Burp Suite and PortSwigger WS Academy

**Description**

Burp Suite is an integrated platform used for performing security testing of web applications. It acts as a proxy server that intercepts HTTP/HTTPS traffic between the user's browser and the web application, allowing for detailed analysis and manipulation of the requests and responses.

**Usages**

* Web Application Security Testing: Identify vulnerabilities like SQL injection, cross-site scripting (XSS), and others.
* Penetration Testing: Simulate attacks to assess the security posture of a web application.
* Security Auditing: Conduct thorough assessments of web applications to find weaknesses.
* Learning and Training: Educate security professionals about web application vulnerabilities and testing methodologies.

**Features**

* Intercepting Proxy: Capture and modify web traffic in real-time.
* Scanner: Automated tool to identify security vulnerabilities in web applications.
* Intruder: Tool for automating customized attacks such as brute force or fuzzing.
* Repeater: Allows users to send modified requests and analyze the server's responses.
* Sequencer: Analyzes the randomness of session tokens or other important data.
* Extensibility: Supports plugins and extensions to enhance functionality.
* Collaborative Features: Allows multiple users to work on the same project.

**How Ethical Hackers Can Use This Tool**

In ethical hacking, Burp Suite is used to:

* Intercept and Analyze Requests: Capture requests from a web application to identify potential vulnerabilities in how data is processed.
* Test for Common Vulnerabilities: Use the Scanner to automate checks for vulnerabilities such as XSS, CSRF, and SQL injection.
* Perform Manual Testing: Use tools like Repeater and Intruder to manually exploit vulnerabilities and understand how they can be attacked.
* Generate Reports: Document findings for stakeholders, helping them understand risks and suggested remediation.

