**Case Study 6**

**Aim -** Use Burp Proxy to test web applications.

**Theory -**

**What is HTTP Protocol?**

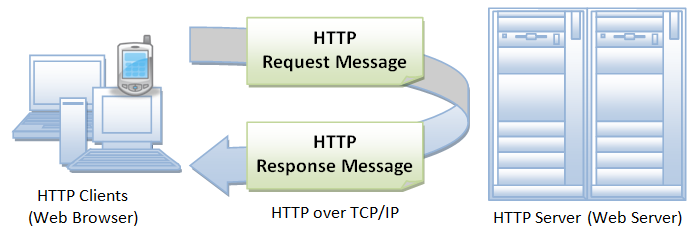
HTTP, or HyperText Transfer Protocol, is a set of rules that allows your web browser to request and display web pages. It's like a language that computers use to talk to each other on the internet. HTTP helps transfer text, pictures, and videos from websites to your device, making it possible for you to browse the web. It's essential for how the internet works.

**Features of HTTP:**

* Connectionless protocol: HTTP is like a conversation where you ask a question, wait for an answer, and then hang up - there's no continuous connection between your computer and the website.
* Media independent: It doesn't care what kind of information you're sending, as long as both sides understand how to read it, but they need to agree on what kind of information it is.
* Stateless: Each time you visit a web page, your computer and the website start with a clean slate and don't remember anything from previous visits.

**HTTP Messages**

HTTP messages are of two types: request and response. Both the message types follow the same message format.\



* Request Message: The request message is sent by the client that consists of a request line, headers, and sometimes a body.
* Response Message: The response message is sent by the server to the client that consists of a status line, headers, and sometimes a body.

**What are the Owasp Web Security Testing Guidelines?**

The OWASP Web Security Testing Guide (WSTG) is a free resource that helps people test the security of websites and web applications. It provides techniques, tools, and tips for finding and fixing common security problems in web apps. It's regularly updated to stay current with new threats. The latest version is 4.2, but there's also a version 5.0 in development to keep up with new attack methods.

**Topics of WSTG**

* Information Gathering: Gathering information about the web server and application.
* Configuration and Deployment Management Testing: Testing network and application configurations, including subdomain takeover and cloud storage.
* Identity Management Testing: Testing user roles, registration, and account enumeration.
* Authentication Testing: Checking for weak passwords, default credentials, and lockout mechanisms.
* Authorization Testing: Examining directory traversal, privilege escalation, and insecure references.
* Session Management Testing: Ensuring session security against hijacking and forgery.
* Input Validation Testing: Detecting and preventing issues like cross-site scripting and injection attacks.
* Weak Cryptography Testing: Identifying weaknesses in encryption and security protocols.
* Business Logic Testing: Looking for flaws in how the application handles business processes.
* Client-Side Testing: Assessing client-side vulnerabilities like DOM XSS, CSS injection, CORS, and clickjacking

**Integrating WSTG to Your SDLC**

To successfully integrate the Web Security Testing Guide (WSTG) into your software development process:

1. Training: Make sure your developer and testing teams receive periodic training on WSTG and the testing tools. This helps them understand and address security issues.
2. Prioritize Tests: Start with tests that relate to your application's architecture and the data your organization protects. Focus on tests from the OWASP Top Ten list, which covers critical vulnerabilities. As your team gains expertise, gradually add more tests.
3. Integration with OWASP: Combine WSTG with other OWASP projects that suit different phases of your development process.
4. WSTG Champion: Appoint a team member who is knowledgeable about WSTG to guide and support the implementation.
5. Monitoring and Reporting: Regularly track results and report them to management. Use indicators like the number of vulnerabilities found by severity to gauge your progress in improving web application security.

**What is VAPT Testing? Tools for VAPT testing.**

Vulnerability Assessment and Penetration Testing (VAPT) is a cybersecurity process to find and fix weaknesses in your systems.

Why you need VAPT:

* + Cyber threats change, so testing regularly is crucial.
  + VAPT helps you meet security standards like GDPR and ISO 27001.

Key VAPT Tools:

* + Astra: Scans your entire system to find and fix security issues.
  + OWASP Zap: Checks websites for hidden problems and shows results clearly.
  + Nmap: Identifies devices, software, and security measures on your network.
  + Metasploit: Offers info on vulnerabilities for testing and configuring networks.
  + Burp Suite: Tests web apps for security flaws.
  + Wireshark: Monitors network traffic for troubleshooting and analysis.
  + Nikto: Scans web servers for potential issues and outdated software.

**What is Burp Suite?**

Burp Suite is a cybersecurity tool used to test the security of websites and web applications. It's like a Swiss Army knife for finding and fixing vulnerabilities.

Key features:

* Easy to Use: It's user-friendly and helps testers find and fix security problems in websites.
* Spider: It's like a web crawler that maps out a website's structure to find potential security issues.
* Proxy: It allows you to see and change web traffic between your computer and a website, making it easier to spot and fix problems.
* Intruder: This tool tries different inputs to see if a website has weak points that hackers could exploit.
* Repeater: It lets testers send requests to a website many times to check if user-supplied data is properly protected.
* Sequencer: It checks if a website generates secure tokens for things like logins or payments.
* Decoder: Helps in understanding how information is hidden or encoded in a website.
* Extender: Lets you add extra tools to Burp Suite to make it even more powerful.
* Scanner: This feature automatically looks for common security issues in websites, but it's not available in the free version.

