

Cyber Security and Digital
Forensics Internship

ASSIGNMENT 5

TYPES OF
INJECTIONS

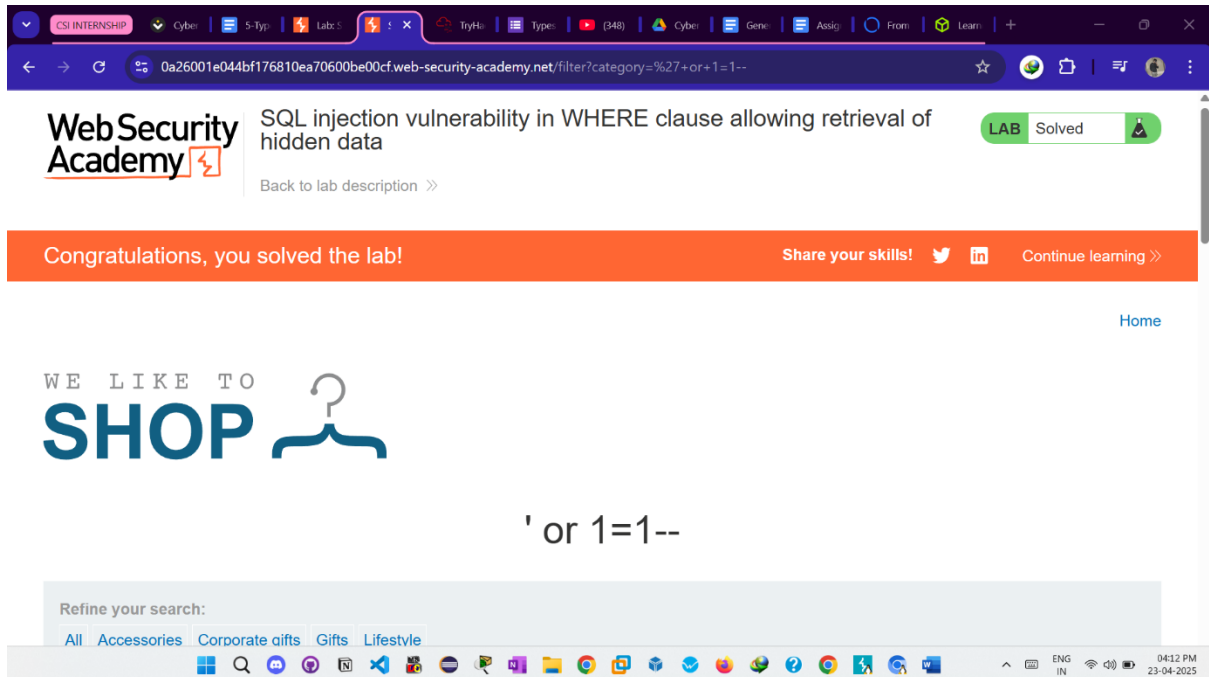
SWASTIK GONDHI

DOON UNIVERSITY

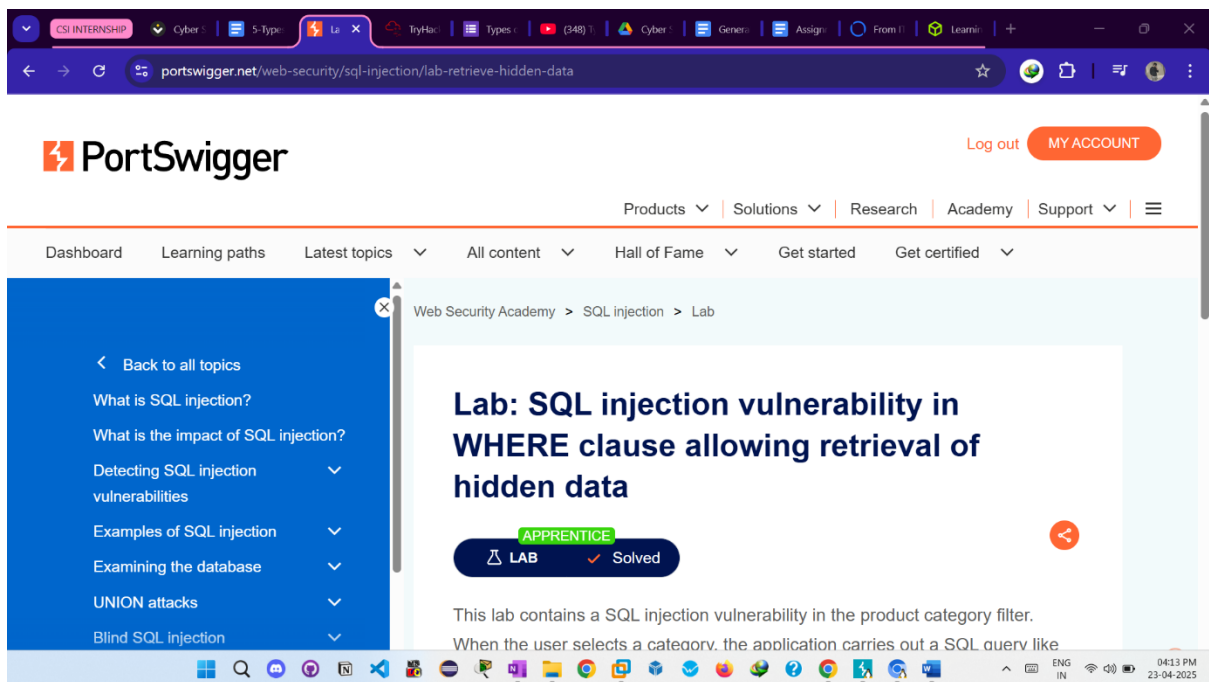
Drive Link -

<https://drive.google.com/drive/folders/1WCK00ki1F3lFPTto7y5tdSmeKcrDeWjvs?usp=sharing>

