ali baddawi

UOP

Burp suite

**What is Burp Suite :**

**Burp Suite is a powerful tool used for security testing of web applications. It's developed by PortSwigger and is popular among security professionals for its comprehensive features. Here's a rundown of what Burp Suite offers:**

**Key Features of Burp Suite**

1. **Proxy:**
   * **Acts as an intercepting proxy, letting you capture, inspect, and modify traffic between your browser and the target web application.**
   * **Essential for manual testing, as it helps you analyze and tweak HTTP/S requests and responses.**
2. **Scanner:**
   * **Automates the detection of security vulnerabilities like SQL injection and cross-site scripting (XSS).**
   * **Performs both passive and active scans to identify potential issues.**
3. **Intruder:**
   * **Automates customized attacks, such as brute force attacks, fuzzing, and parameter manipulation.**
   * **You can set up payloads and attack positions to test for various vulnerabilities.**
4. **Repeater:**
   * **Allows you to manually modify and resend individual HTTP/S requests.**
   * **Useful for testing how web applications respond and confirming vulnerabilities.**
5. **Sequencer:**
   * **Analyzes the randomness of session tokens and other data.**
   * **Helps identify weak or predictable tokens that could be exploited.**
6. **Decoder:**
   * **Decodes or encodes data in formats like Base64 and URL encoding.**
   * **Useful for understanding and manipulating encoded data.**
7. **Comparer:**
   * **Compares two pieces of data side-by-side.**
   * **Often used to spot differences in responses that might indicate vulnerabilities.**
8. **Extender:**
   * **Enhances Burp Suite's capabilities with extensions and plugins from the BApp Store.**
   * **You can also write custom extensions using the Burp Extender API.**

**Editions of Burp Suite**

1. **Community Edition:**
   * **Free with limited features.**
   * **Good for learning and basic manual testing.**
2. **Professional Edition:**
   * **Paid with full access to all features, including automated scanning and advanced tools.**
   * **Widely used by security professionals for comprehensive testing.**
3. **Enterprise Edition:**
   * **Designed for large-scale automated scanning.**
   * **Ideal for organizations needing to integrate security testing into their development processes.**

**Typical Use Cases**

* **Web Application Security Testing:**
  + **Finding and exploiting security vulnerabilities.**
  + **Conducting penetration tests and ethical hacking.**
* **Development and QA:**
  + **Helping developers and QA teams spot security issues during development.**
* **Bug Bounty Programs:**
  + **Used by security researchers to find and report vulnerabilities.**

