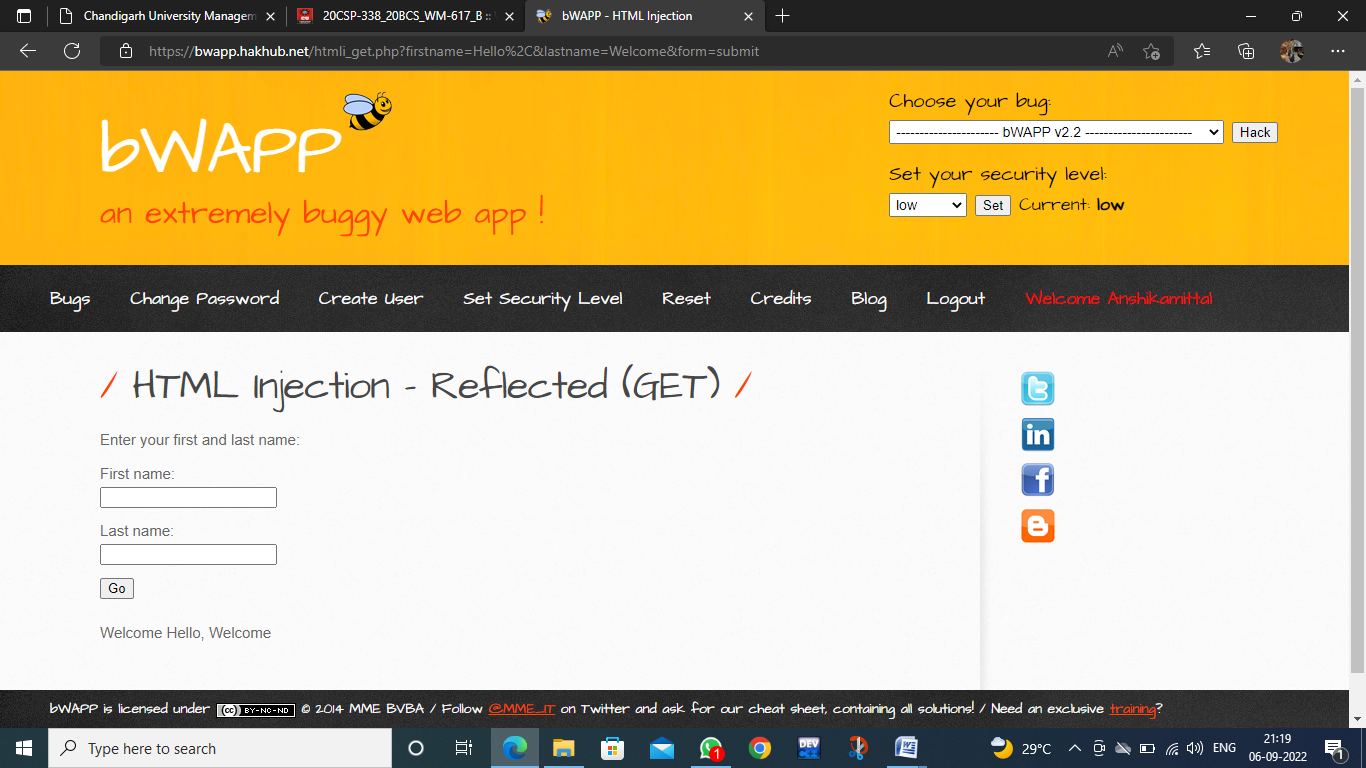
Bwapp is a php application that uses MySQL database.

**HTML Injection:**

1. Open bwapp login page and login with default credentials given on the page.
2. The 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.