**Phases**

Gaining Access

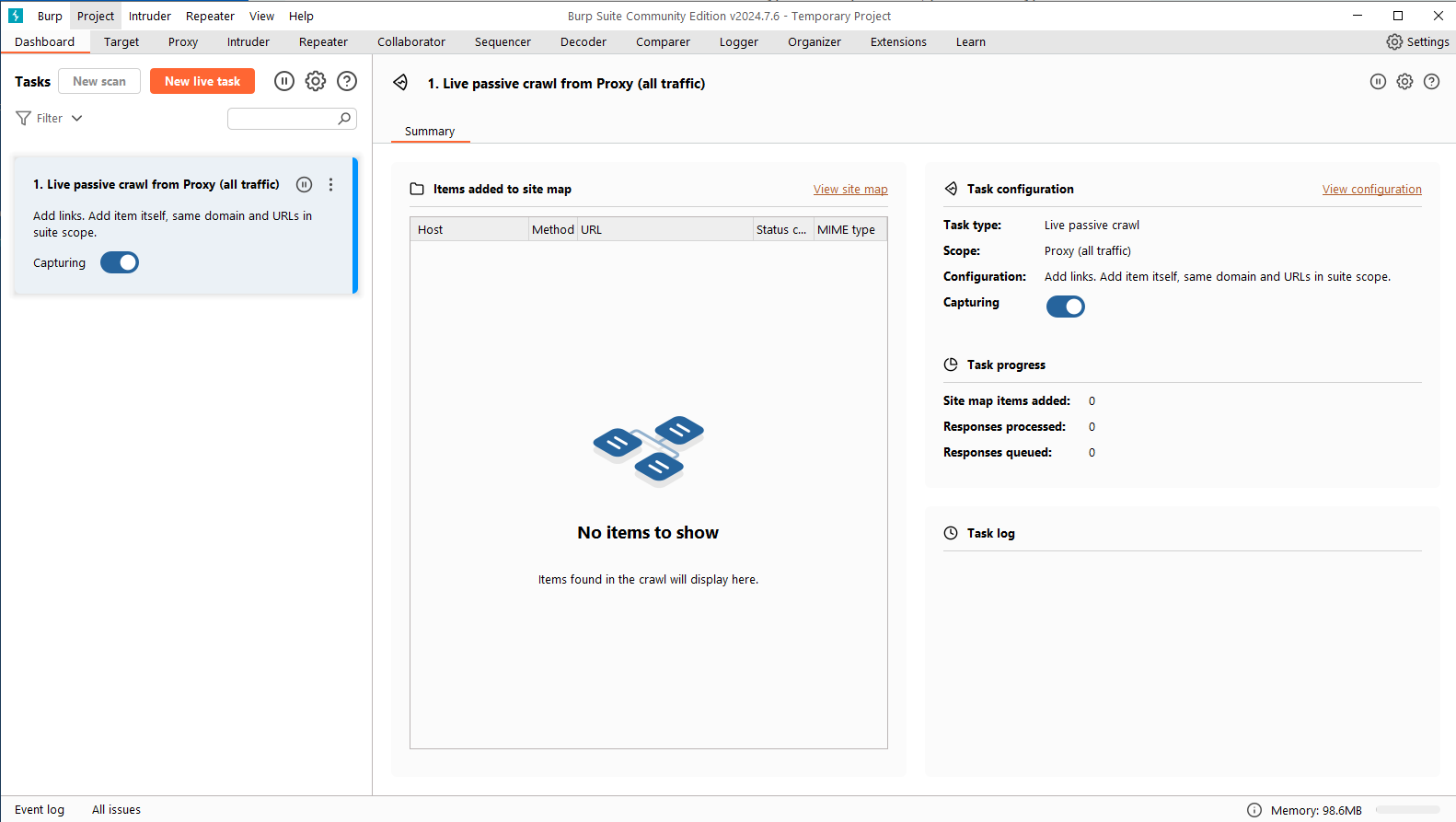
**PortSwigger Web Security Academy**

The Web Security Academy contains high-quality learning materials, interactive vulnerability labs, and video tutorials. This website serves as the base for using Burp Intruder tool.

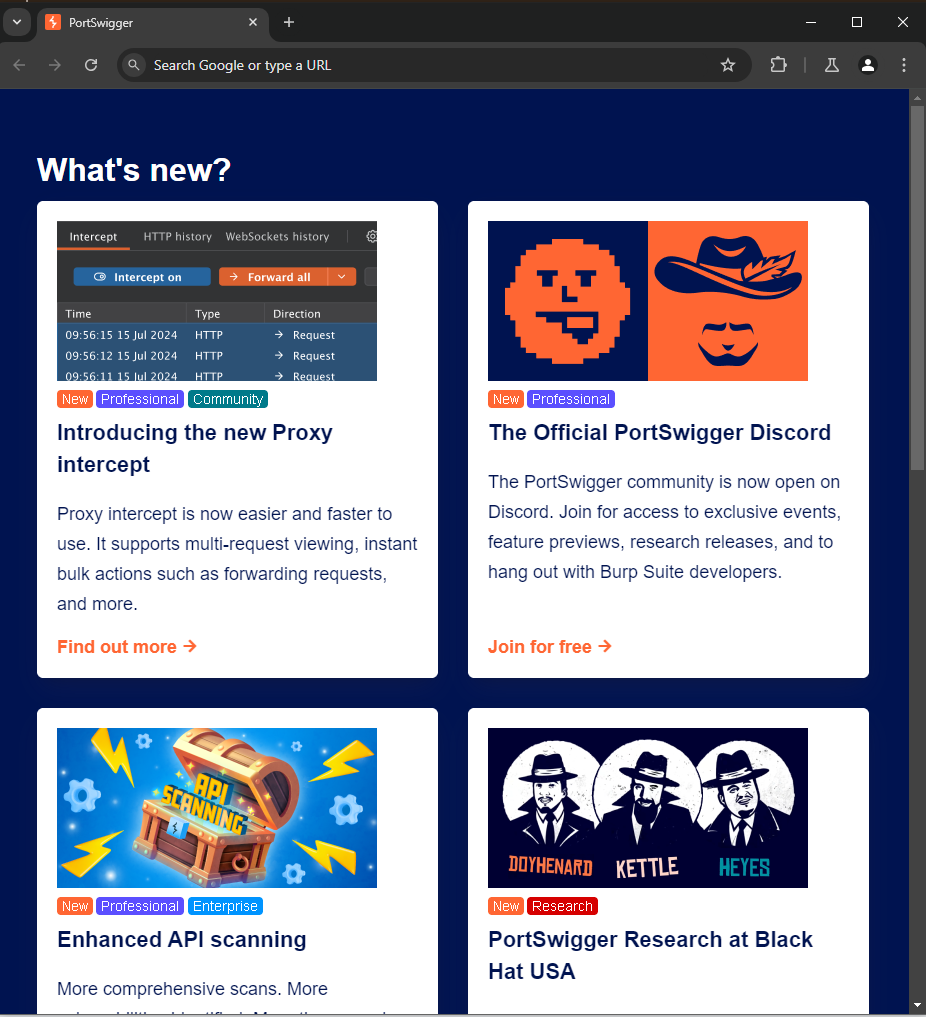
Using Burp Intruder for brute forcing login