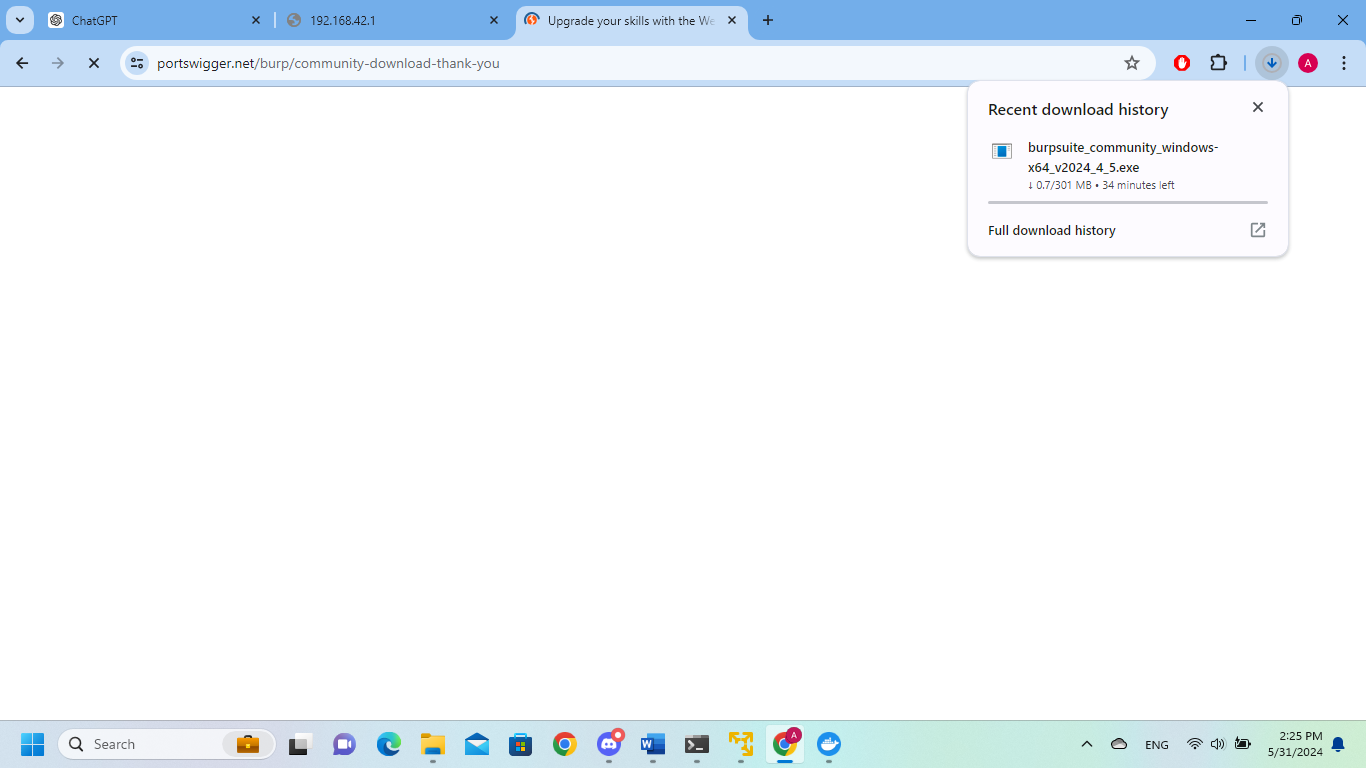
**How to Use Burp Suite**

1. **Set Up Burp Suite:**
   * Install Burp Suite on your system (Windows, macOS, or Linux).

**Intalling for windows :**

**Go to port swigger site and download the community edition   
A screenshot of a computer

Description automatically generated**

****

**Then run the Exe file and install the burp suite .**

**For docker desktop :**

**Search for the image on google and open gethub .**

A screenshot of a computer

Description automatically generated

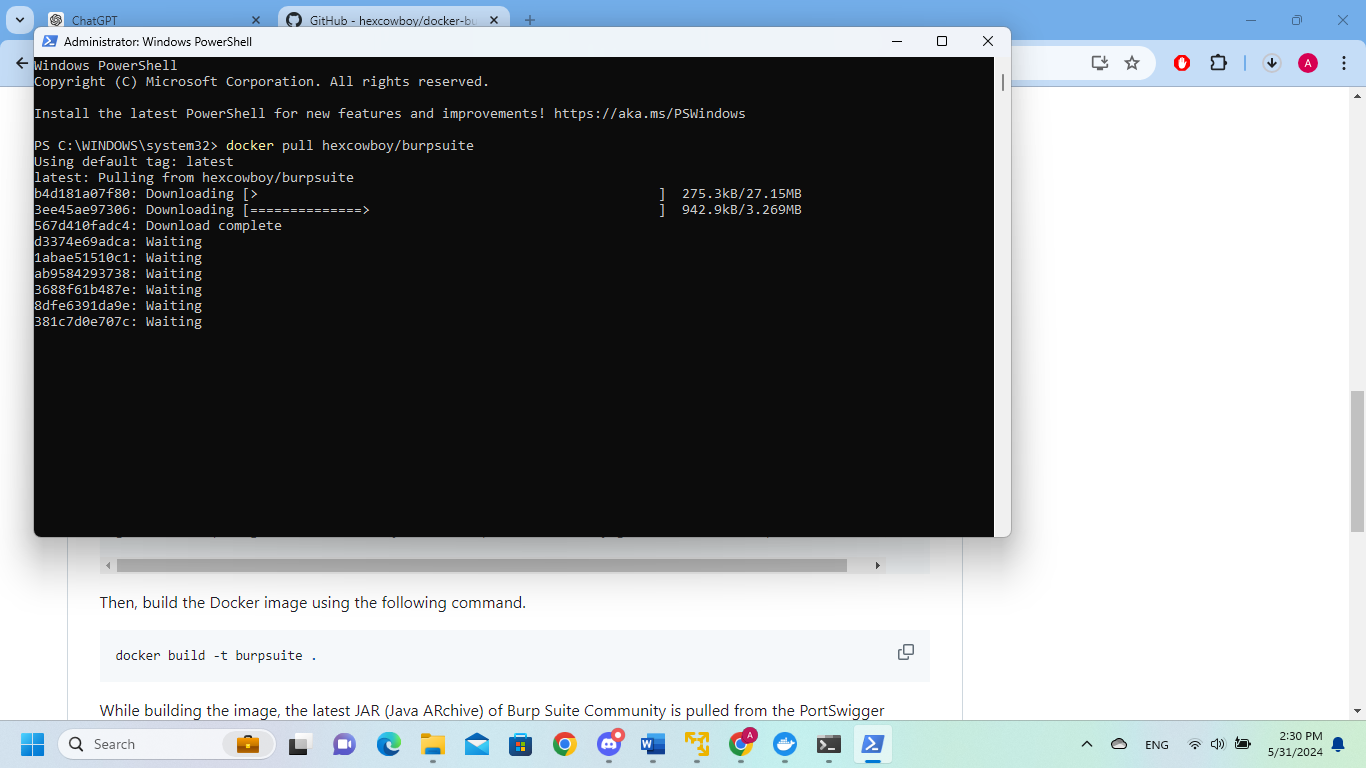
**Then you will find the commands to install and run the image on power shell**