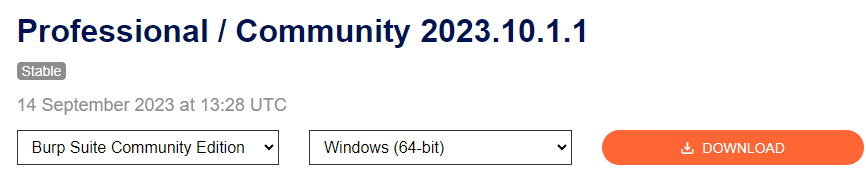
Overall, Burp Suite is like a toolbox for finding and fixing problems in websites to make them more secure. It's used by cybersecurity professionals to make sure websites can't be easily hacked.

**Get Started with Burp Suite**

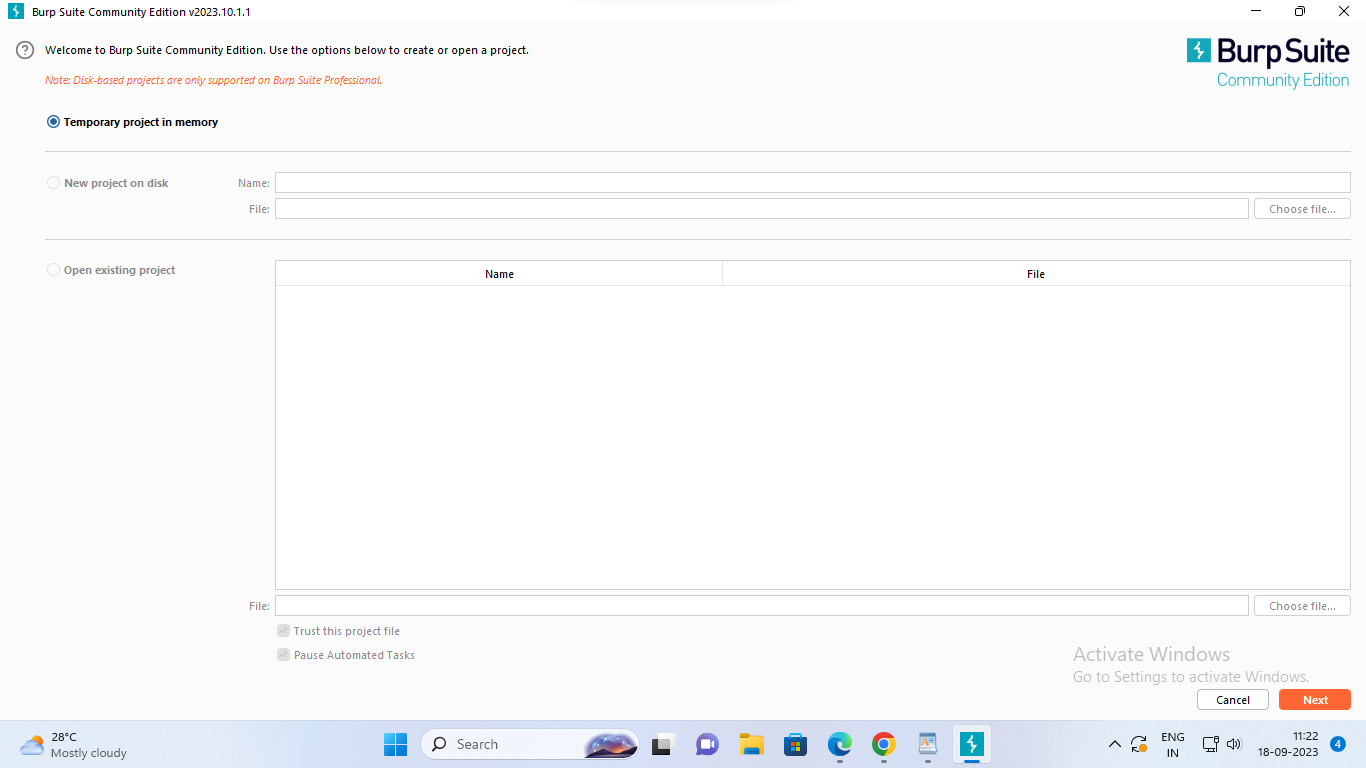
Getting started with Burp Suite professional and community edition is achieved in the following five steps:

**1. Download and Install**

**Step 1:** You can download the latest version of Burp Suite professional and community edition using the links provided on the PortSwigger website.