**\*\*IMPORTANT\*\*: You have to create the project each time, saving is not possible on community edition**

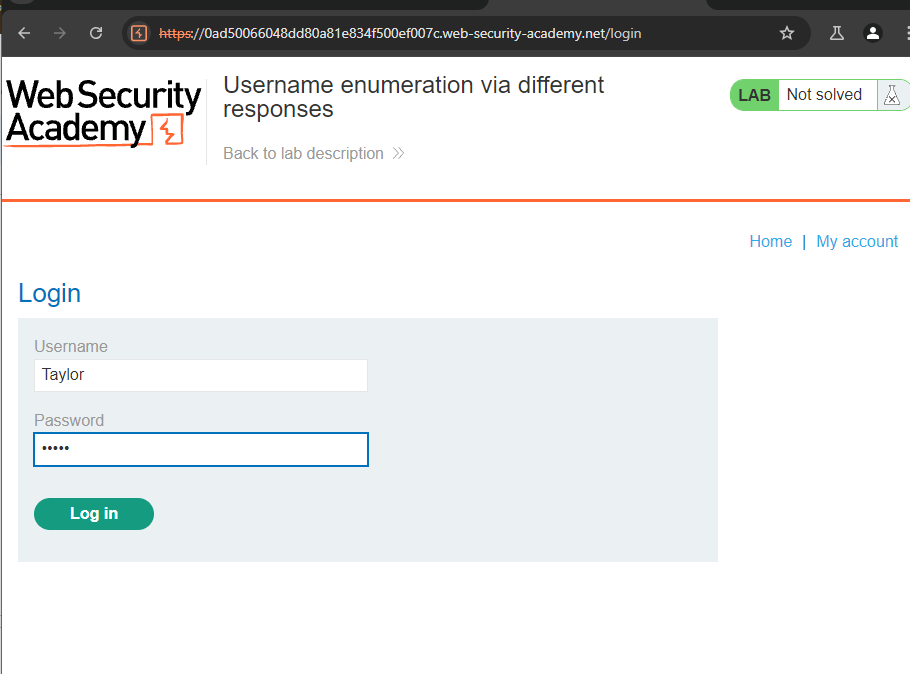
Main Dashboard



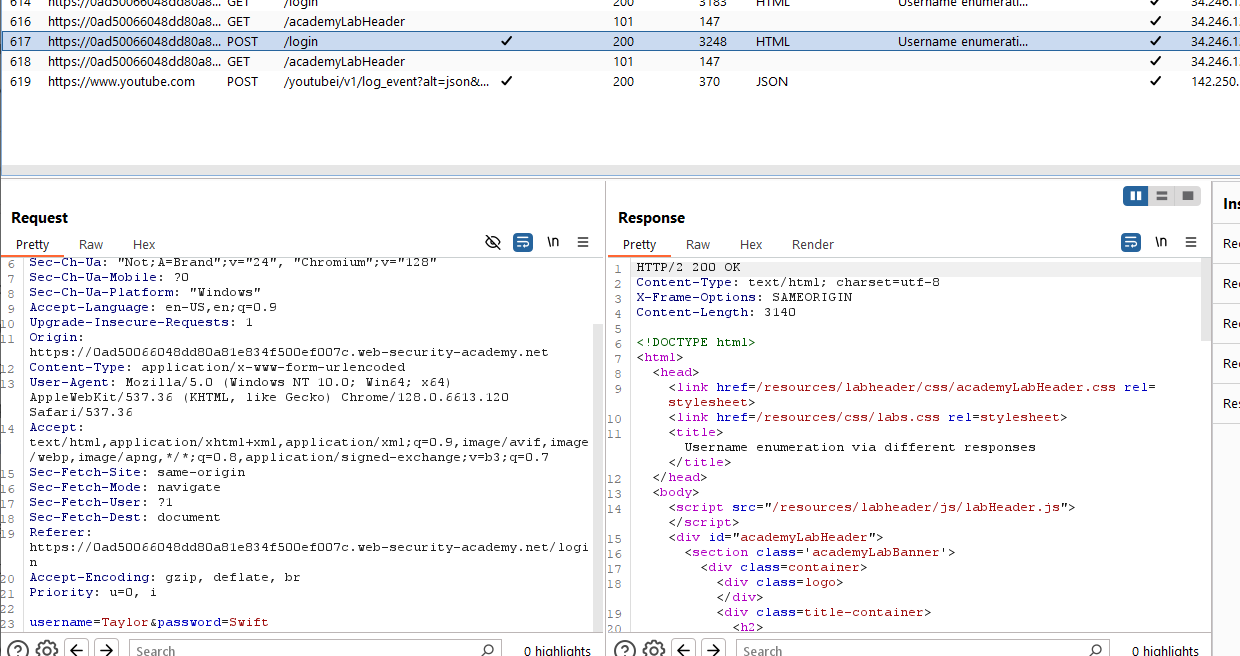
Opening Burp Browser (which is pre-configured for proxy)



