Security Testing Report.

Table of Contents

Overview –

This report presents the findings from security testing of the login functionality, focusing on Man-in-the-Middle (MITM) and Brute Force attacks. The goal was to identify potential vulnerabilities that could be exploited by attackers and provide recommendations to mitigate these risks.

Scope and Objective -

Scope:

The login functionality of the “http://testphp.vulnweb.com/login.php” was tested.

Objectives:

- Assess the application's susceptibility to MITM attacks.
- Evaluate the robustness of authentication mechanisms against brute force attacks.

Methodology -

Security testing was performed using Burp Suite, following these steps:

1. Setup:

   Configured Burp Suite as a proxy to capture login requests and responses.

2. Analysis:

   Intercepted and analysed HTTP requests and responses.

3. Testing:
   - Man-in-the-Middle (MITM) Attack
   - Brute Force Attack

Findings –

Man-in-the-Middle (MITM) Attack

Test:

- Intercept and manipulate traffic between the client and the server.

Steps:

1. Configured Burp Suite as a proxy and intercepted login requests.
2. Modified intercepted requests to see if sensitive information could be captured or altered.

Impact:

- High: Potential exposure of sensitive information such as usernames, passwords, and session tokens.

Recommendation:

- Ensure all communication is encrypted using HTTPS.
- Implement HSTS (HTTP Strict Transport Security) to prevent HTTPS downgrade attacks.

Brute Force Attack

Test:

- Automate multiple login attempts using common password lists.

Steps:

1. Intercepted a login request.
2. Used Burp Suite Intruder to send multiple login attempts with different passwords.

Observation:

- The application did not implement an account lockout mechanism after multiple failed login attempts.

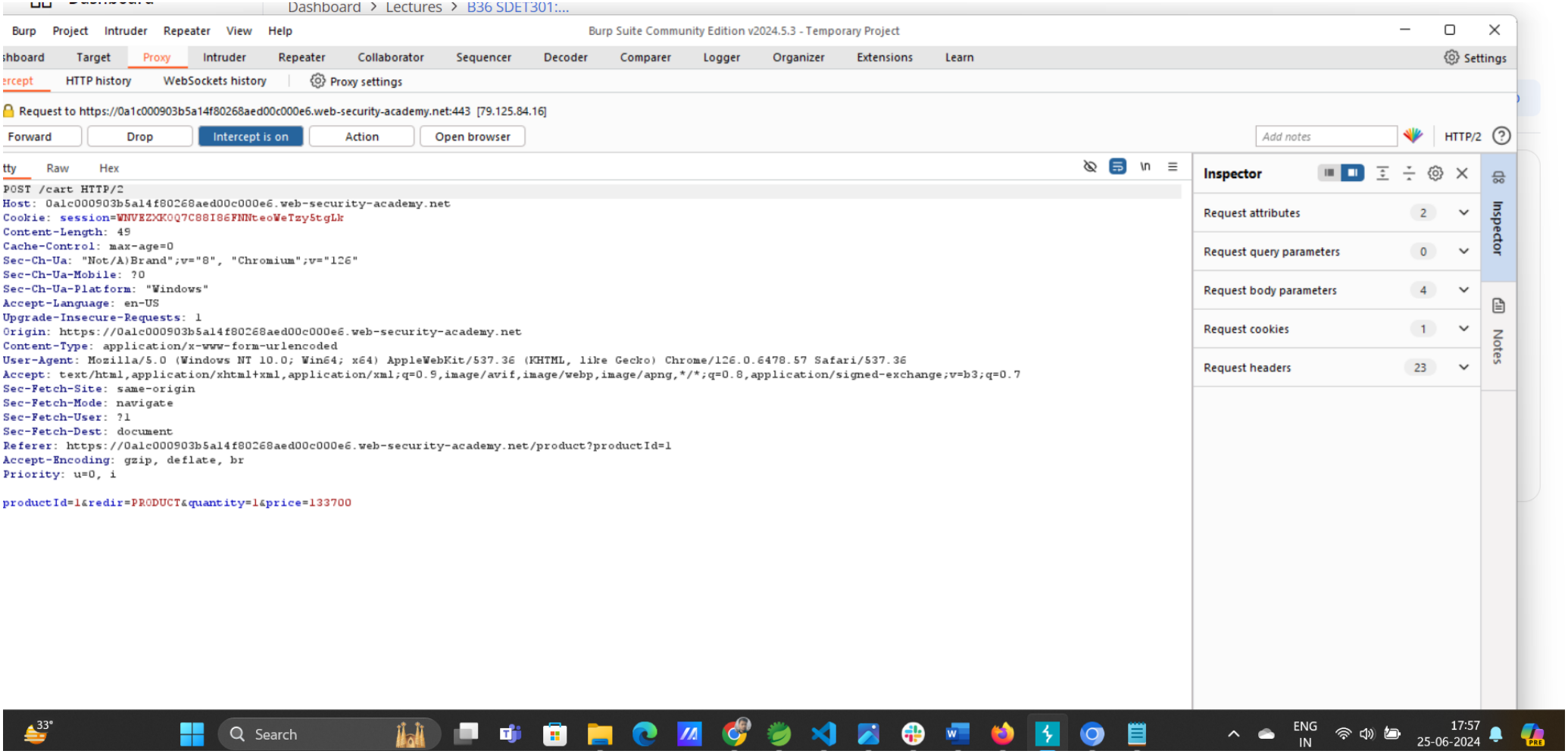
Impact:

- Medium: Increased risk of account compromise through password guessing attacks.

Recommendation:

- Implement account lockout mechanisms after a certain number of failed login attempts.

Some Screenshots of Man-in-the-Middle (MITM) Attack



Description:

Do you often feel as though people aren't aware of just how "l33t" you are? Do you find yourself struggling to make others feel inferior with public displays of your advanced "l33t-ness"? If either of these things are at the top of your priority list, it's time to the welcome Lightweight "l33t" Leather Jacket into your life.

Handcrafted from leather and single strands of recycled bitcoin, so you can enjoy environmental smugness on top of your high-ranking leather-clad "l33t" levels, this jacket is far superior to anything currently available on the high street. Once you've explained to your friends and colleagues what "l33t" means, we guarantee you'll be at least 18% cooler when donning your "l33t" leather. Inspired by the term-coiners, the jacket comes with hand-stitched CISSP insignia so you can channel the original elite every time you rock your Lightweight "l33t" Leather Jacket.

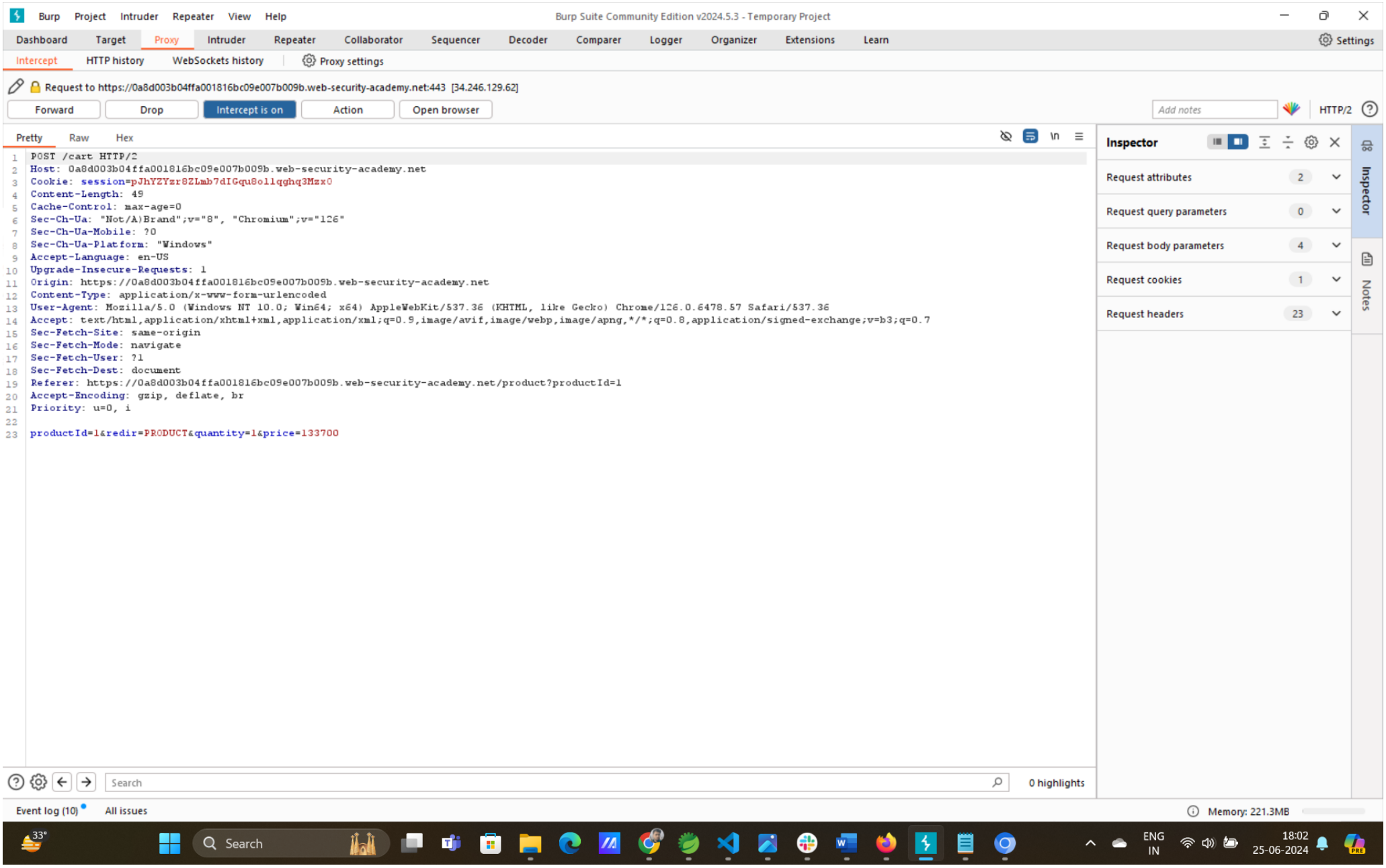
Make your apparel as formidable as your intellect, and dazzle noobs the world over, with the Lightweight "l33t" Leather Jacket.*

*Every purchase comes with a free leaflet, detailing how best to explain the superiority of being "l33t" to noobs.