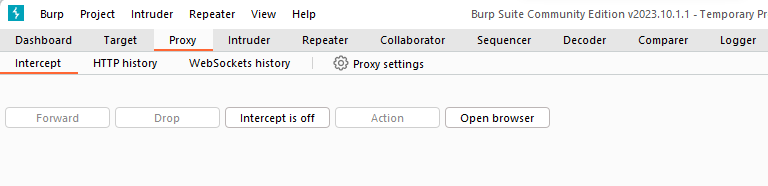


**Step 2:** Now, run the installer and open the Burp Suite software.

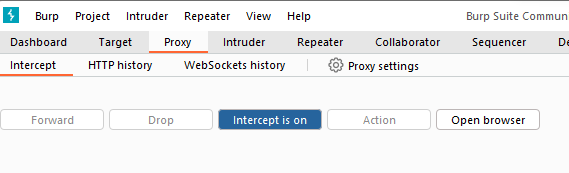


**2. Intercepting HTTP traffic with Burp Proxy.**

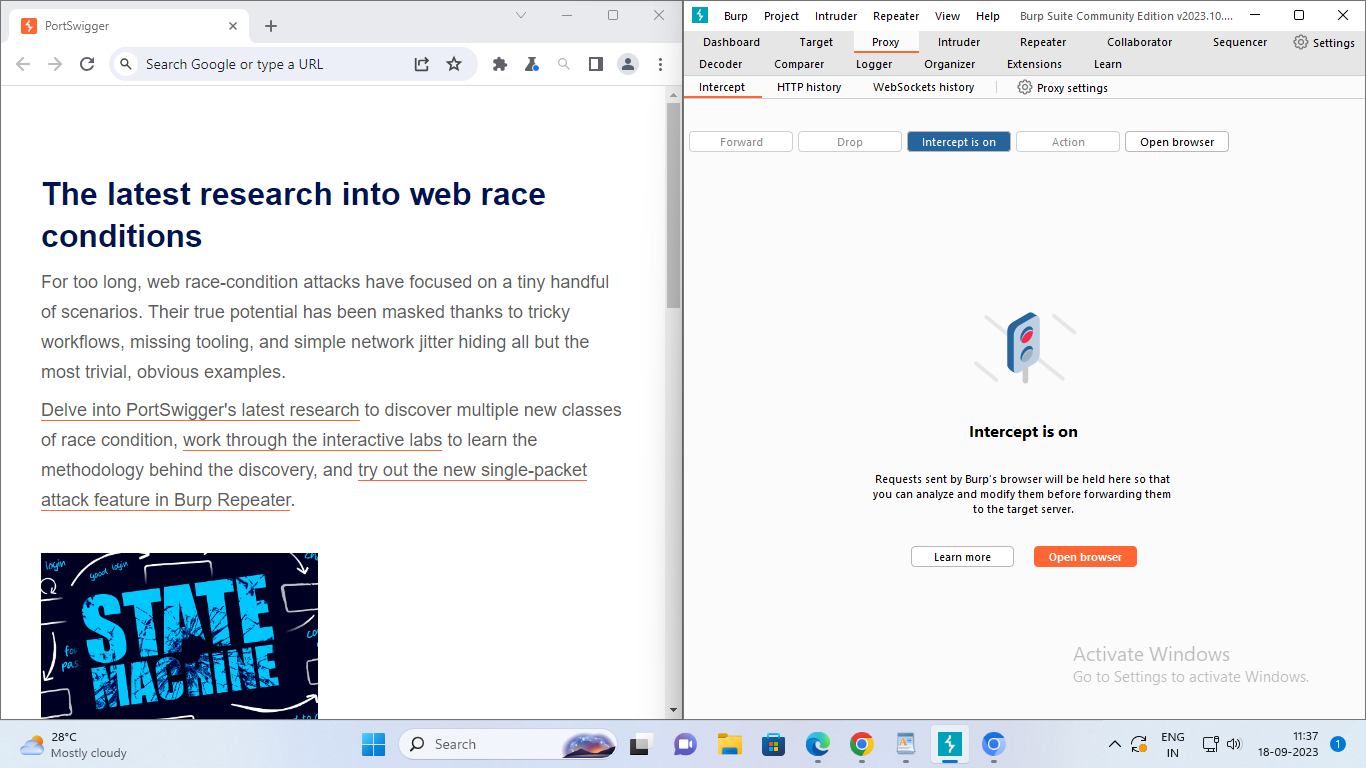
* Go to the Proxy -> Intercept tab.



* Click the Intercept is off button, so it toggles to Intercept is on.



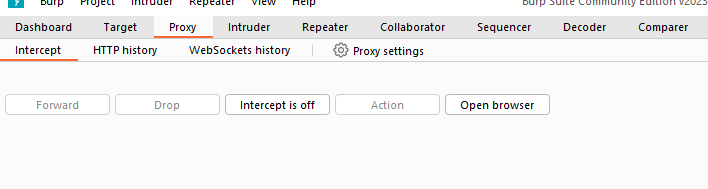
* Click Open Browser. This launches Burp's browser, which is preconfigured to work with Burp right out of the box. Position the windows so that you can see both Burp and Burp's browser.



* Using Burp's browser, try to visit <https://portswigger.net> and observe that the site doesn't load. Burp Proxy has intercepted the HTTP request that was issued by the browser before it could reach the server. You can see this intercepted request on the Proxy -> Intercept tab.

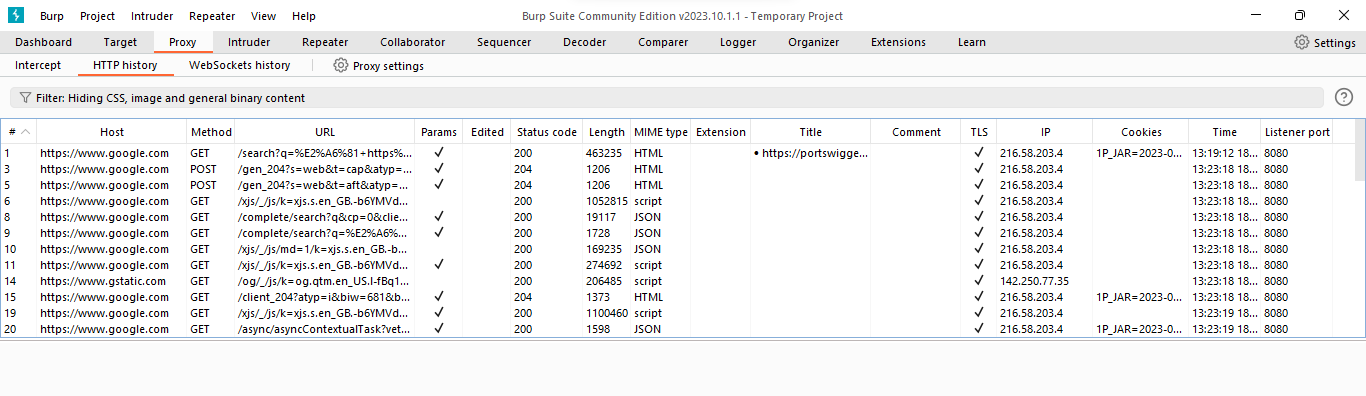


* The request is held here so that you can study it, and even modify it, before forwarding it to the target server.
* Click the Forward button several times to send the intercepted request, and any subsequent ones, until the page loads in Burp's browser.
* Due to the number of requests browsers typically send, you often won't want to intercept every single one of them. Click the Intercept is on button so that it now says Intercept is off.