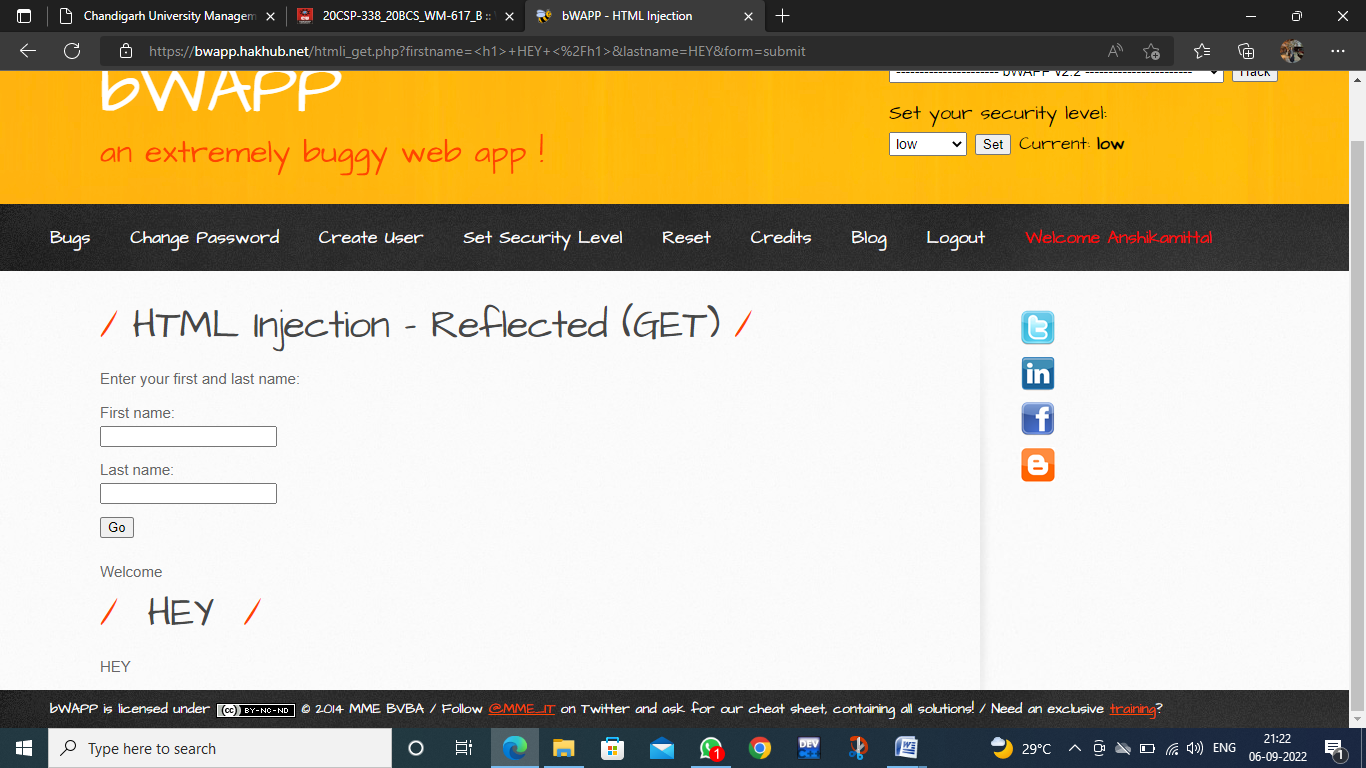


1. Now enter input with any html tag. E.g.

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

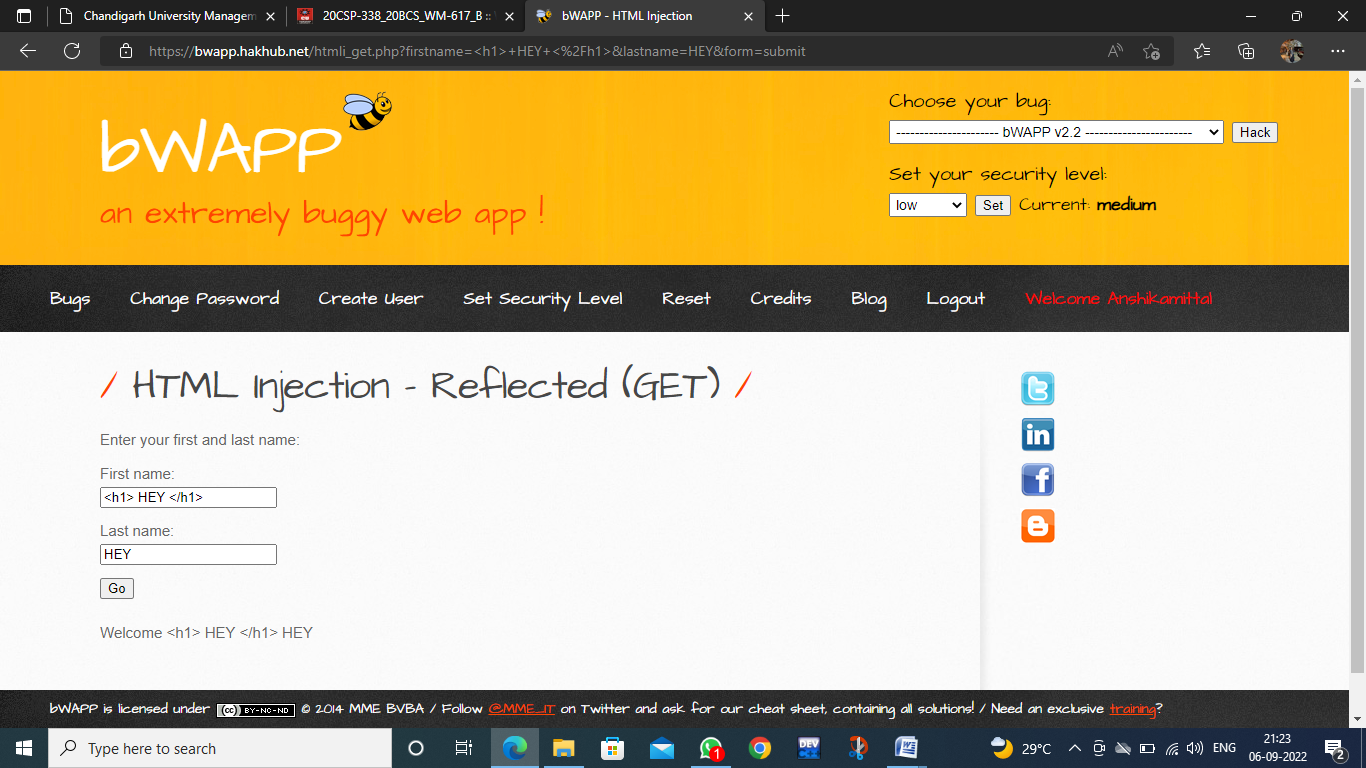
In 2nd: Hello

Do vice versa and then fill both fields with html code

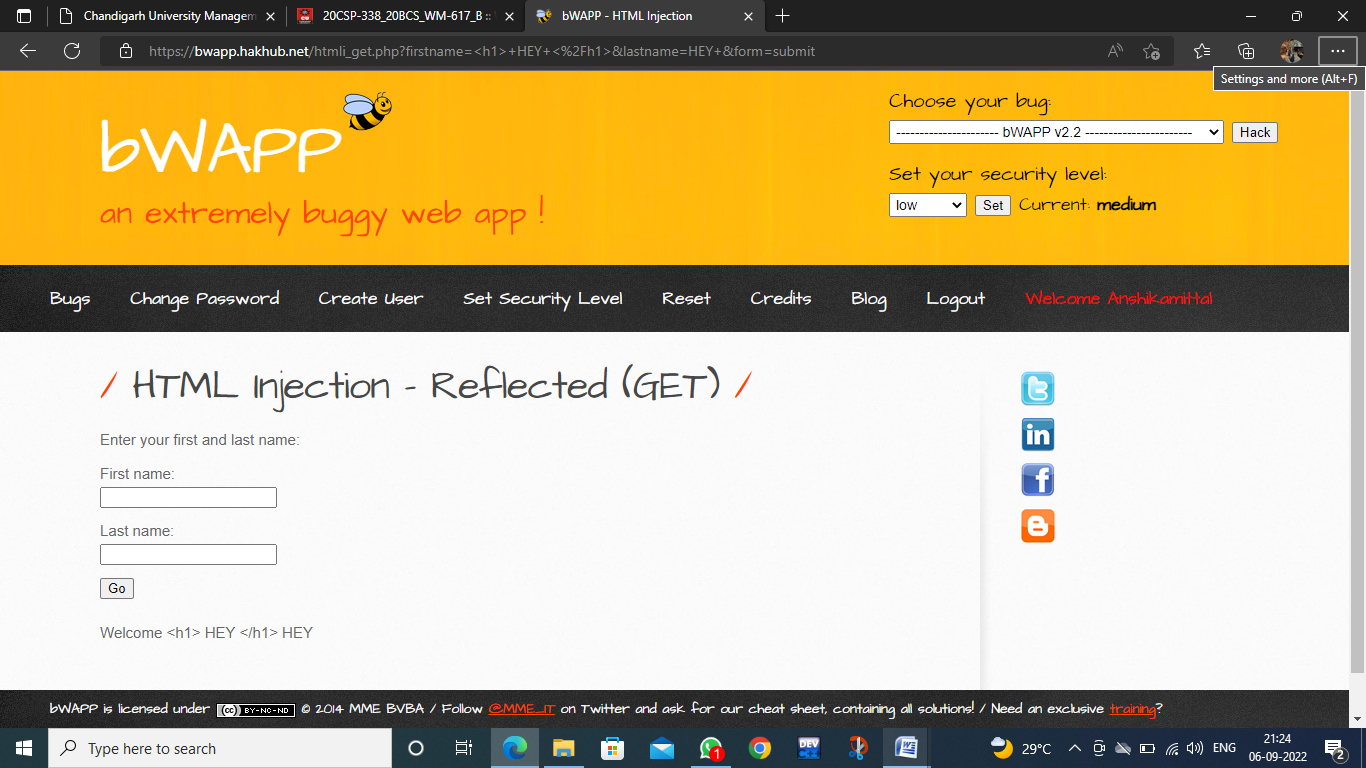