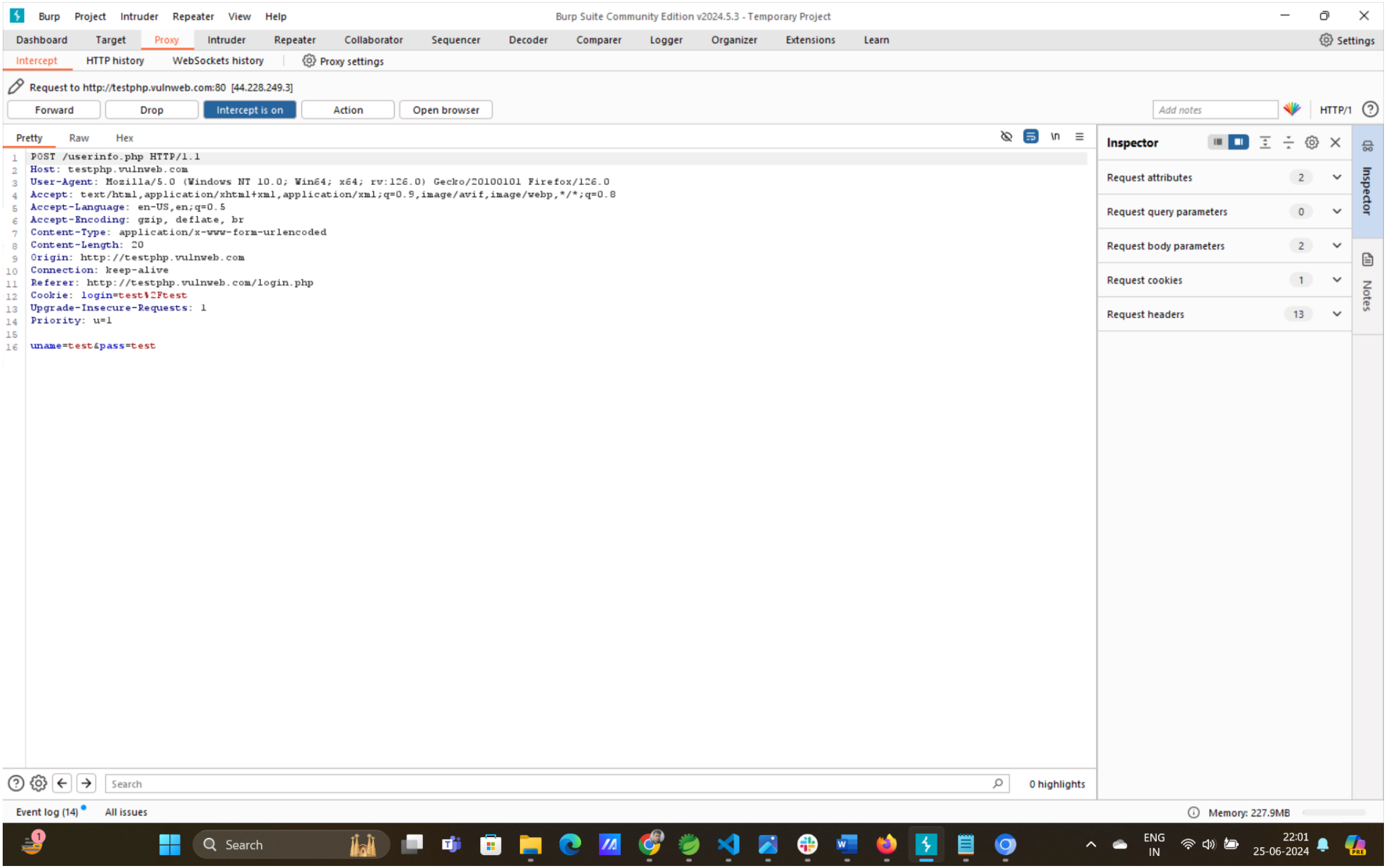
1

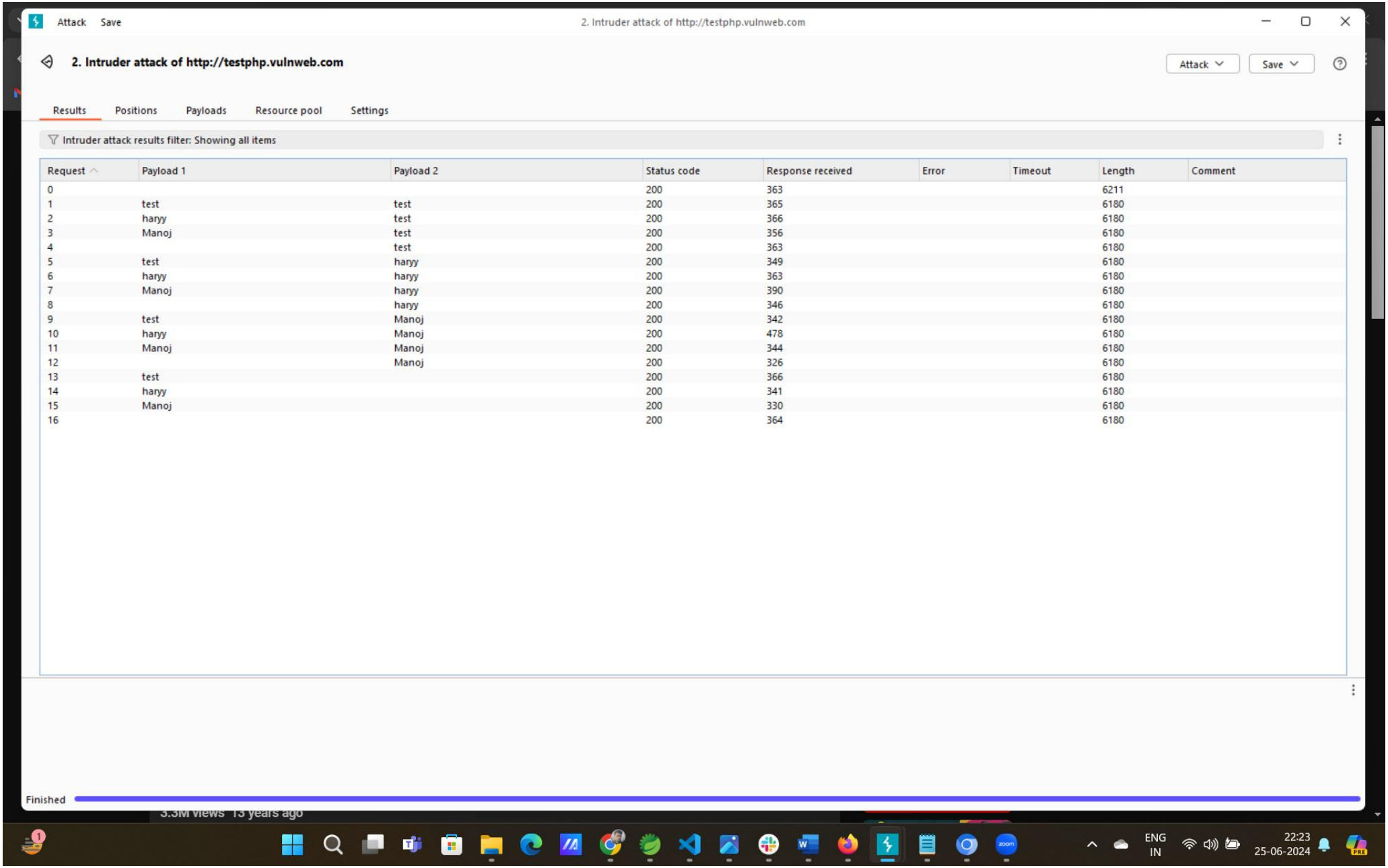
Add to cart

< Return to list


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://0a8d003b04ffa001816bc09e007b009b.web-security-academy.net:443 [34.246.129.62]
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/2
Pretty Raw Hex
1 POST /cart HTTP/2
2 Host: 0a8d003b04ffa001816bc09e007b009b.web-security-academy.net
3 Cookie: session=pJhYZYzr8ZLmb7dIGqu8ollqghq3Mzx0
4 Content-Length: 49
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: en-US
10 Upgrade-Insecure-Requests: 1
11 Origin: https://0a8d003b04ffa001816bc09e007b009b.web-security-academy.net
12 Content-Type: application/x-www-form-urlencoded
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.57 Safari/537.36