A screenshot of a computer

Description automatically generated

**I will run throw the commands with a screenshots to make it clearer .**

**docker pull hexcowboy/burpsuite**

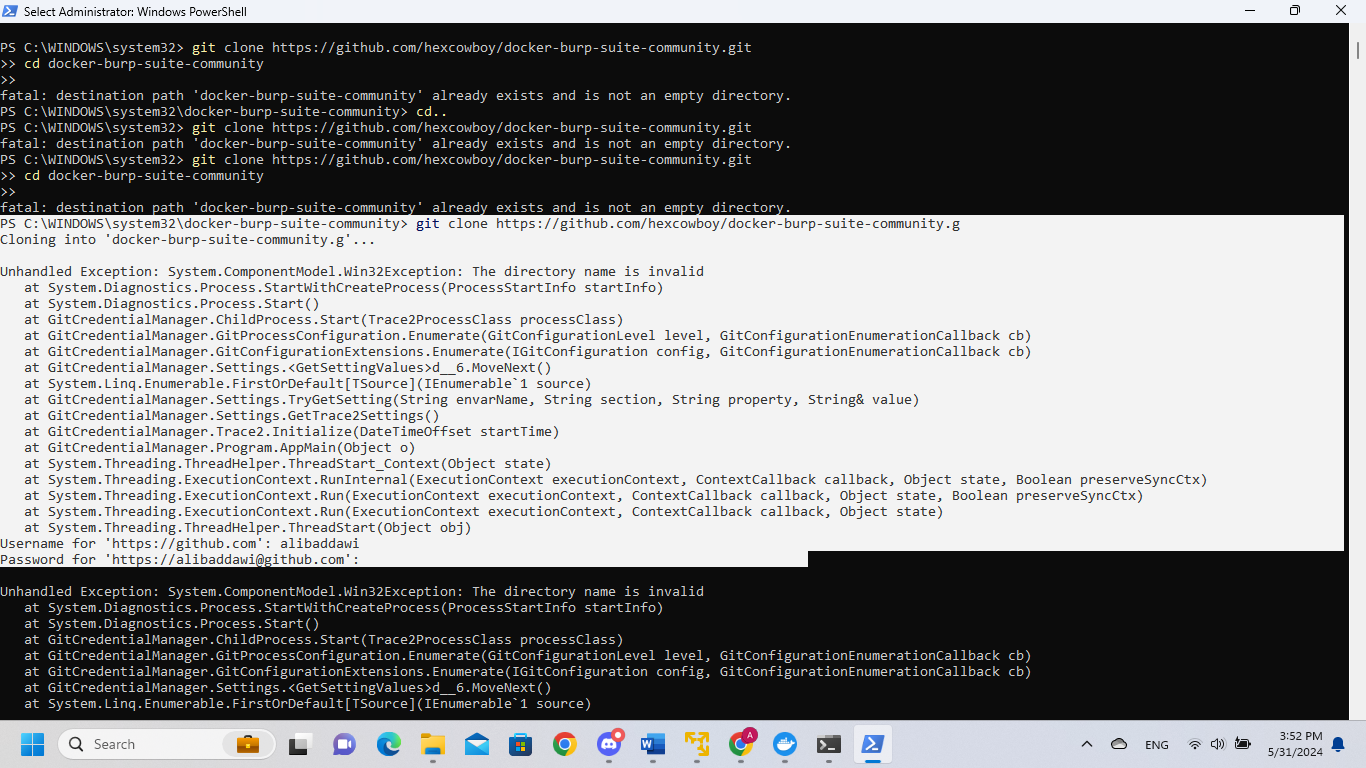


**docker image tag hexcowboy/burpsuite burpsuite**

A screenshot of a computer

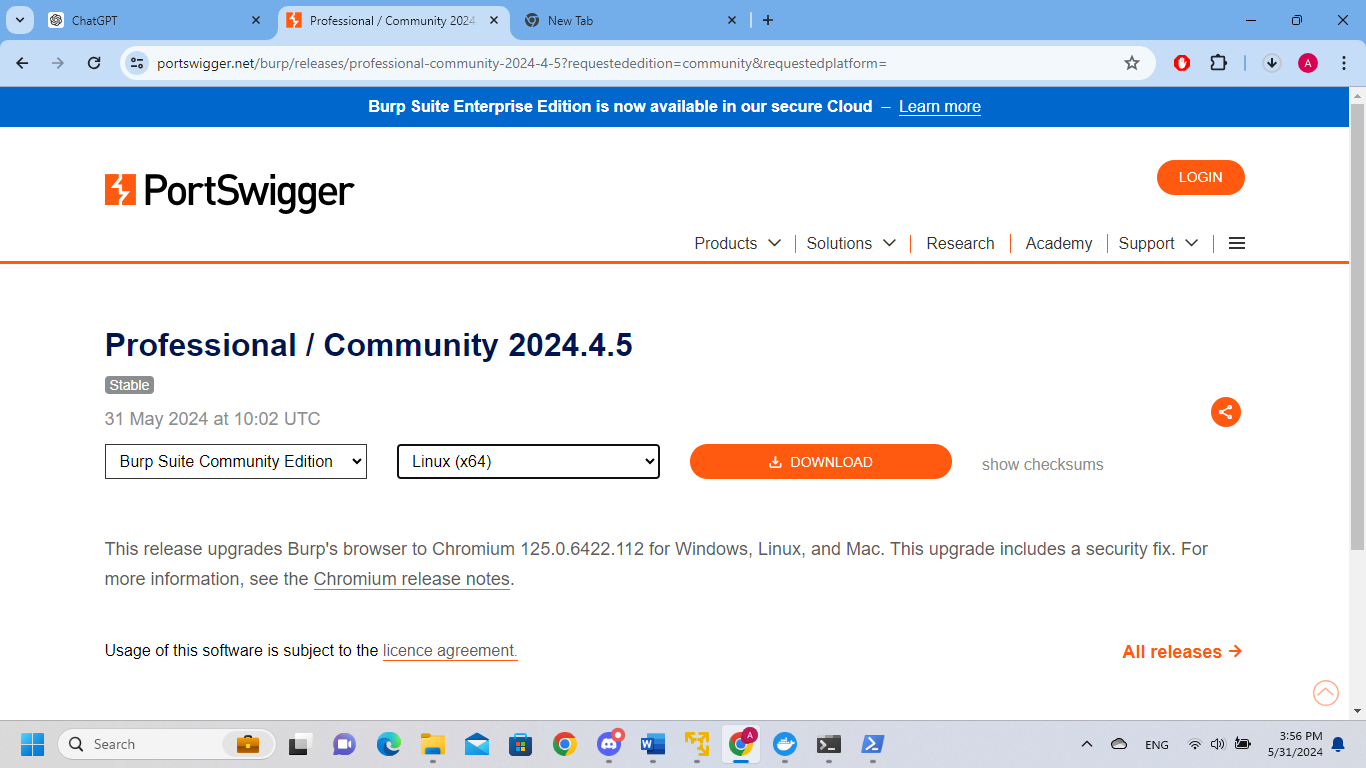
Description automatically generated

**then set up the clone**



**For linux :**

**Just like windows , you can just choose which OS you need to install the tool to .**



* + Configure your browser to use Burp Suite's proxy.

1. **Intercept Traffic:**
   * Capture and inspect HTTP/S requests and responses.
2. **Scan for Vulnerabilities:**
   * Use the automated scanner to find common vulnerabilities.
3. **Manual Testing:**
   * Use tools like Repeater, Intruder, and Sequencer for in-depth testing.
4. **Analyze Results:**
   * Review scan results and intercepted traffic for security issues.
5. **Report Findings:**
   * Document vulnerabilities and recommend fixes.