Both input fields are vulnerable with html attack.

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



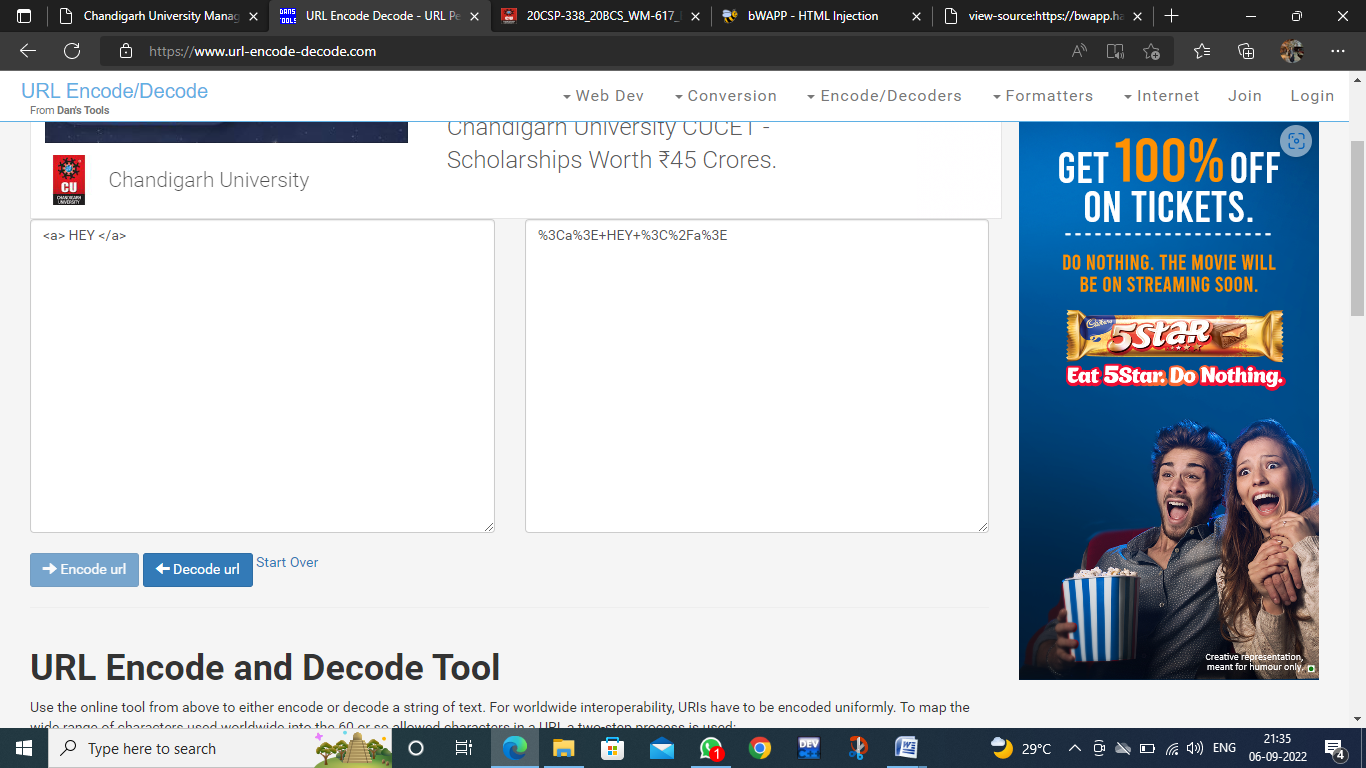
Click on go then check. Here tag is not executed successfully. Check with another tags also like <a> etc. Same result will appear.