14 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0a8d003b04ffa001816bc09e007b009b.web-security-academy.net/product?productId=1
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 productId=1&redir=PRODUCT&quantity=1&price=133700
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 4
Request cookies 1
Request headers 23
Inspector
Notes
Search
0 highlights
Event log (10)
All issues
Memory: 221.3MB
33°
Search
ENG IN
18:02 25-06-2024

Some Screenshots of Brute Force Attack




Attack Save
2. Intruder attack of http://testphp.vulnweb.com
2. Intruder attack of http://testphp.vulnweb.com
Attack
Save
Results
Positions
Payloads
Resource pool
Settings
Intruder attack results filter: Showing all items
Request
Payload 1
Payload 2
Status code
Response received
Error
Timeout
Length
Comment
0 200 363 6211
1 test test 200 365 6180
2 haryy test 200 366 6180
3 Manoj test 200 356 6180
4 test 200 363 6180
5 test haryy 200 349 6180
6 haryy haryy 200 363 6180
7 Manoj haryy 200 390 6180
8 haryy 200 346 6180
9 test Manoj 200 342 6180
10 haryy Manoj 200 478 6180
11 Manoj Manoj 200 344 6180
12 Manoj 200 326 6180
13 test 200 366 6180
14 haryy 200 341 6180
15 Manoj 200 330 6180
16 200 364 6180
Finished
ENG
IN
22:23
25-06-2024

Tools –

Tools Used

- **Burp Suite Community Edition**:

  For intercepting and modifying HTTP requests and responses.

- **Browser Configuration**:

  Firefox/Chrome configured to use Burp Suite proxy.

Created by

Hariom kumar
25-06-2024