Go back to the browser and confirm that you can now interact with the site as normal.

* In Burp, go to the Proxy > HTTP history tab. Here, you can see the history of all HTTP traffic that has passed through Burp Proxy, even while interception was switched off.
* Click on any entry in the history to view the raw HTTP request, along with the corresponding response from the server.







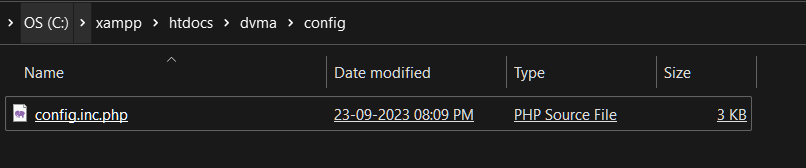
This lets you explore the website as normal and study the interactions between Burp's browser and the server afterward, which is more convenient in many cases.

**Step 3:** Now Download DVWA (Damn Vulnerable Web Application) from Github for Pen Testing purpose. [digininja/DVWA - Damn Vulnerable Web Application](https://github.com/digininja/DVWA)

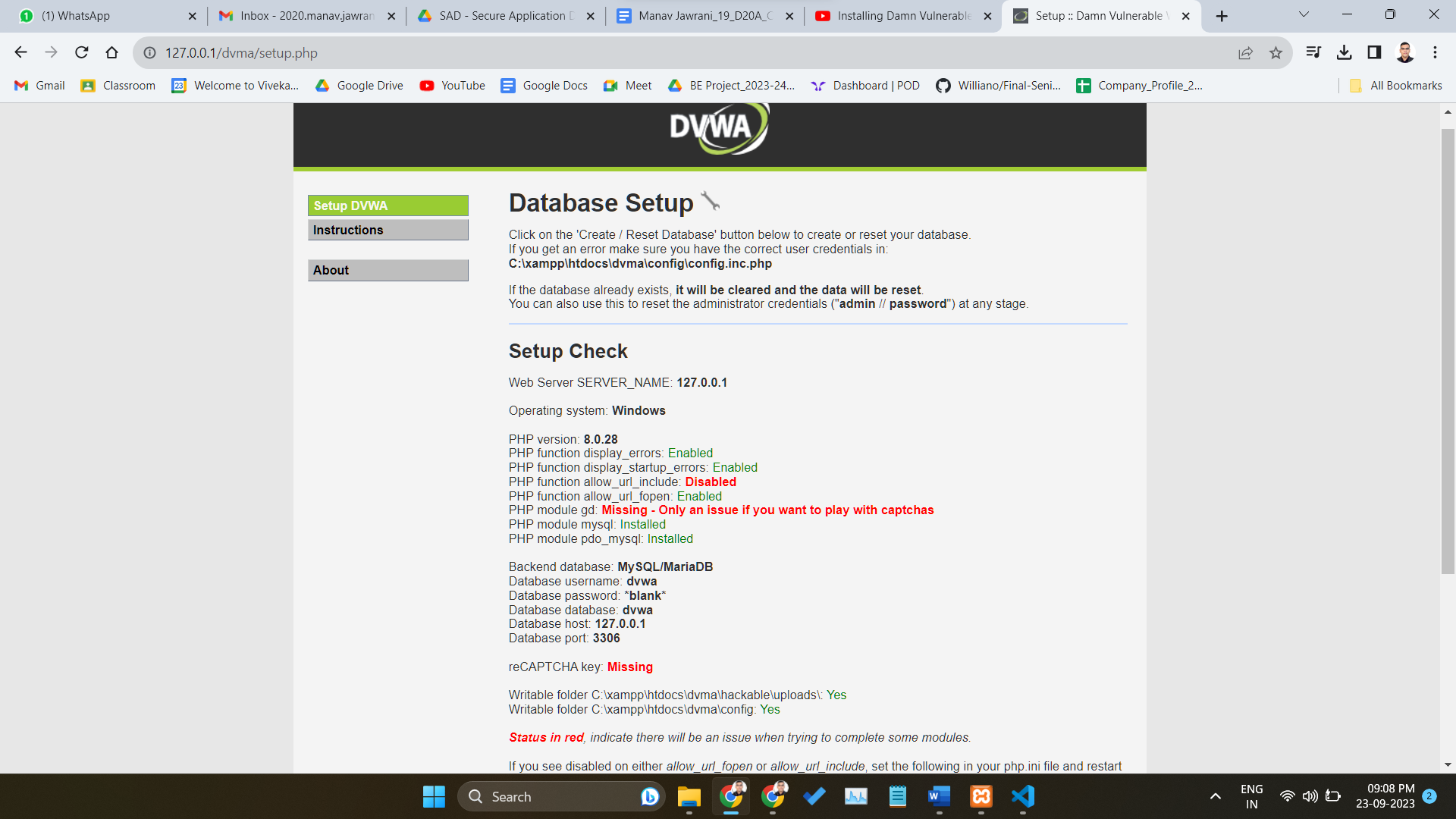
**Step 4:** Download Xampp and install. Reference for installation of Burp Suite, Xampp and DVWA. [Installing Damn Vulnerable Web Application (DVWA) on Windows 10](https://www.youtube.com/watch?v=cak2lQvBRAo)

**Step 5:** Move the DVWA folder to htdocs folder under Xampp:

* Goto config -> Change the **config.inc.php.dist** file name to **config.inc.php**