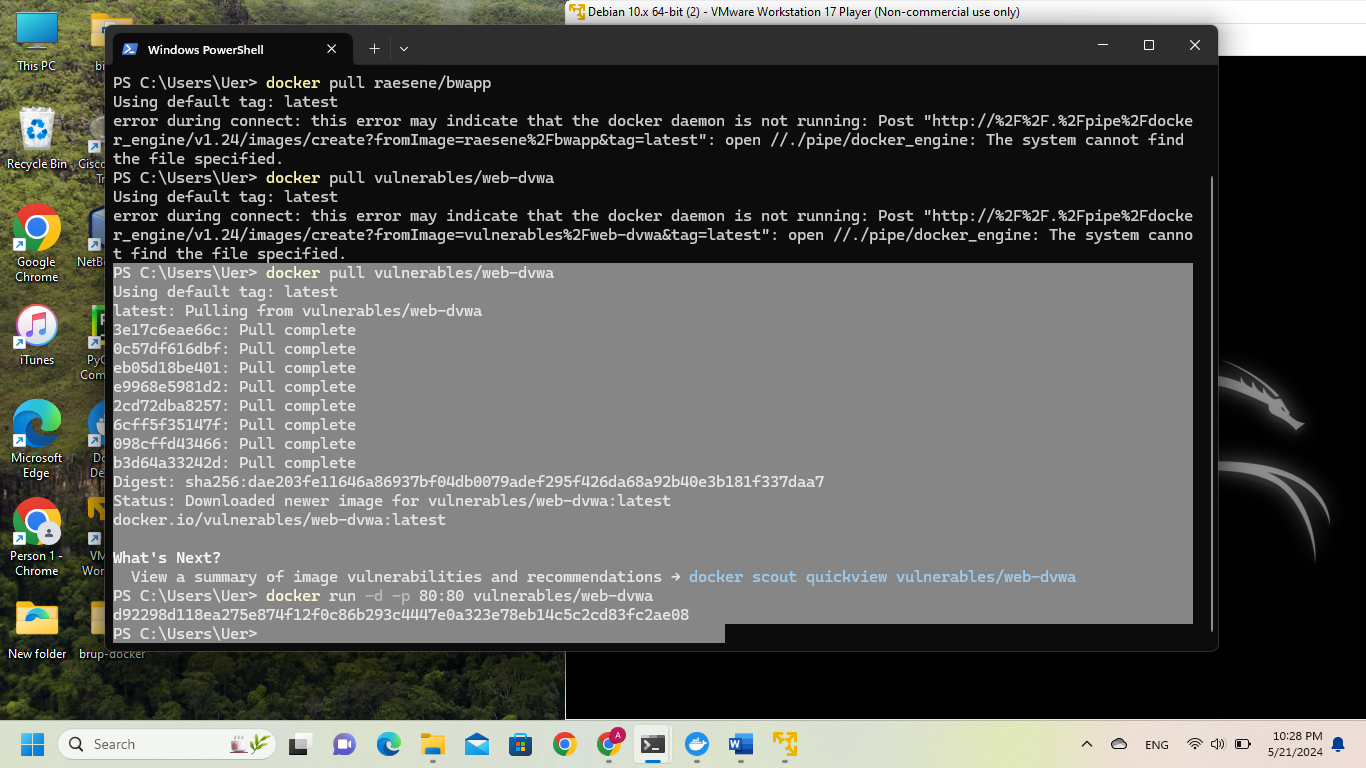
Burp Suite is a versatile tool that plays a crucial role in ensuring the security of web applications, making it a favorite among security experts.

**Scenario #1 (SQLI)**

So first of all , I set up a vulnerable web server using docker and I made sure to make it vulnerable for the sqli with the port 80:80 .

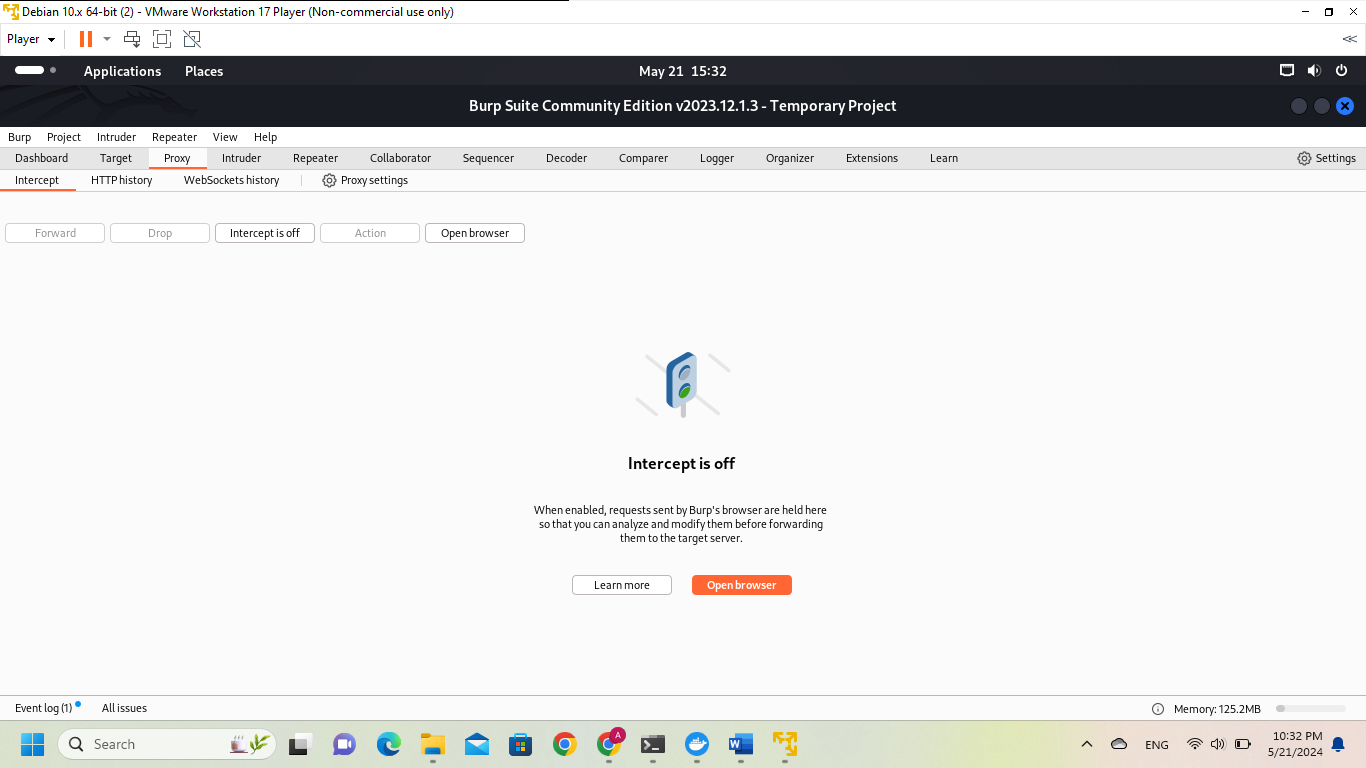
Command on shell: docker pull vulnerables/web-dvwa

