Sri Lanka Institute of Information Technology

Web Security - IE2062

Cross-site request forgery (CSRF) Report

C.D Aluthge

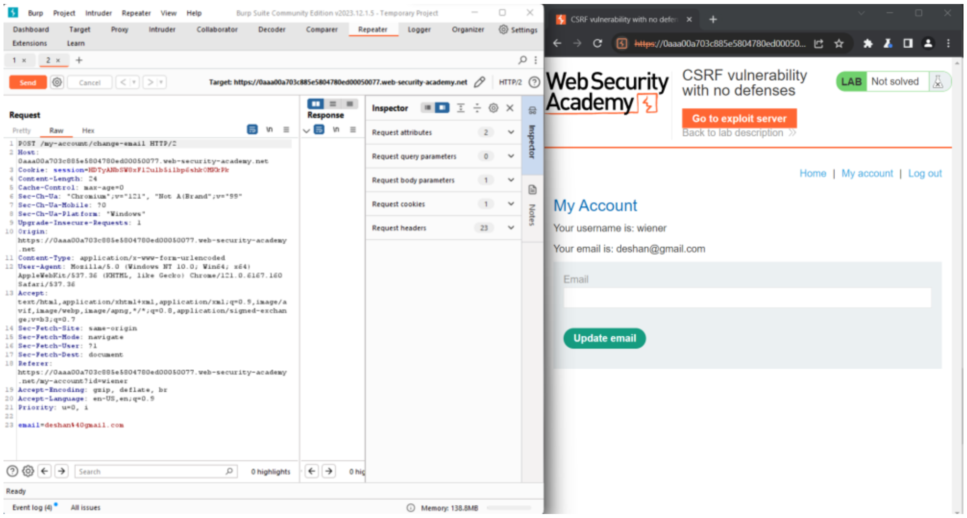
IT22581402

Y2S2

Weekday - Group 1.2

Lab 01

- Open Burp's browser and log in to your account. Submit the "Update email" form, and find the resulting request in your Proxy history.



Target: https://0aaa00a703c885e5804780ed00050077.web-security-academy.net HTTP/2

```
POST /my-account/change-email HTTP/2
Host:
0aaa00a703c885e5804780ed00050077.web-security-academy.net
Cookie: session=HDTyANbSW0xF12ulb5ilbp6shkOMKkPk
Content-Length: 24
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin:
https://0aaa00a703c885e5804780ed00050077.web-security-academy
.net
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/121.0.6167.160
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
ge;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0aaa00a703c885e5804780ed00050077.web-security-academy
.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

email=deshan%40gmail.com
```

https://0aaa00a703c885e5804780ed00050...

CSRF vulnerability with no defenses

My Account

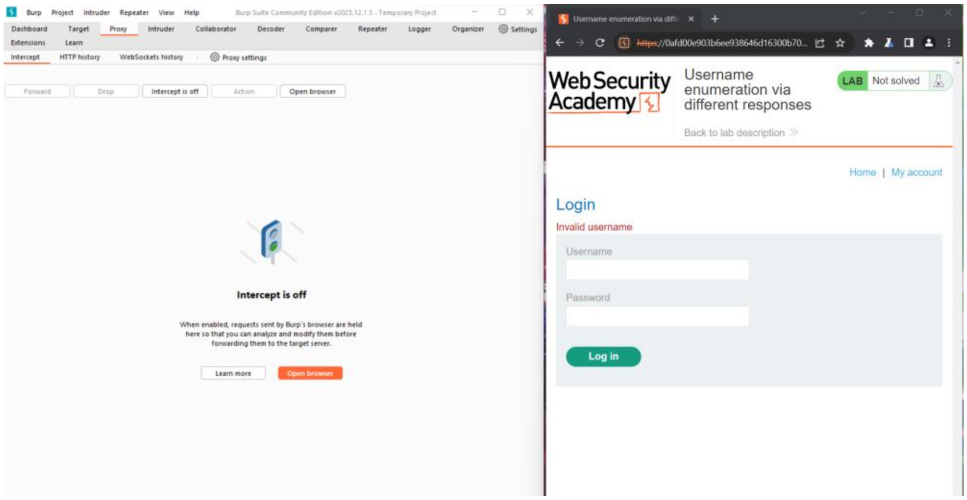
Your username is: wiener

Your email is: deshan@gmail.com

Email

Lab 02

- With Burp running, investigate the login page and submit an invalid username and password