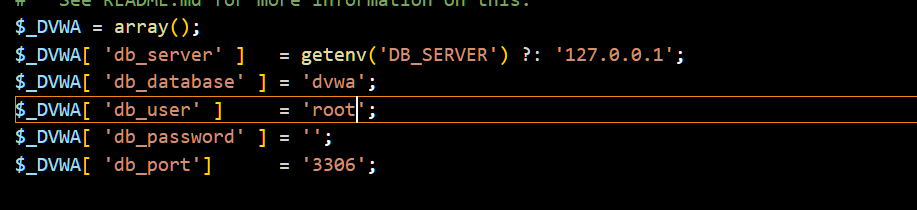
* Browse to <http://127.0.0.1/DVWA-master>

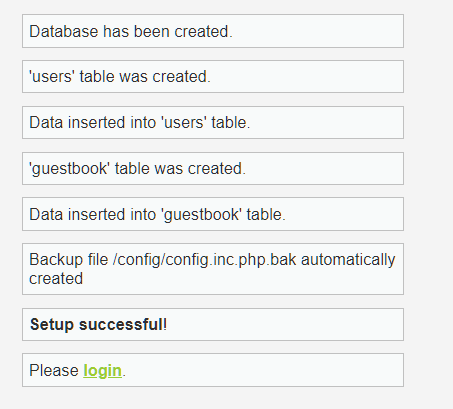


* If it gives Sql Error , Open Config.inc.php file and change the

$\_DVWA[ 'db\_user' ] = 'root';

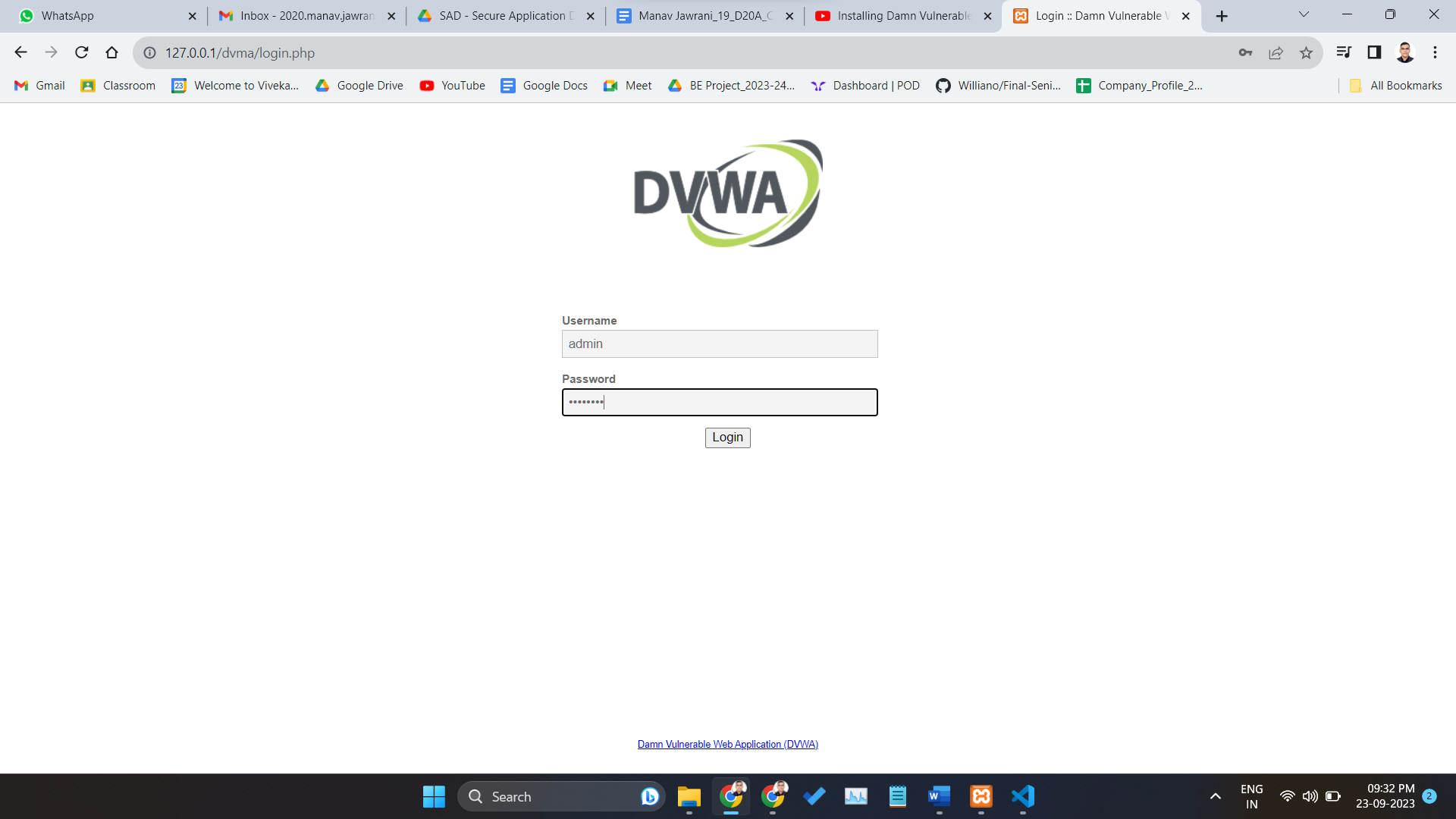
$\_DVWA[ 'db\_password' ] = ' ';