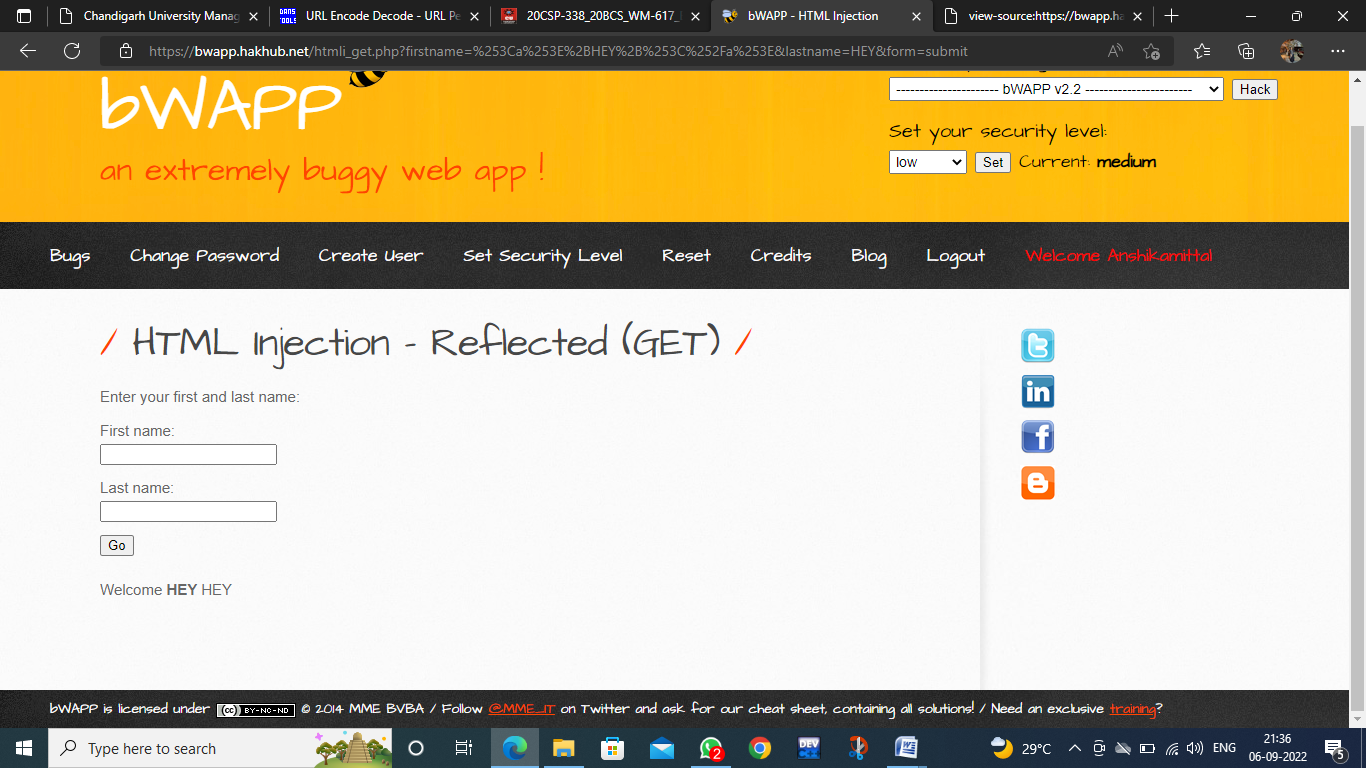
1. Right click on page and view source code. Check HTML reflected get code part. Angular brackets are encoded with lt and gt. This is url encoding. Check in browser URL also.