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
Learn more
Open browser
Username enumeration via diff
https://0afd00e903b6ee938646d16300b70...
WebSecurity Academy
LAB Not solved
Back to lab description
Home | My account
Username
Password
Log in

Intercept is off

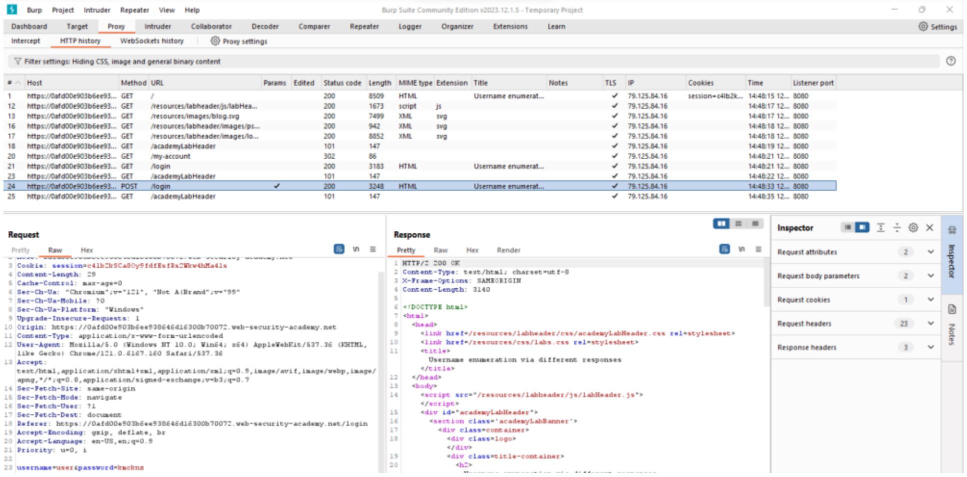
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Username enumeration via different responses

Login

Invalid username

- In Burp, go to Proxy > HTTP history and find the POST /login request. Highlight the value of the username parameter in the request and send it to Burp Intruder.



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.12.1.5 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Decoder Comparer Repeater Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Notes

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port
1	https://0afd00e903b6ee93...	GET	/			200	8509	HTML		Username enumerat...		✓	79.125.84.16	session=c4lb2k...	14:48:15 12...	8080
12	https://0afd00e903b6ee93...	GET	/resources/labheader/js/labHea...			200	1673	script	js			✓	79.125.84.16		14:48:17 12...	8080
13	https://0afd00e903b6ee93...	GET	/resources/images/blog.svg			200	7499	XML	svg			✓	79.125.84.16		14:48:17 12...	8080
16	https://0afd00e903b6ee93...	GET	/resources/labheader/images/ps...			200	942	XML	svg			✓	79.125.84.16		14:48:18 12...	8080
17	https://0afd00e903b6ee93...	GET	/resources/labheader/images/lo...			200	8852	XML	svg			✓	79.125.84.16		14:48:18 12...	8080
18	https://0afd00e903b6ee93...	GET	/academyLabHeader			101	147					✓	79.125.84.16		14:48:19 12...	8080
20	https://0afd00e903b6ee93...	GET	/my-account			302	86					✓	79.125.84.16		14:48:21 12...	8080
21	https://0afd00e903b6ee93...	GET	/login			200	3183	HTML		Username enumerat...		✓	79.125.84.16		14:48:21 12...	8080
23	https://0afd00e903b6ee93...	GET	/academyLabHeader			101	147					✓	79.125.84.16		14:48:22 12...	8080
24	https://0afd00e903b6ee93...	POST	/login	✓		200	3248	HTML		Username enumerat...		✓	79.125.84.16		14:48:33 12...	8080
25	https://0afd00e903b6ee93...	GET	/academyLabHeader			101	147					✓	79.125.84.16		14:48:35 12...	8080