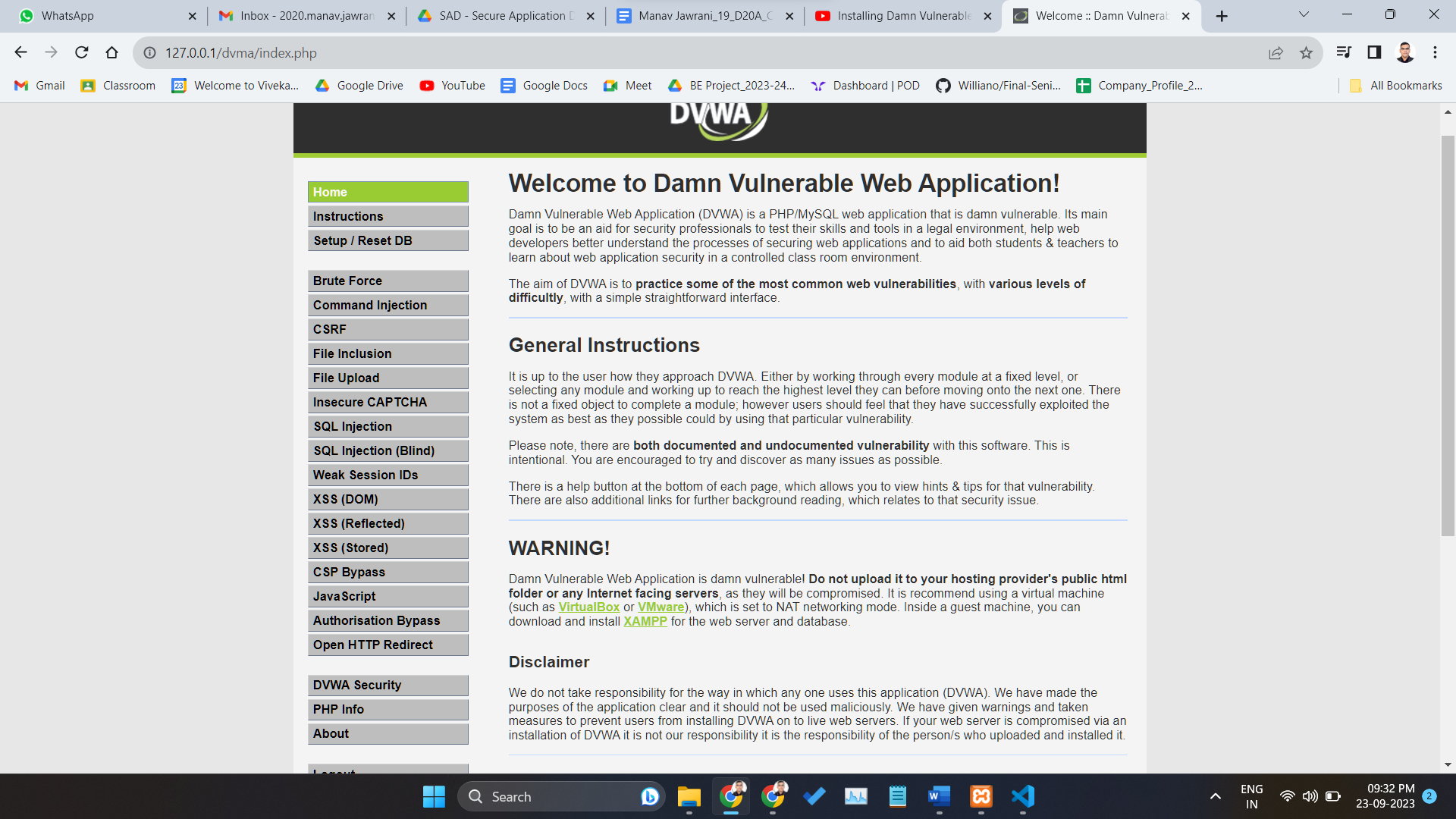




2. Default Credentials

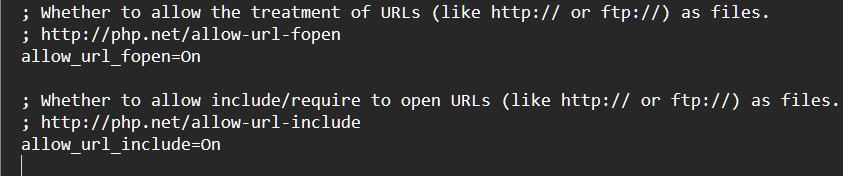
* Default username = admin
* Default password = password