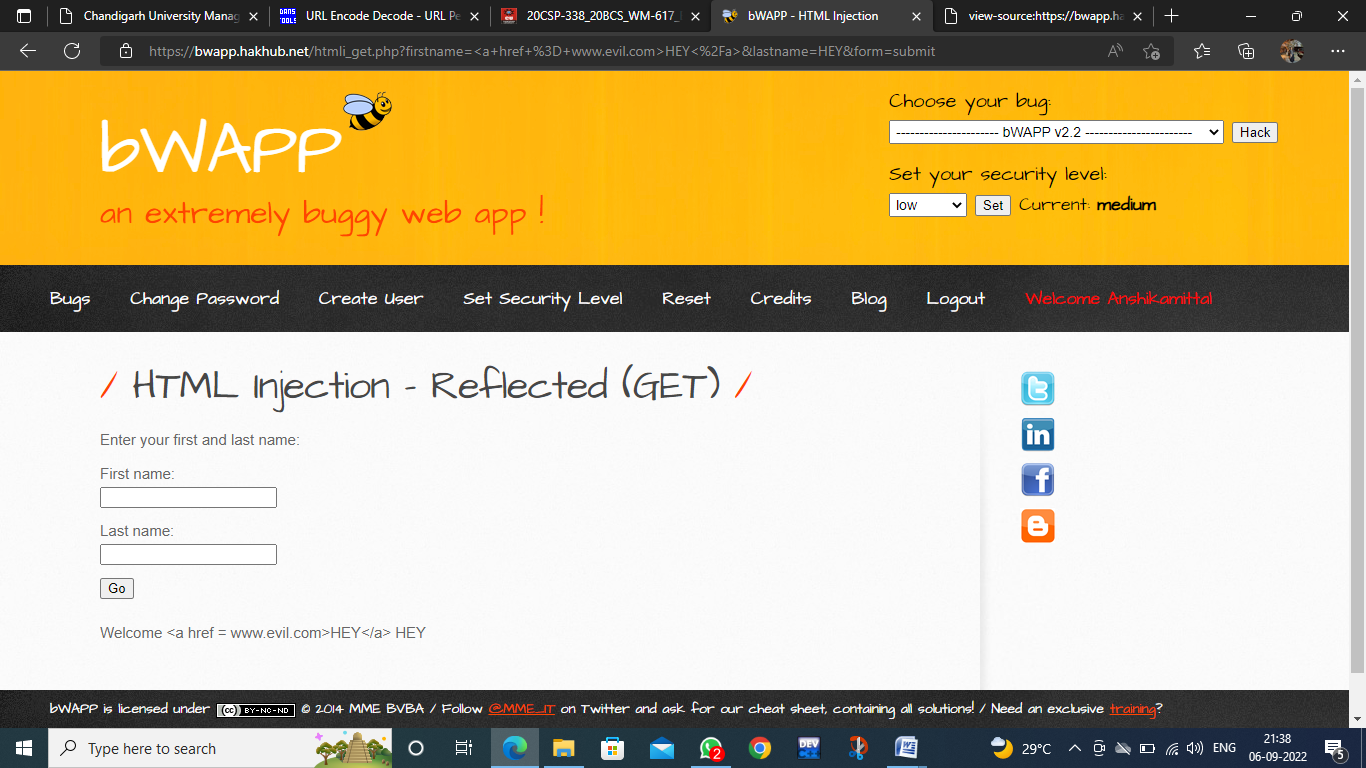
1. To bypass it, we will encode the input data that we are entering in input fields. Search url encoding online on google and encode it.



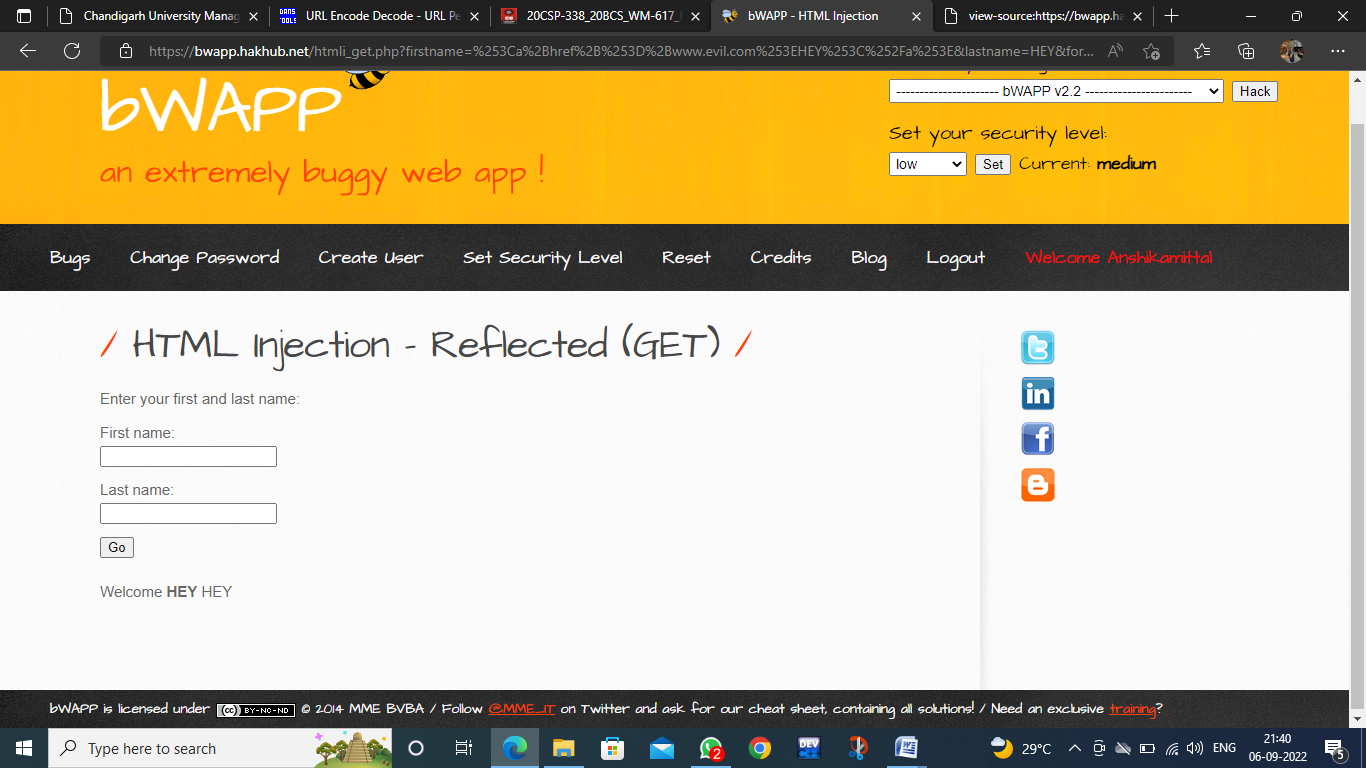
1. Inject encoded code in input fields. It will be executed.