To run the container : docker run -d -p 80:80 vulnerables/web-dvwa

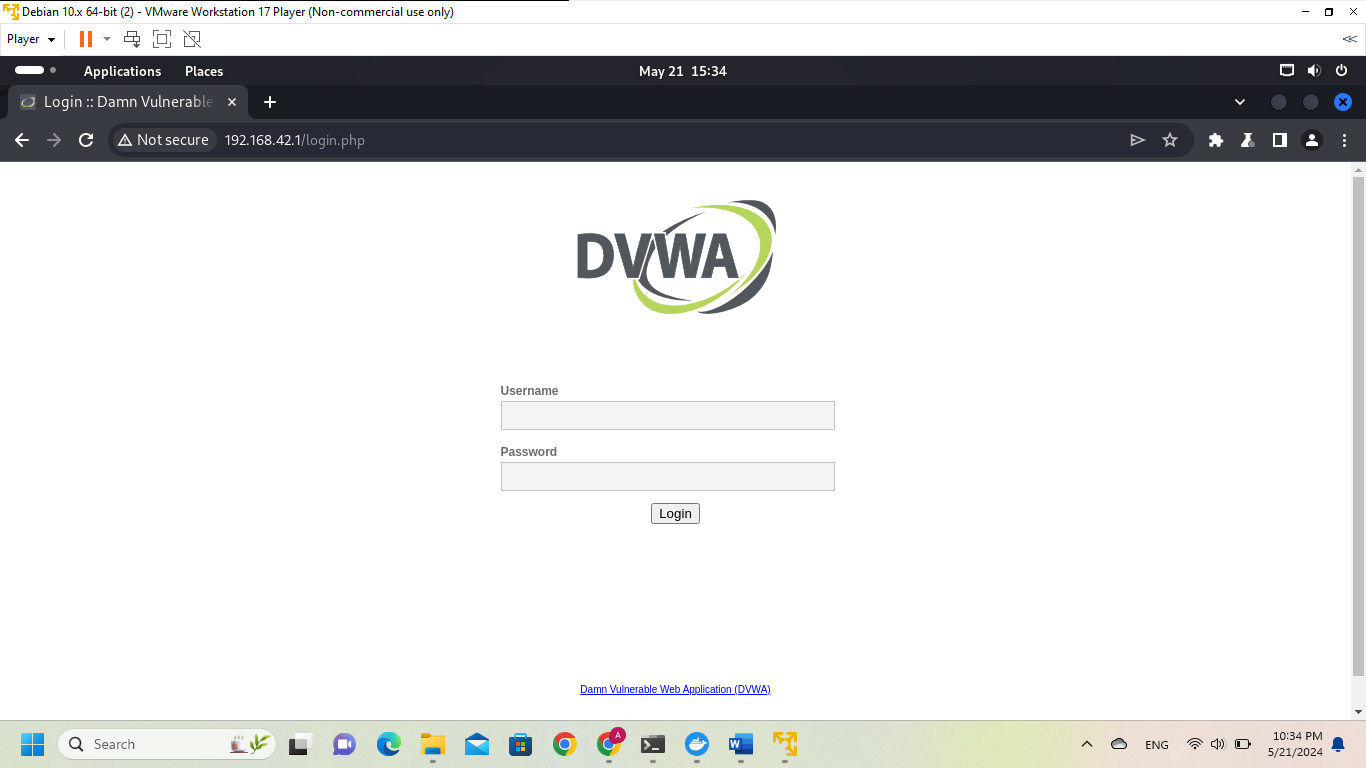


Secondly , I will access the web application using the burp suite by following these steps :