PORTSWIGGER LAB-1

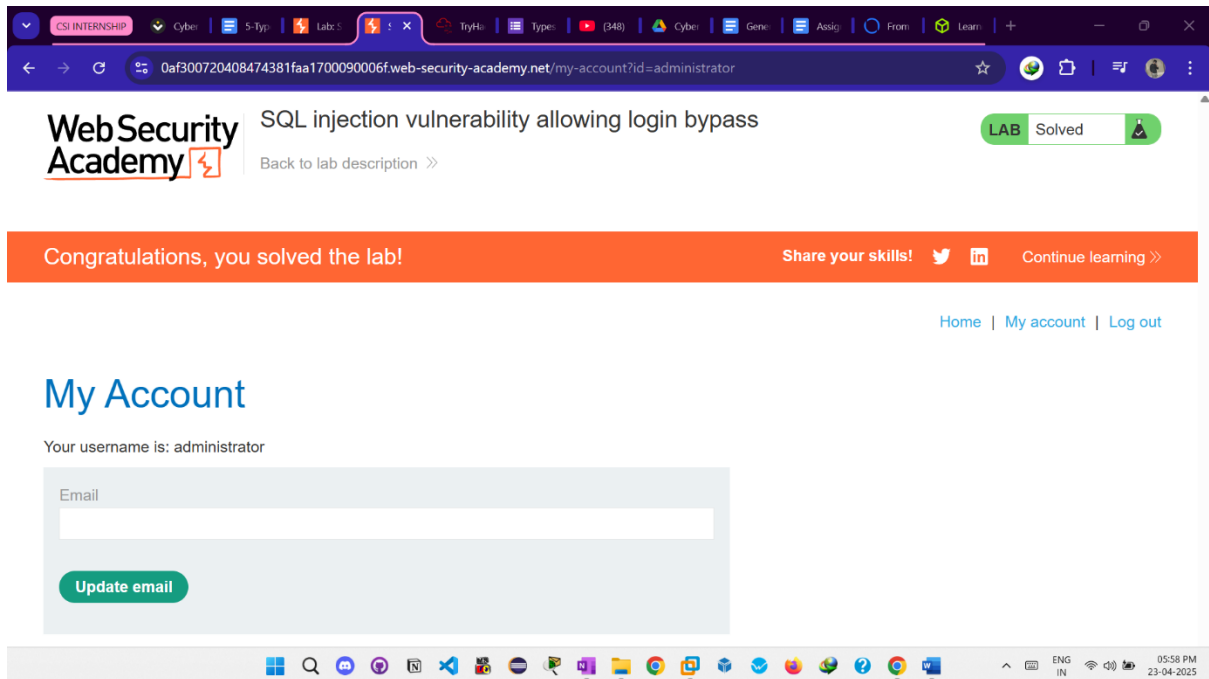


This screenshot shows a web browser window with the URL `0a26001e044bf176810ea70600be00cf.web-security-academy.net/filter?category=%27+or+1=1--`. The page title is "SQL injection vulnerability in WHERE clause allowing retrieval of hidden data". A green "LAB Solved" badge is visible in the top right. Below the title, there is an orange banner that says "Congratulations, you solved the lab!". To the right of the banner are links for "Share your skills!", "Continue learning >>", and a "Home" link. The main content area displays a shopping cart icon and the text "WE LIKE TO SHOP". Below this, the payload "' or 1=1--" is shown. At the bottom, there is a search bar with the text "Refine your search:" and a list of categories: "All", "Accessories", "Corporate gifts", "Gifts", and "Lifestyle". The Windows taskbar is visible at the bottom of the browser window.

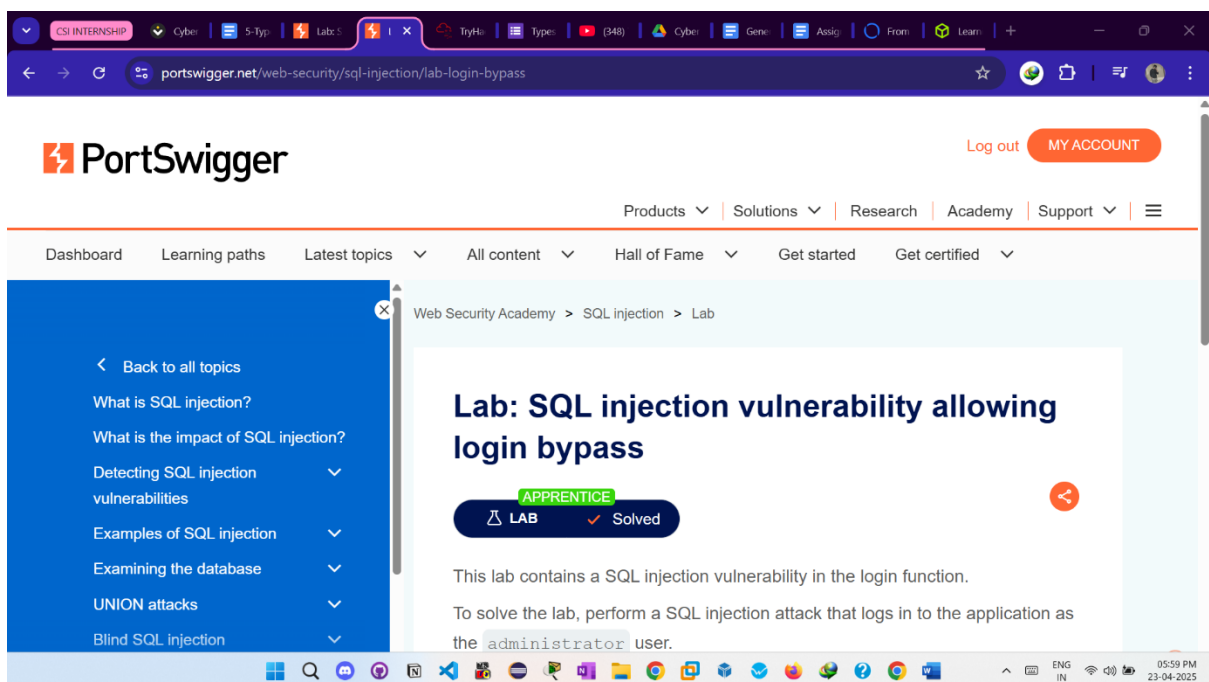


This screenshot shows the PortSwigger Academy website. The URL is `portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data`. The page features the PortSwigger logo and a navigation bar with links for "Products", "Solutions", "Research", "Academy", and "Support". Below the navigation bar, there is a sidebar with a list of topics: "Back to all topics", "What is SQL injection?", "What is the impact of SQL injection?", "Detecting SQL injection vulnerabilities", "Examples of SQL injection", "Examining the database", "UNION attacks", and "Blind SQL injection". The main content area displays the lab title "Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data" and a green "APPRENTICE" badge. Below the title, there is a blue "LAB Solved" badge. The text below the badge states: "This lab contains a SQL injection vulnerability in the product category filter. When the user selects a category, the application carries out a SQL query like". The Windows taskbar is visible at the bottom of the browser window.