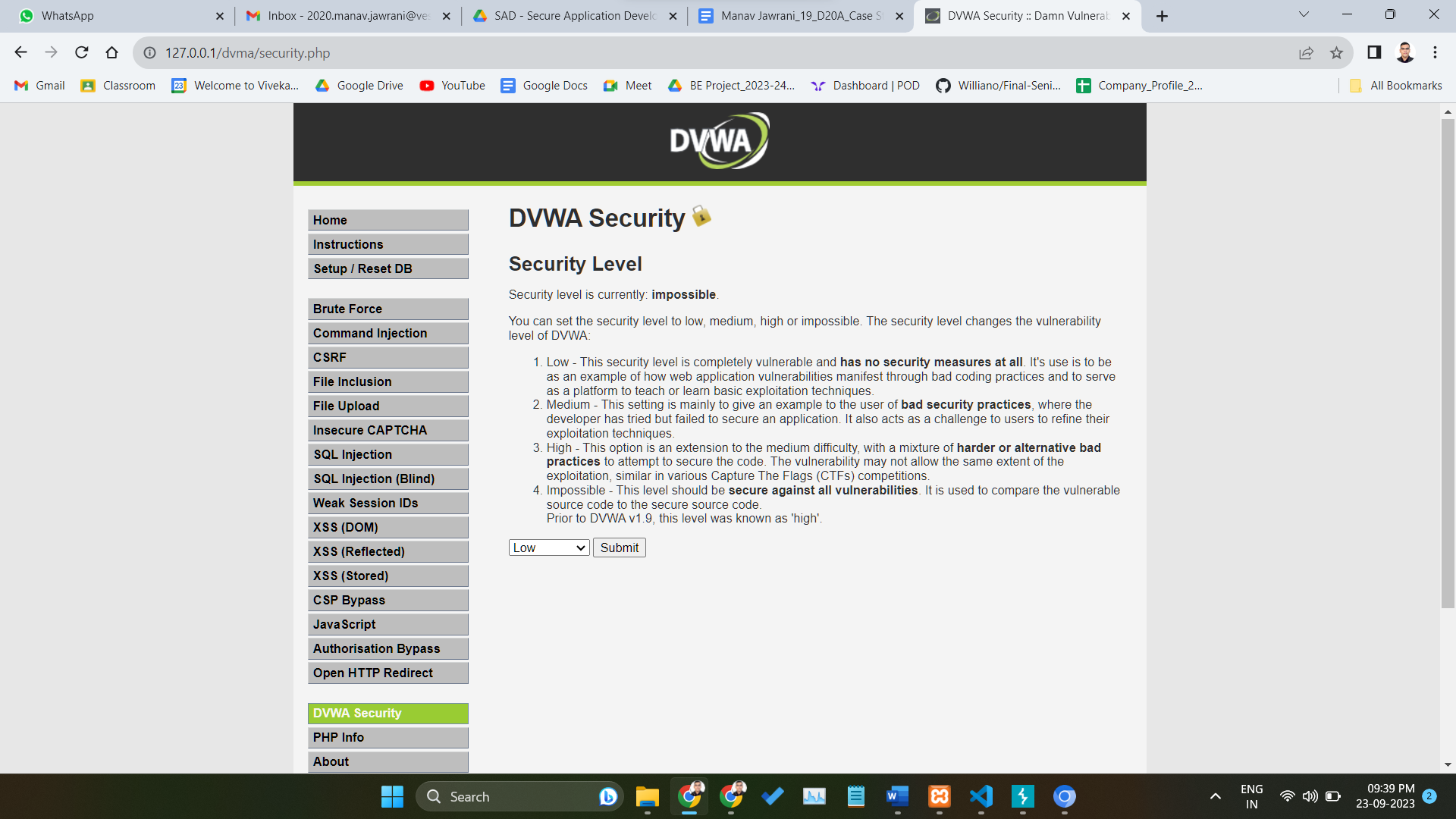
**allow\_url\_fopen = on**

This allows for Remote File Inclusions (RFI) [allow\_url\_fopen]. Make this change to a php.ini file in Xampp. Now try to login to the web application



**3. Modify HTTP requests with Burp Proxy**

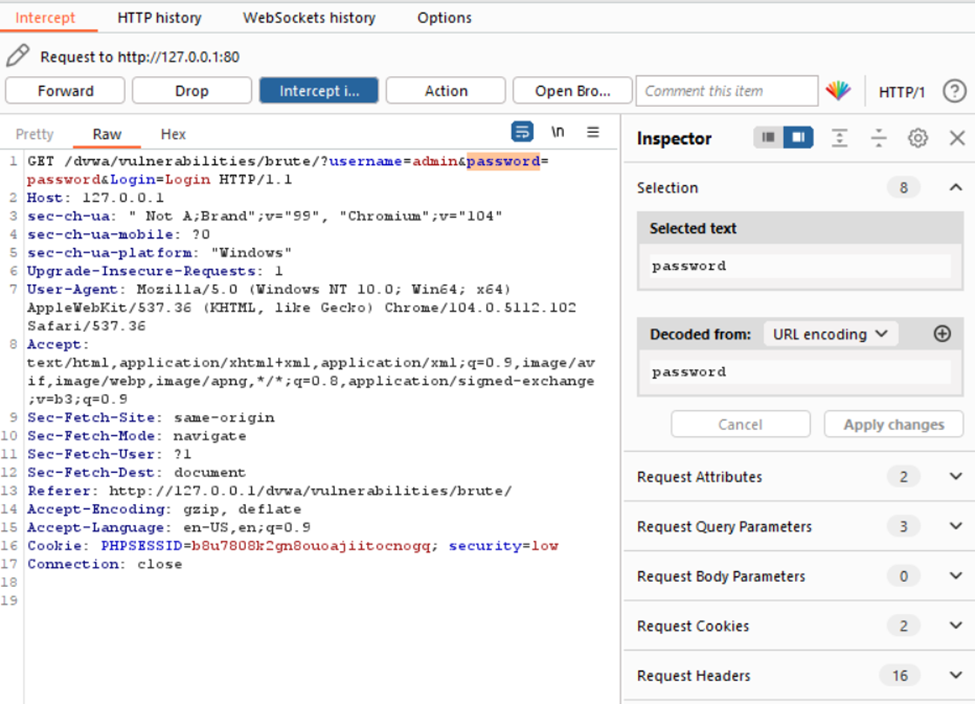
Change the security settings to low to turn off security features. Move to the Brute force tab and try to login using the default credentials. Intercept should be on.