Request

```
Cookie: session=c4lb2kSCa8Oy9fdfEsfRs2Wrw4hMa4ls
Content-Length: 29
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0afd00e903b6ee938646d16300b70072.web-security-academy.net
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/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: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0afd00e903b6ee938646d16300b70072.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

username=user&password=kmcknz
```

Response

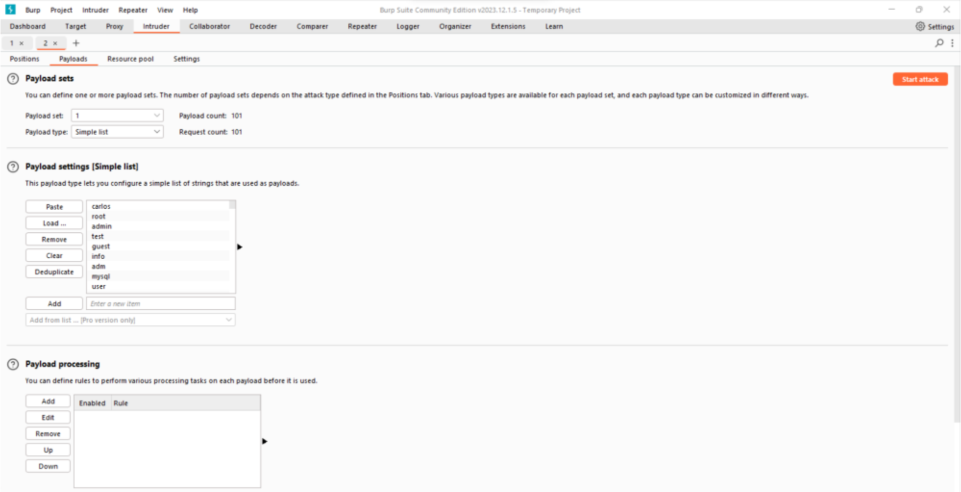
```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3140

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Username enumeration via different responses
    </title>
  </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>
```

Inspector	
Request attributes	2
Request body parameters	2
Request cookies	1
Request headers	23
Response headers	3

- Make sure that the Sniper attack type is selected.
- On the Payloads tab, make sure that the Simple list payload type is selected.
- Under Payload settings, paste the list of candidate usernames. Finally, click Start attack. The attack will start in a new window.
- When the attack is finished, on the Results tab, examine the Length column. You can click on the column header to sort the results. Notice that one of the

entries is longer than the others. Compare the response to this payload with the other responses. Notice that other responses contain the message Invalid username, but this response says Incorrect password. Make a note of the username in the Payload column.



Burp Suite Community Edition v2023.12.1.5 - Temporary Project

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 | Payload count: 101
Payload type: Simple list | Request count: 101

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

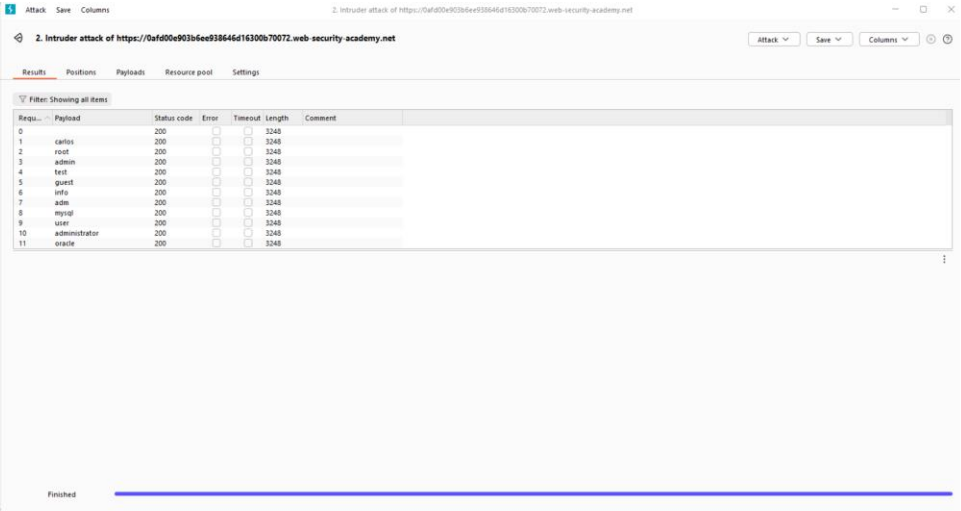
```
carlos
root
admin
test
guest
info
adm
mysql
user
```