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.

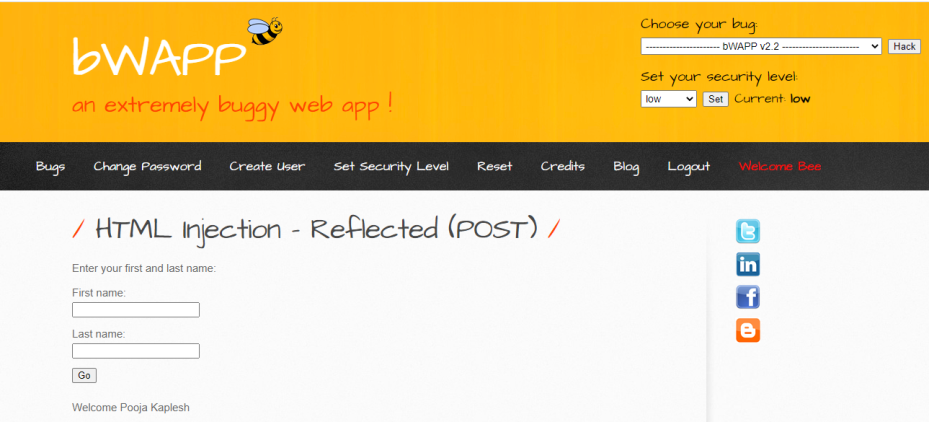


After encoding: Hacked is displayed as a link. Repeat and Check for both input fields.

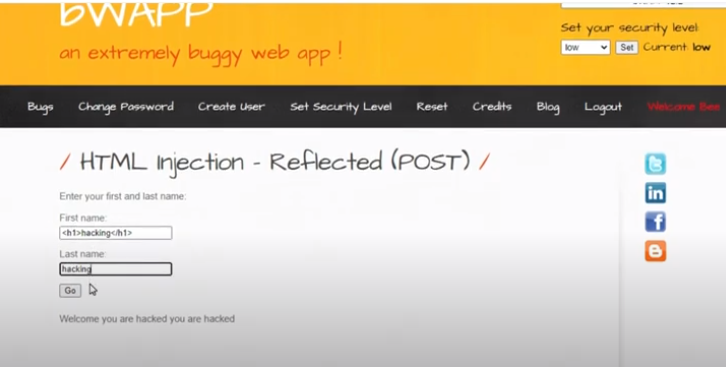
****

**HTML Injection-Reflected(POST)**

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



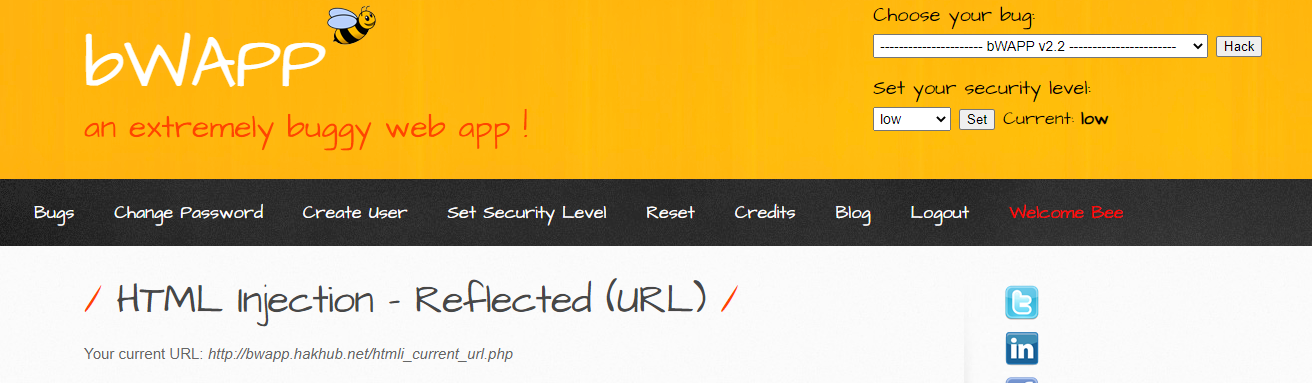
1. No parameters are shown in URL in POST method. Repeat same steps here as we have done in GET method and check all the cases.