PORTSWIGGER LAB-2



This screenshot shows the completion page for a lab on the WebSecurity Academy website. The browser's address bar displays the URL: `0af300720408474381faa1700090006f.web-security-academy.net/my-account?id=administrator`. The page header includes the WebSecurity Academy logo, the lab title "SQL injection vulnerability allowing login bypass", and a "LAB Solved" badge. A green banner at the top of the main content area reads "Congratulations, you solved the lab!". Below this, there are links to "Share your skills!" (with social media icons), "Continue learning >>", and a navigation bar with "Home", "My account", and "Log out". The "My Account" section shows the username "administrator" and an "Update email" form with a text input field and a green "Update email" button. The Windows taskbar at the bottom shows the time as 05:58 PM on 23-04-2025.



This screenshot shows the PortSwigger website interface for the same lab. The browser's address bar shows the URL: `portswigger.net/web-security/sql-injection/lab-login-bypass`. The PortSwigger logo is in the top left, and "Log out" and "MY ACCOUNT" buttons are in the top right. A navigation menu includes "Products", "Solutions", "Research", "Academy", and "Support". Below this is a secondary menu with "Dashboard", "Learning paths", "Latest topics", "All content", "Hall of Fame", "Get started", and "Get certified". The main content area is titled "Web Security Academy > SQL injection > Lab" and features the lab title "Lab: SQL injection vulnerability allowing login bypass". A badge indicates the lab is "APPRENTICE" level and "Solved". The text describes the lab: "This lab contains a SQL injection vulnerability in the login function. To solve the lab, perform a SQL injection attack that logs in to the application as the `administrator` user." The Windows taskbar at the bottom shows the time as 05:59 PM on 23-04-2025.

PORTSWIGGER LAB-3

The screenshot shows a web browser window with the URL `0a7f00d1033f67cb81cc3ead005f001c.web-security-academy.net/filter?category=Accessories%27+UNION+SELECT+BANNER...`. The page header includes the Web Security Academy logo and the title "SQL injection attack, querying the database type and version on Oracle". A green "LAB Solved" badge is visible. Below the title, there is a message "Congratulations, you solved the lab!" and a "Share your skills!" button. The main content area displays the text "Accessories' UNION SELECT BANNER, NULL FROM v\$version--".

The screenshot shows the PortSwigger Academy website. The header includes the PortSwigger logo and a "Log out MY ACCOUNT" button. The navigation menu includes "Products", "Solutions", "Research", "Academy", and "Support". The main content area displays the title "Lab: SQL injection attack, querying the database type and version on Oracle". A "PRACTITIONER" badge is visible, along with a "LAB Solved" badge. The text below the title states: "This lab contains a SQL injection vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query. To solve the lab, display the database version string."