Add from list ... [Pro version only]

Payload processing

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

Enabled	Rule



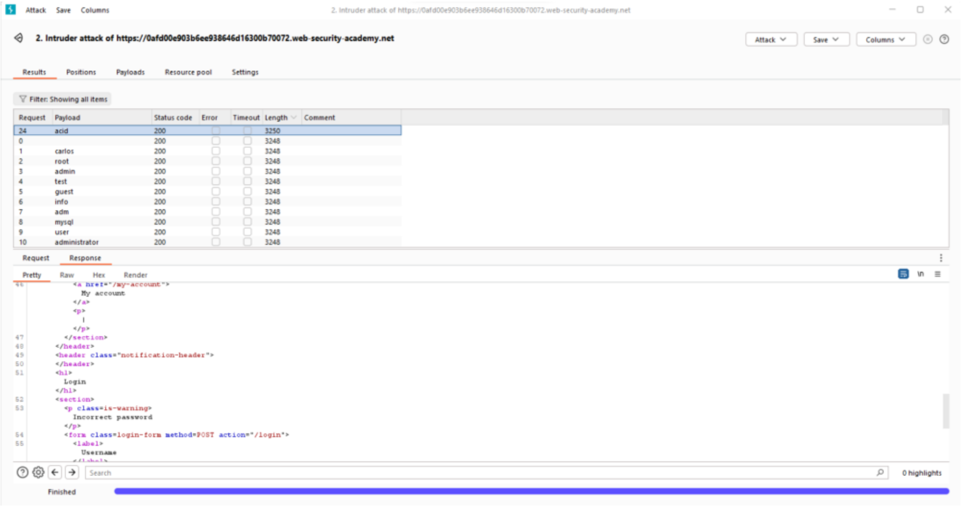
2. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net

Filter: Showing all items

Requ...	Payload	Status code	Error	Timeout	Length	Comment
0		200	□	□	3248	
1	carlos	200	□	□	3248	
2	root	200	□	□	3248	
3	admin	200	□	□	3248	
4	test	200	□	□	3248	
5	guest	200	□	□	3248	
6	info	200	□	□	3248	
7	adm	200	□	□	3248	
8	mysql	200	□	□	3248	
9	user	200	□	□	3248	
10	administrator	200	□	□	3248	
11	oracle	200	□	□	3248	