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

**HTML Injection-Reflected (URL)**

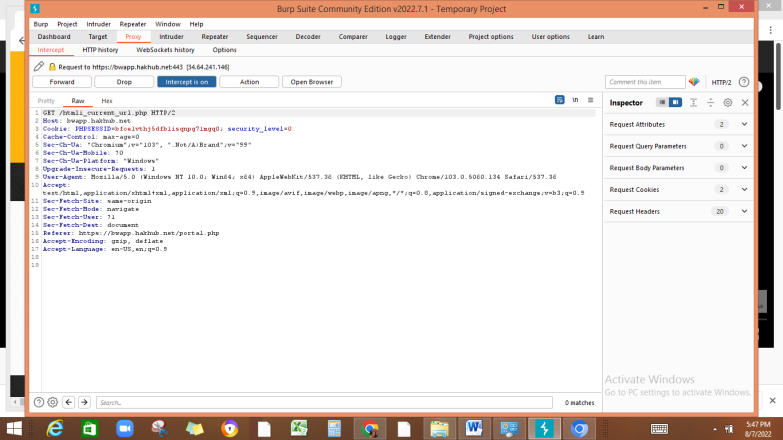
1. Choose you bug as HTML Injection-Reflected (URL).



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

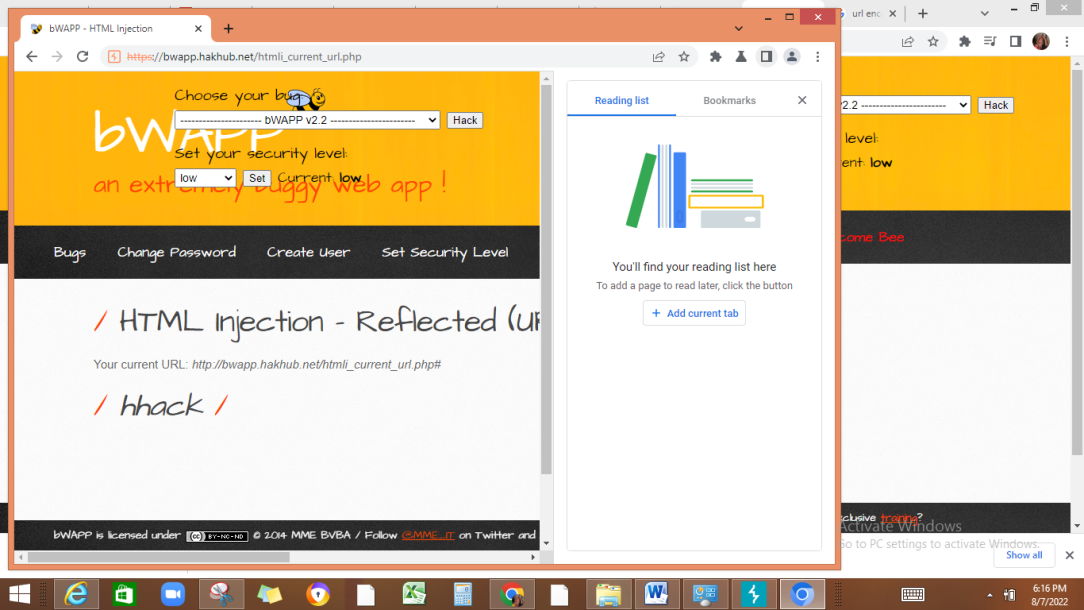
Host:evil.com

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

**No need to change host name**

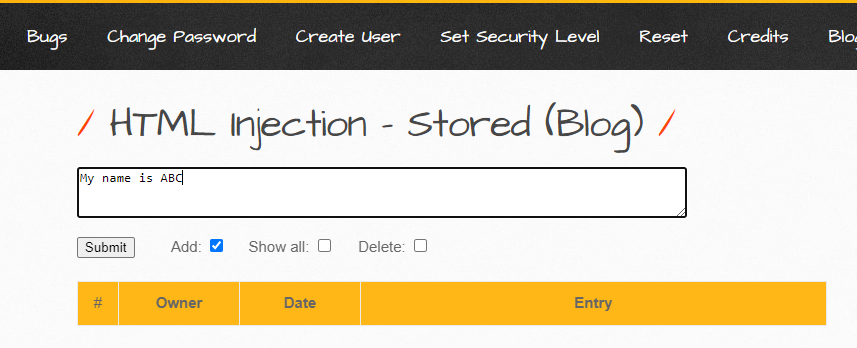
Then click on forward