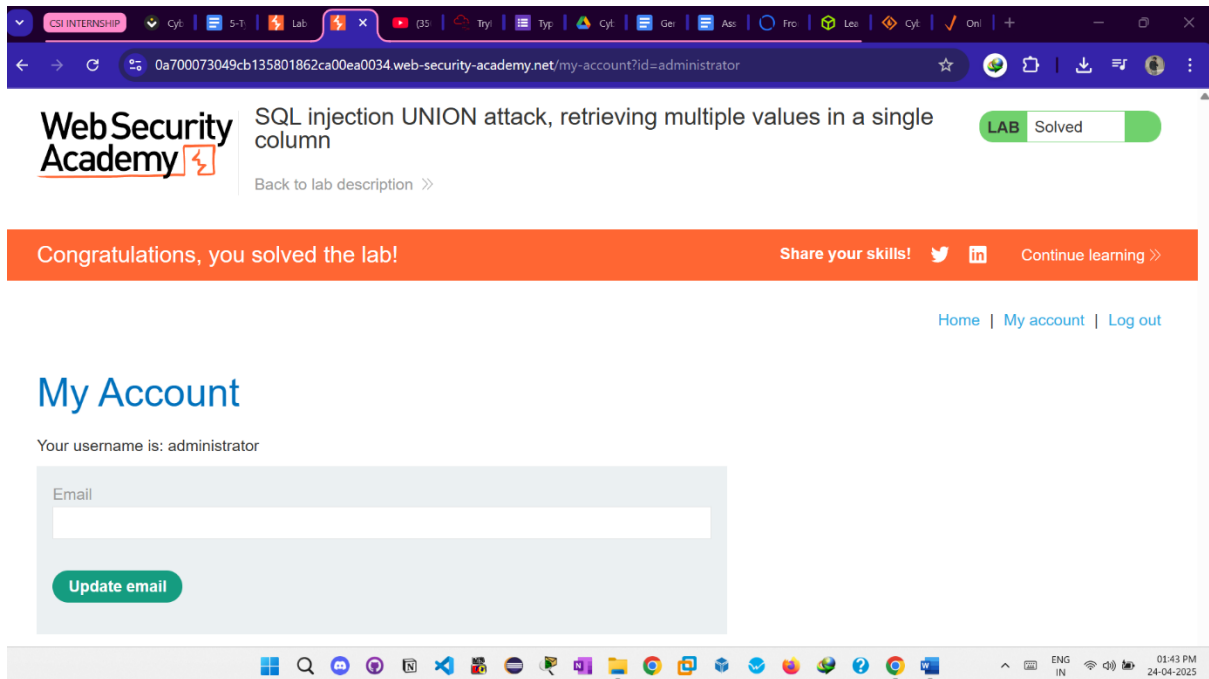
PORTSWIGGER LAB-4

The screenshot shows a web browser window with the URL `0a7f00d1033f67cb81cc3ead005f001c.web-security-academy.net/filter?category=Accessories%27+UNION+SELECT+BANNER,...`. 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!' with links to 'Share your skills!' and 'Continue learning >>'. The main content area displays a shopping cart icon and the text 'Accessories' UNION SELECT BANNER, NULL FROM v\$version--'. The browser's taskbar at the bottom shows various application icons and the system clock indicating 01:32 PM on 24-04-2025.

The screenshot shows the PortSwigger website interface. The top navigation bar includes links for 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. A sidebar on the left lists various topics under 'Web Security Academy > SQL injection > Examining the database > Lab'. The main content area features the lab title 'Lab: SQL injection attack, querying the database type and version on Oracle' and a 'PRACTITIONER LAB Solved' badge. The lab description states: 'This lab contains a SQL injection vulnerability in the product category filter. You can use a UNION attack to retrieve the results from an injected query. To solve the lab, display the database version string.' The browser's taskbar at the bottom shows various application icons and the system clock indicating 01:34 PM on 24-04-2025.

IT WAS THE SAME LAB AS THE PREVIOUS ONE

PORTSWIGGER LAB-5



This screenshot shows the WebSecurity Academy interface. The browser address bar displays the URL: 0a700073049cb135801862ca00ea0034.web-security-academy.net/my-account?id=administrator. The page header includes the WebSecurity Academy logo and the lab title: "SQL injection UNION attack, retrieving multiple values in a single column". A green "LAB Solved" badge is visible. Below the header, an orange banner reads "Congratulations, you solved the lab!". Navigation links for "Home", "My account", and "Log out" are present. The "My Account" section shows the username "administrator" and an "Update email" button.

WebSecurity 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! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