Finished

Attack
Save
Columns
2. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings

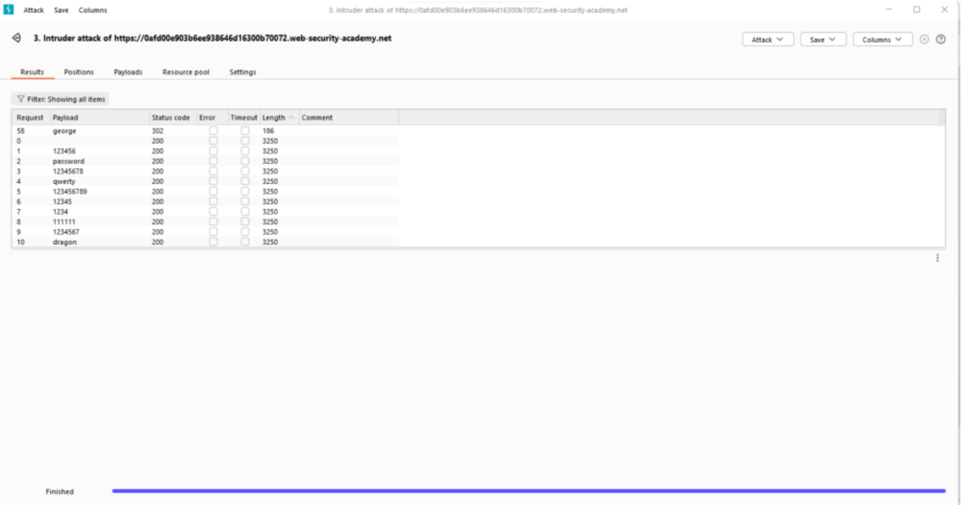

Attack Save Columns
2. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items

2. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net

Request	Payload	Status code	Error	Timeout	Length	Comment
24	acid	200	☐	☐	3250	
0		200	☐	☐	3248	
1	carlos	200	☐	☐	3248	
2	root	200	☐	☐	3248	
3	admin	200	☐	☐	3248	
4	test	200	☐	☐	3248	
5	guest	200	☐	☐	3248	
6	info	200	☐	☐	3248	
7	adm	200	☐	☐	3248	
8	mysql	200	☐	☐	3248	
9	user	200	☐	☐	3248	
10	administrator	200	☐	☐	3248	

```
        <a href="/my-account">
          My account
        </a>
        <p>
          |
        </p>
      </section>
    </header>
    <header class="notification-header">
    </header>
    <h1>
      Login
    </h1>
    <section>
      <p class=is-warning>
        Incorrect password
      </p>
      <form class=login-form method=POST action="/login">
        <label>
          Username
```

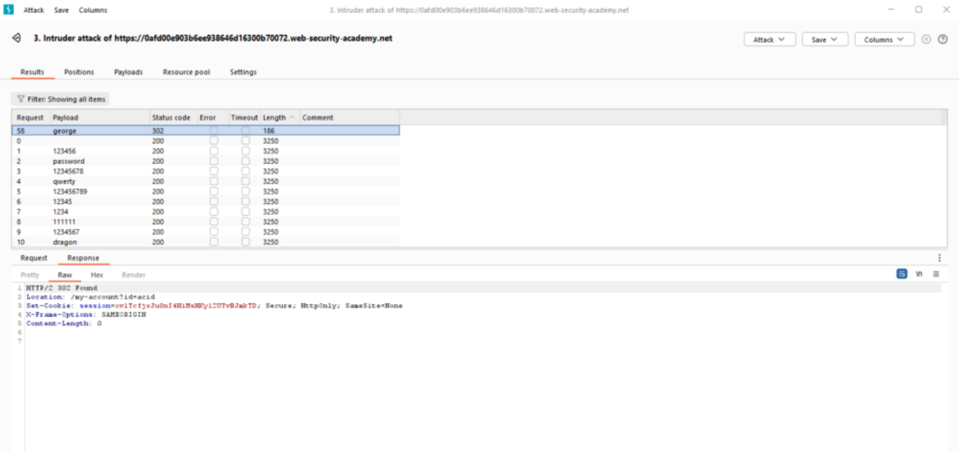
- Close the attack and go back to the Positions tab. Click Clear, then change the username parameter to the username you just identified. Add a payload position to the password parameter. The result should look something like this:
-
- username=identified-user&password=§invalid-password§
- On the Payloads tab, clear the list of usernames and replace it with the list of candidate passwords. Click Start attack.
- When the attack is finished, look at the Status column. Notice that each request received a response with a 200 status code except for one, which got a 302 response. This suggests that the login attempt was successful - make a note of the password in the Payload column.
- Log in using the username and password that you identified and access the user account page to solve the lab.