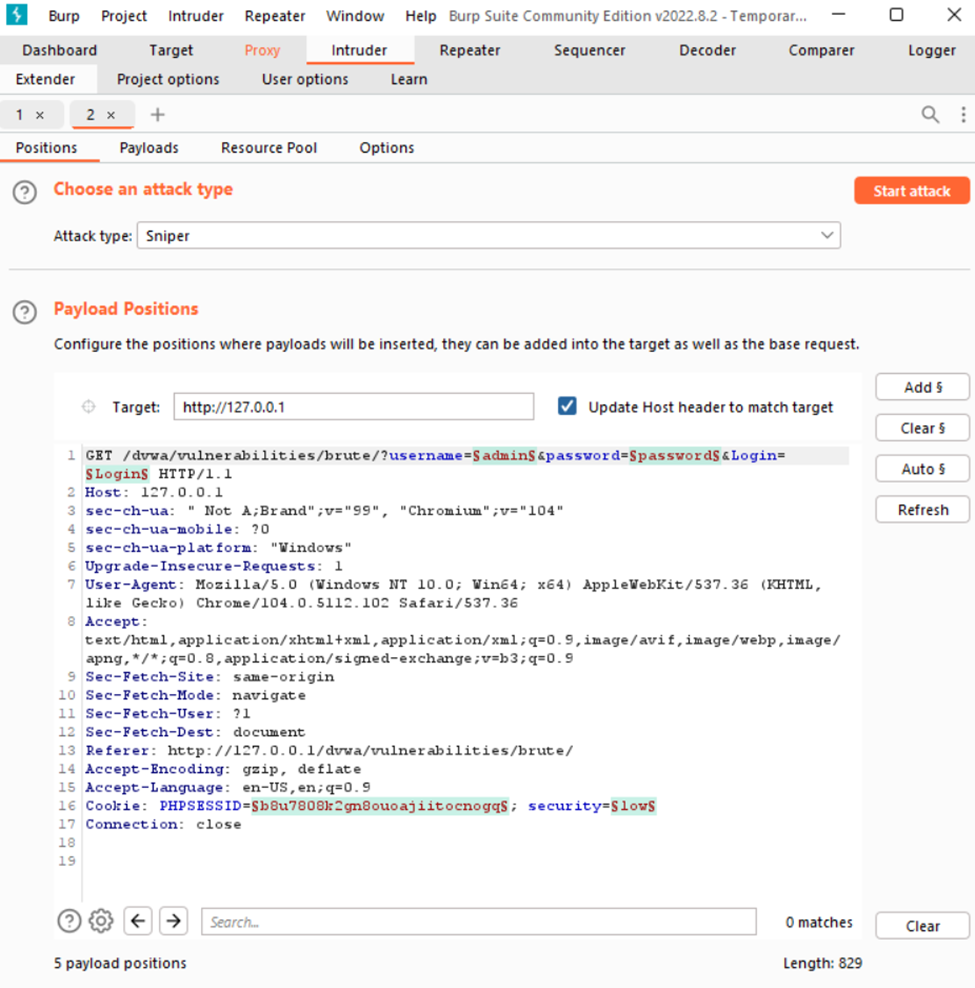
Now open the **Burp Suite Brower** you can see the request in your intercept work area.



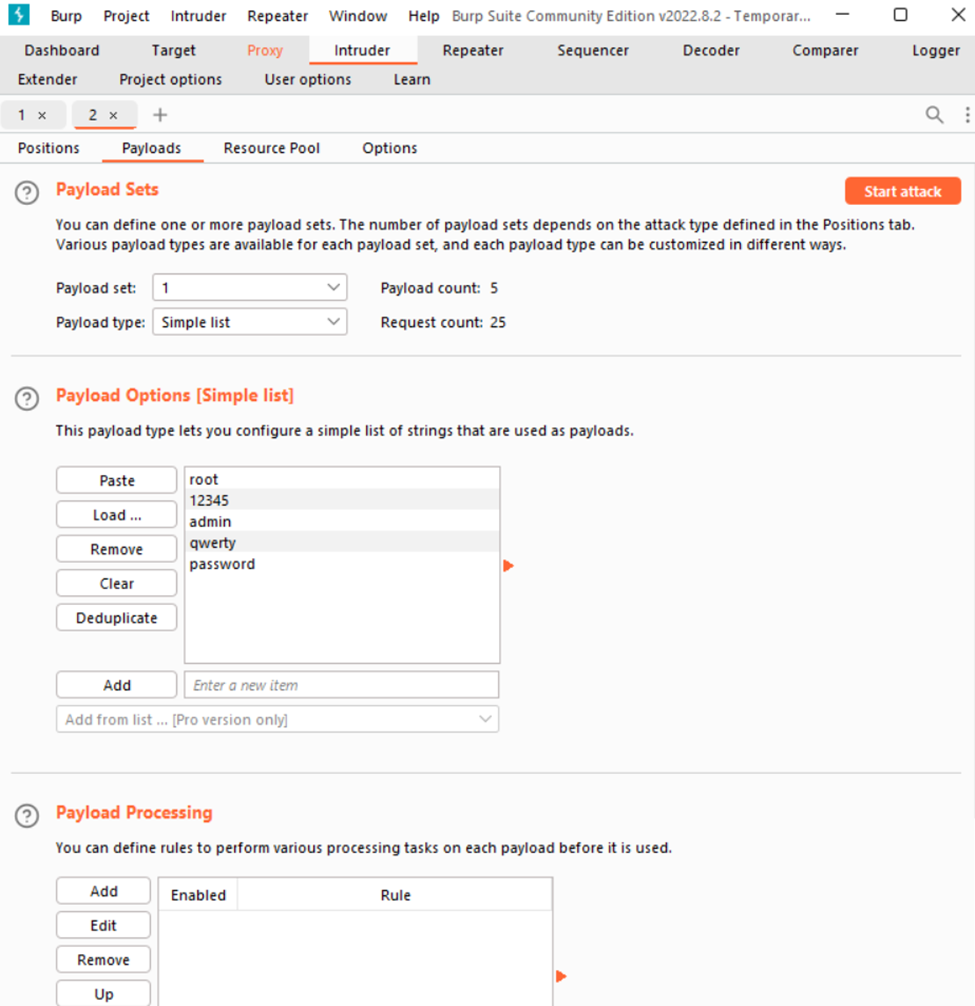
Click on the Action Tab and Send this request to the Intruder.



Modifying the Request. Now, you can make changes to the page.



Intruder will now be able to change the required field in the request and start an attack to find the correct password.



**Conclusion -**

Thus we have studied OWASP Web Security Testing Guidelines, VAPT Testing and the tools used in VAPT. We also have used Burp proxy to test web applications.