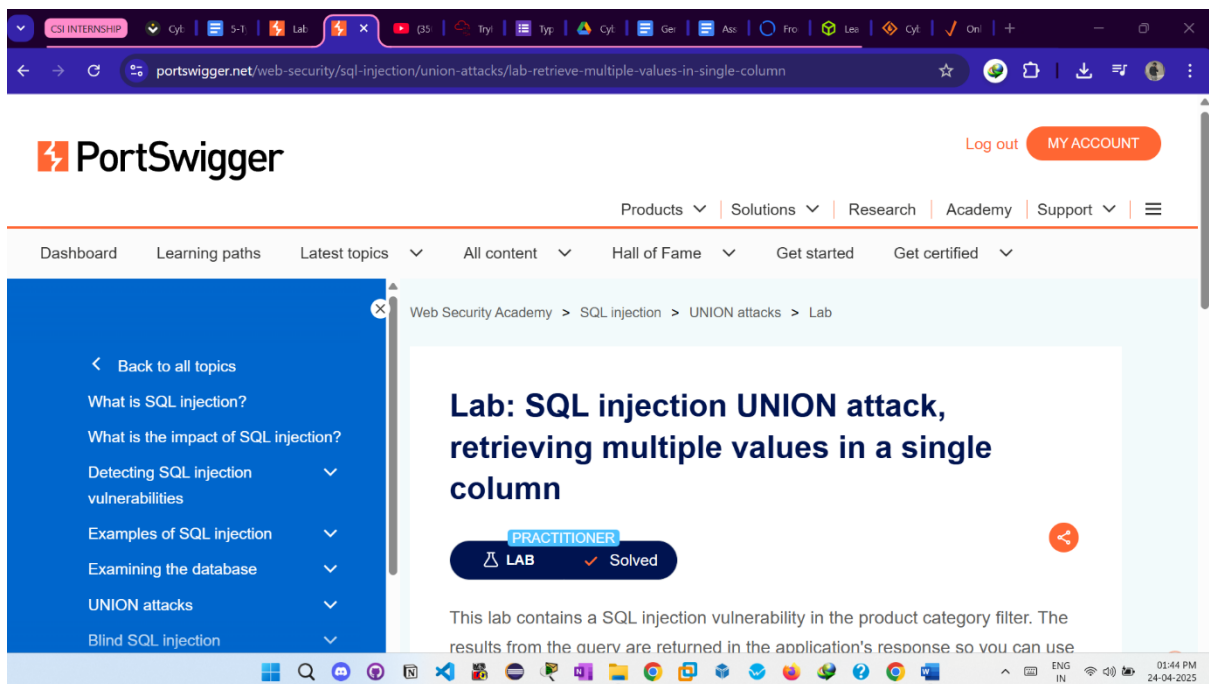
[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

Update email



This screenshot shows the PortSwigger Academy interface. The browser address bar displays the URL: portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-multiple-values-in-single-column. The page header includes the PortSwigger logo and a "Log out MY ACCOUNT" button. The navigation menu includes "Products", "Solutions", "Research", "Academy", and "Support". The main content area shows the lab title: "Lab: SQL injection UNION attack, retrieving multiple values in a single column". A "PRACTITIONER LAB Solved" badge is visible. The lab description states: "This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use".

PortSwigger

Log out MY ACCOUNT

Products Solutions Research Academy Support

Dashboard Learning paths Latest topics All content Hall of Fame Get started Get certified

Web Security Academy > SQL injection > UNION attacks > Lab

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

PRACTITIONER LAB Solved

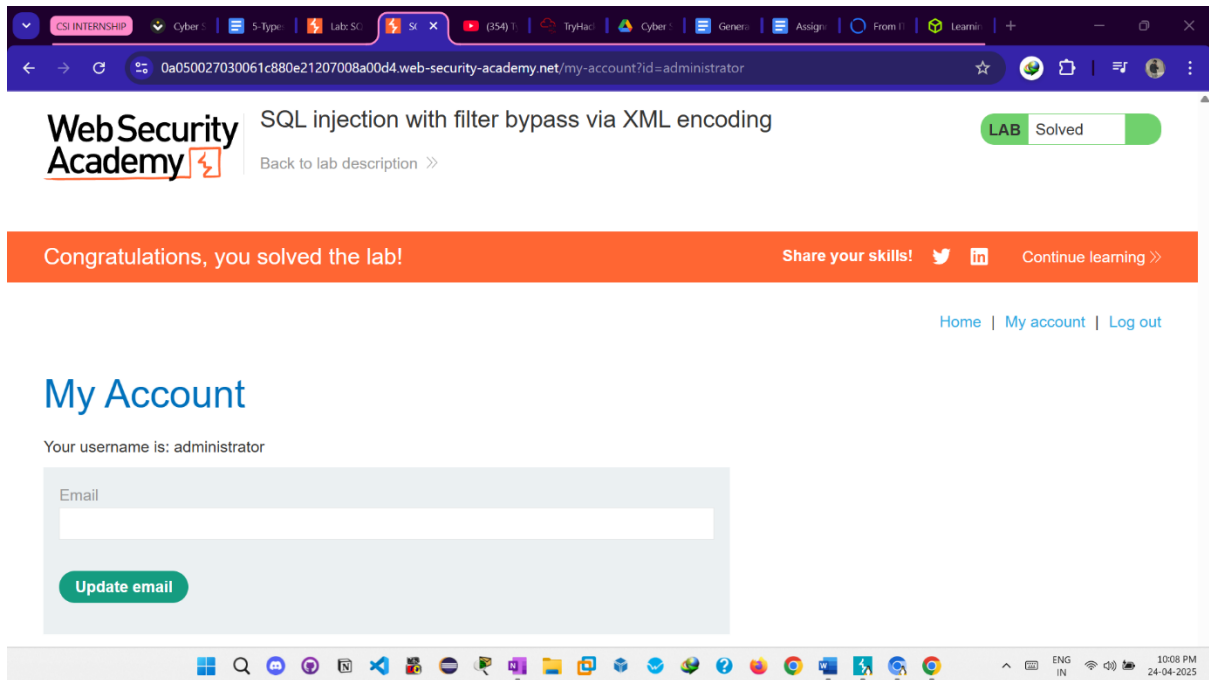
This lab contains a SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response so you can use