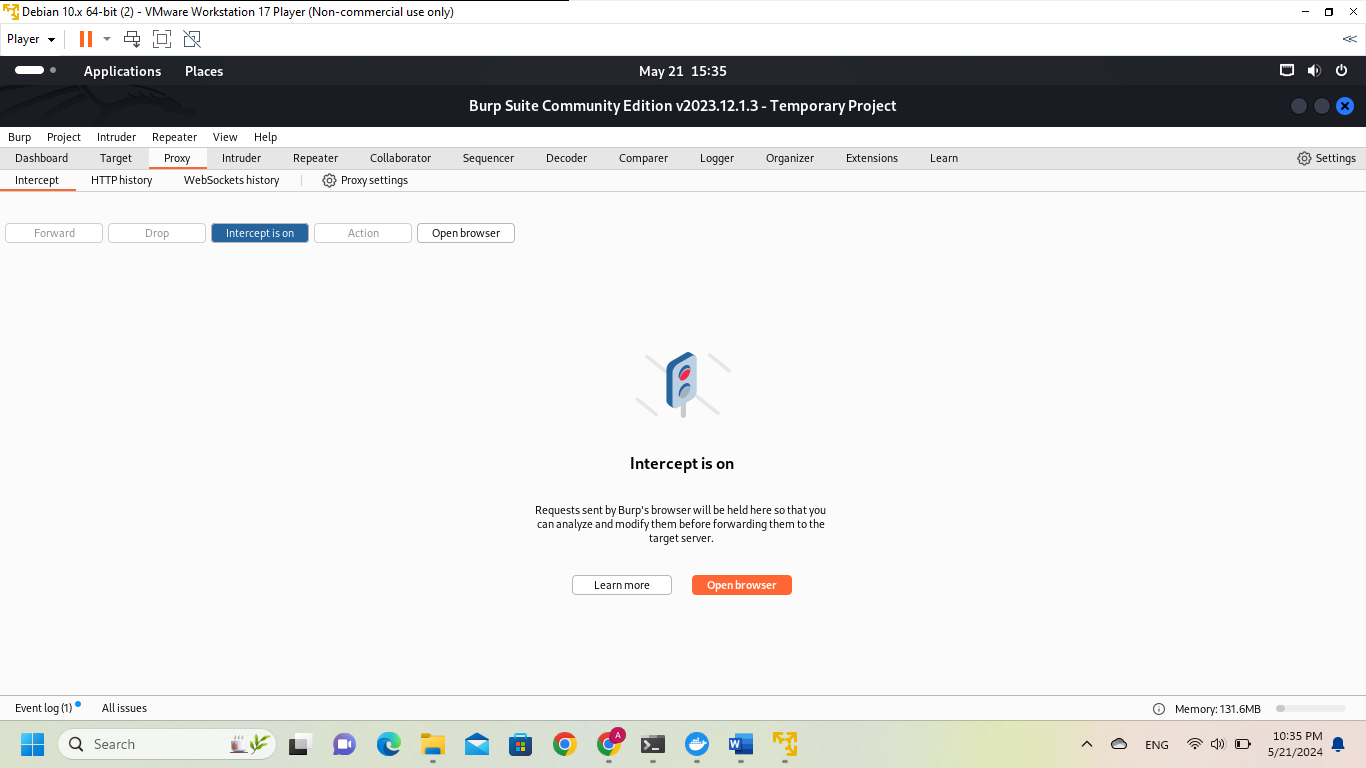
1. I will run the burp suite and go to proxy tab then click on open browser .