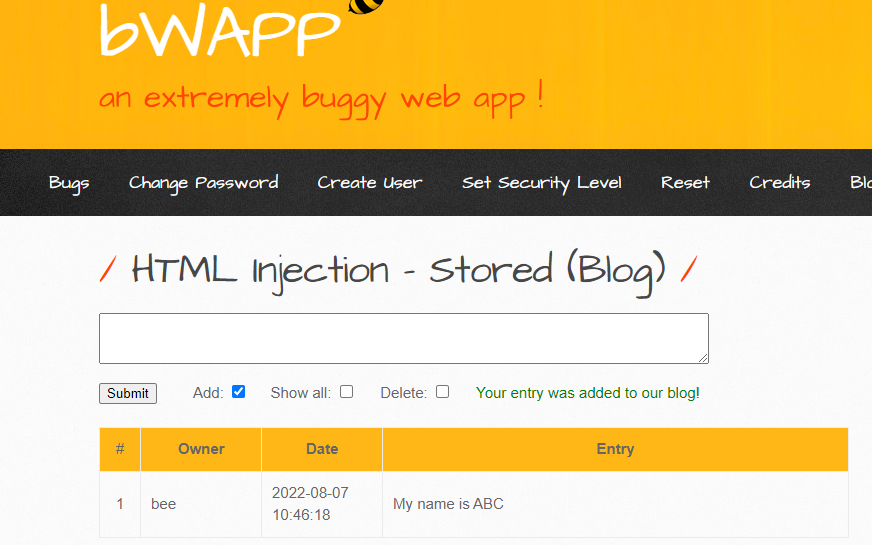




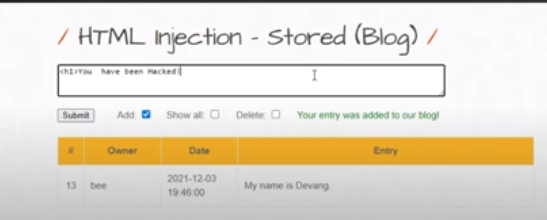
**HTML injection-Stored Blog**

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





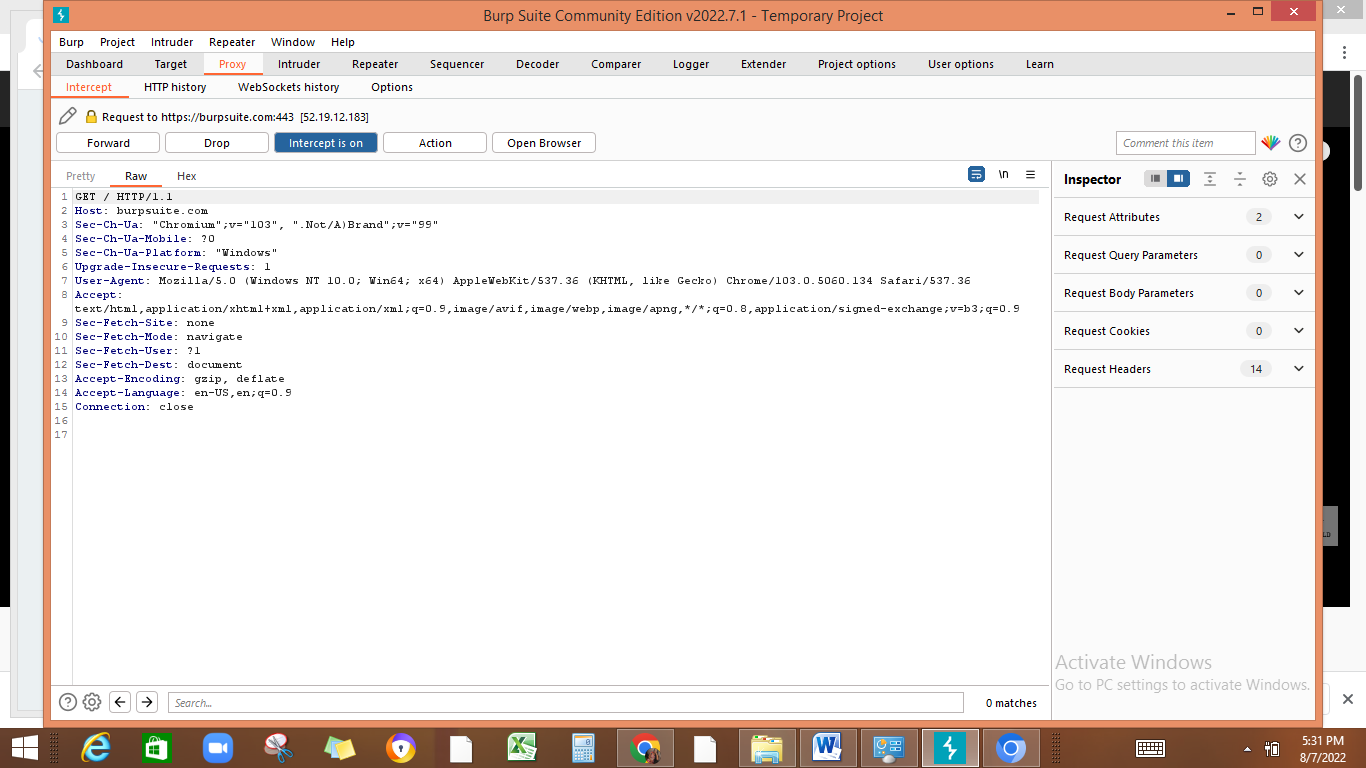
1. If attacker enters its malicious code or any link then it will be added there in database or this table. So if users access this website then they may be affected of the malicious code.
2. Enter any html code



**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.