Attack
Save
Columns
3. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Finished

3. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net

Request	Payload	Status code	Error	Timeout	Length	Comment
58	george	302	□	□	186	
0		200	□	□	3250	
1	123456	200	□	□	3250	
2	password	200	□	□	3250	
3	12345678	200	□	□	3250	
4	qwerty	200	□	□	3250	
5	123456789	200	□	□	3250	
6	12345	200	□	□	3250	
7	1234	200	□	□	3250	
8	111111	200	□	□	3250	
9	1234567	200	□	□	3250	
10	dragon	200	□	□	3250	



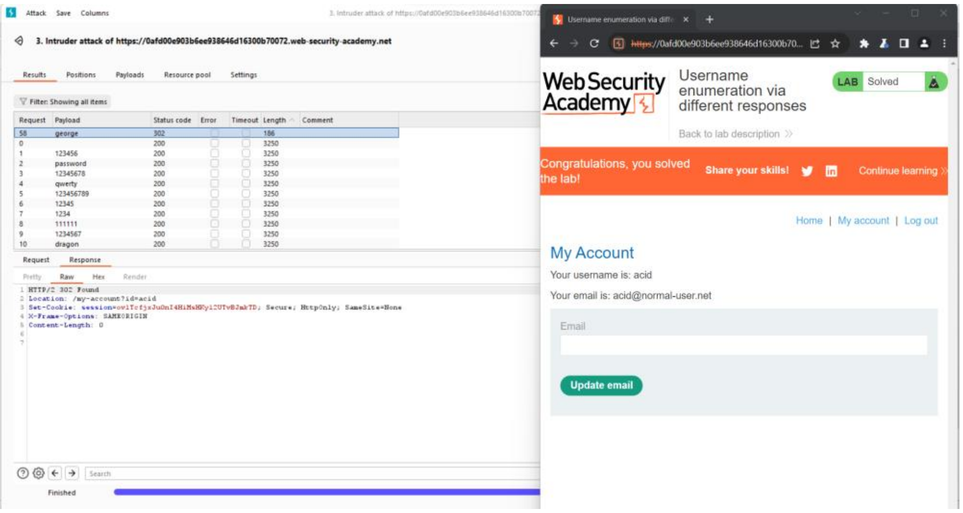
Attack
Save
Columns
3. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items
Request
Response
Pretty
Raw
Hex
Render

3. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net

Request	Payload	Status code	Error	Timeout	Length	Comment
58	george	302	□	□	186	
0		200	□	□	3250	
1	123456	200	□	□	3250	
2	password	200	□	□	3250	
3	12345678	200	□	□	3250	
4	qwerty	200	□	□	3250	
5	123456789	200	□	□	3250	
6	12345	200	□	□	3250	
7	1234	200	□	□	3250	
8	111111	200	□	□	3250	
9	1234567	200	□	□	3250	
10	dragon	200	□	□	3250	

```
HTTP/2 302 Found
Location: /my-account?id=acid
Set-Cookie: session=ovlTcfjxJu0nI4HiMsHKyl2UTvBJmkTD; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```



3. Intruder attack of https://0afd00e903b6ee938646d16300b70072.web-security-academy.net

Request	Payload	Status code	Error	Timeout	Length	Comment
58	george	302	□	□	186	
0		200	□	□	3250	
1	123456	200	□	□	3250	
2	password	200	□	□	3250	
3	12345678	200	□	□	3250	
4	qwerty	200	□	□	3250	
5	123456789	200	□	□	3250	
6	12345	200	□	□	3250	
7	1234	200	□	□	3250	
8	111111	200	□	□	3250	
9	1234567	200	□	□	3250	
10	dragon	200	□	□	3250	

```
HTTP/2 302 Found
Location: /my-account?id=acid
Set-Cookie: session=ovlTcfjxJu0nI4HiMsHKyl2UTvBJmkTD; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```

Username enumeration via different responses

Congratulations, you solved the lab!

My Account

Your username is: acid

Your email is: acid@normal-user.net

Email