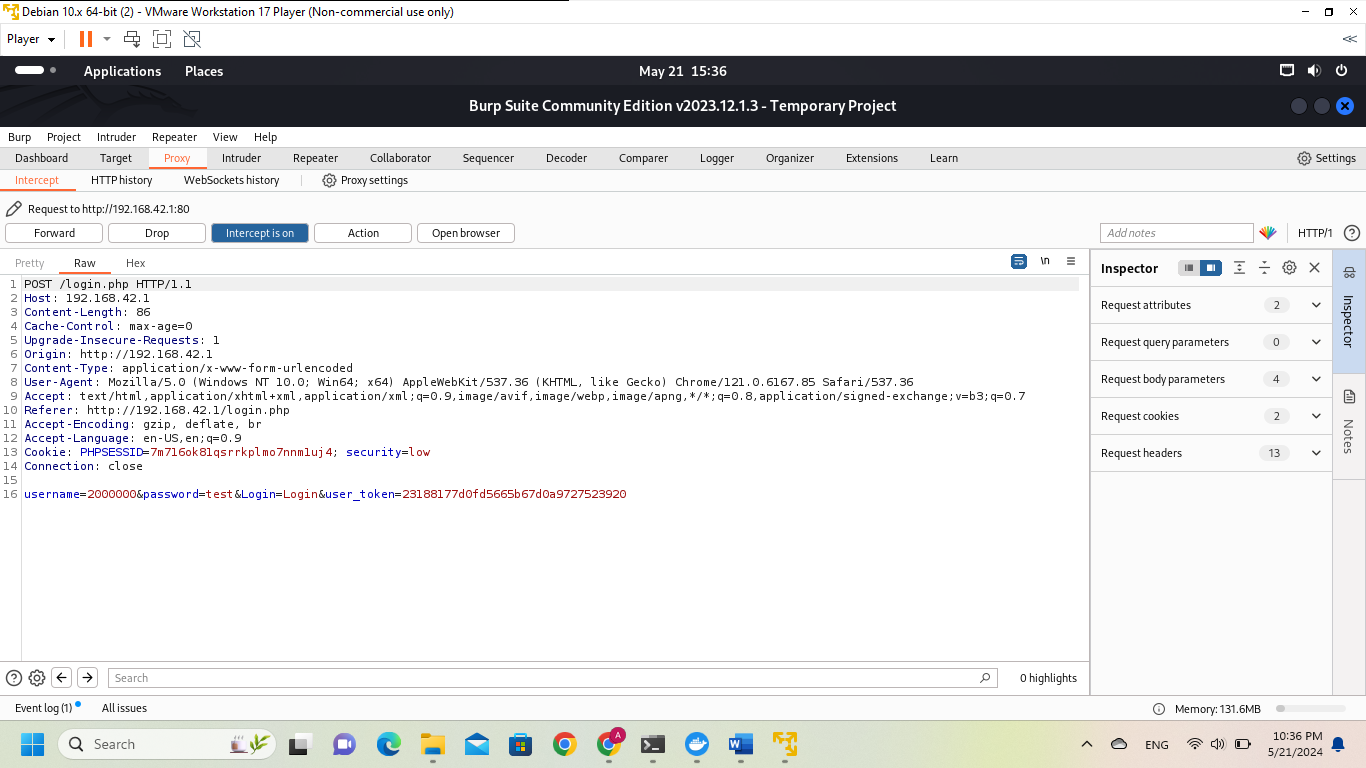


1. I will access the vulnerable web server using my own ip address .



1. I will turn the intercept on so I can intercept the request that I will send to the server and modify it .





1. **Analyze and Test for SQLi**

We will try to send some packets after modifying the request using the repeater   
I will try to modify the payload of the username to make the query match the true statement .

1. **Basic SQLi Payloads:**

* ' OR '1'='1
* "' OR '1'='1
* ') OR ('1'='1

1. **Advanced SQLi Payloads:**

* ' OR 1=1--
* " OR 1=1--
* ') OR 1=1--
* ' OR '1'='1' --
* ") OR ("1"="1"--
* ' OR 1=1 #

1. **With Comment to Bypass Additional Conditions:**

* ' OR '1'='1' /\*
* ' OR 1=1 /\*
* " OR 1=1 /\*
* ' OR 'x'='x' /\*
* ') OR ('x'='x' /\*

Scenario #2 (Brute force attack)

1. **Intercept Login Request:**
   * Navigate to the DVWA login page (http://localhost/dvwa/login.php).
   * Enter any credentials and submit the form.
   * Burp Suite will intercept the request.

**Step 4: Analyzing the Request**

1. **View the Intercepted Request:**
   * In Burp Suite, go to the Proxy tab and select the HTTP history sub-tab.
   * Find the POST request to login.php.
2. **Send the Request to Intruder:**
   * Right-click the intercepted request and select Send to Intruder.

**Step 5: Configuring Intruder for Brute Force Attack**

1. **Set Attack Positions:**
   * Go to the Intruder tab and select the Positions sub-tab.
   * Clear any existing payload markers.
   * Highlight the username value and click Add to mark it as a position.
   * Highlight the password value and click Add to mark it as a position.
   * Your payload positions should look like this:

Make file

POST /dvwa/login.php HTTP/1.1

Host: localhost

User-Agent: ...

Content-Type: application/x-www-form-urlencoded

username=^USER^&password=^PASS^&Login=Login

1. **Configure Payloads:**
   * Go to the Payloads sub-tab.
   * Select Simple list as the payload type.
   * Enter a list of possible usernames and passwords (e.g., admin, password, admin123, etc.).
   * Example for usernames:

sql

Copy code

admin

user

guest

* + Example for passwords:

Copy code

password

admin123

12345

**Step 6: Executing the Attack**

1. **Start the Attack:**
   * Click the Start attack button in the Intruder tab.
   * Burp Suite will start sending requests with different combinations of usernames and passwords.
2. **Analyze the Results:**
   * Once the attack is complete, look for responses with different status codes or content lengths. A successful login will usually have a different response.

**Step 7: Reviewing the Results**

1. **Identify Successful Login:**
   * In the Intruder results window, look for the request that has a different response length or status code.
   * This indicates a successful login.
2. **Verify the Credentials:**
   * Use the identified username and password to log in to DVWA manually and confirm access.