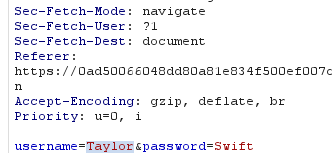
Trying to login with wrong credentials



Intercepting the POST request

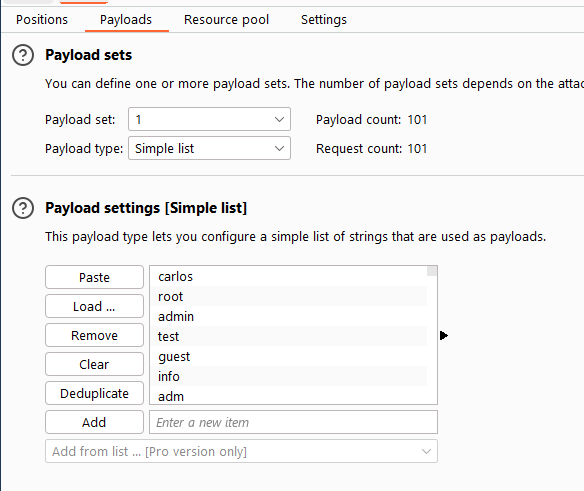


Changing the payload of the request



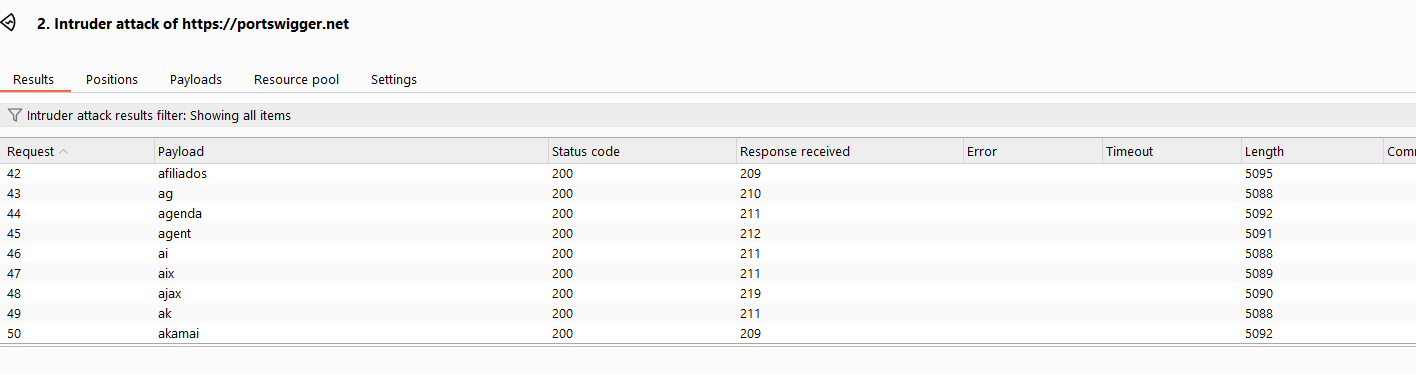
Choosing Sniper as attack type

Payload

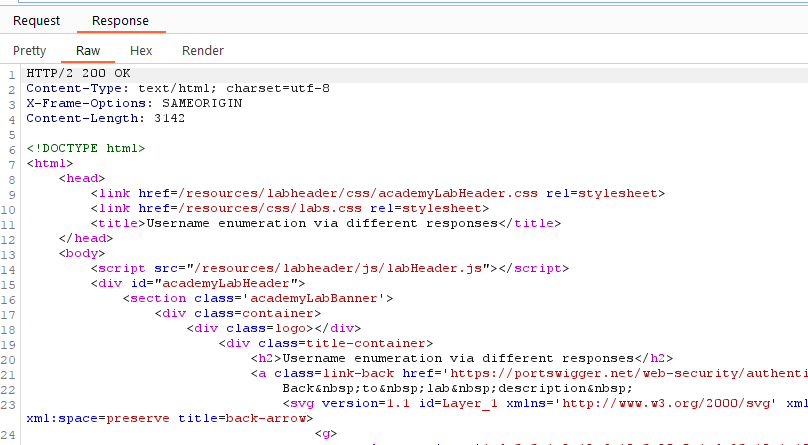


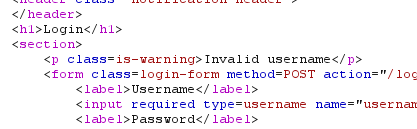
Starting the Attack

We try to find a username such that the website will give an error “wrong password” rather than “login failed” so that we can know that an account with that username name exists and then we can try brute forcing its password.



Most Response will contain “Invalid Username” so no account with that username exists





For Username “afiliados” it displays “Incorrect Password” so account with that username exists