PORTSWIGGER LAB-6

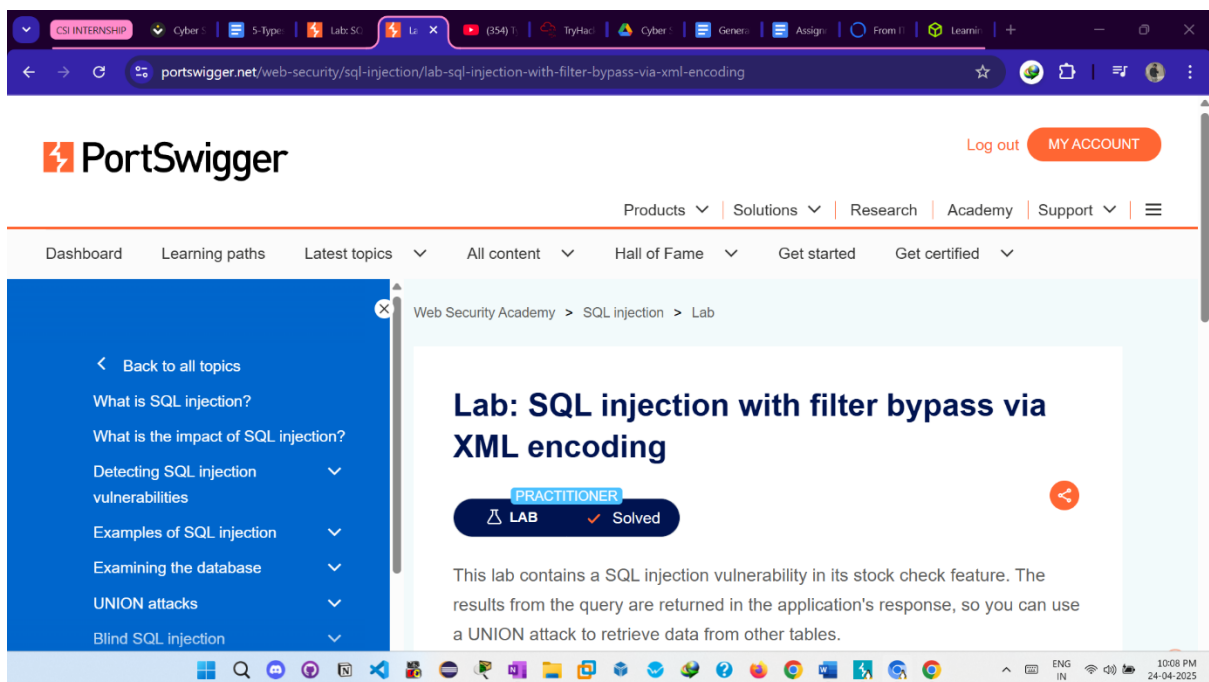
The screenshot shows a web browser window with the URL `0a1400280304a6eb80204446006d003b.web-security-academy.net`. The page header includes the Web Security Academy logo and the lab title "Blind SQL injection with time delays". A green "LAB Solved" badge is visible. Below the header, an orange banner reads "Congratulations, you solved the lab!". Navigation links for "Share your skills!" (with Twitter and LinkedIn icons) and "Continue learning >>" are present. At the bottom, there are links for "Home" and "My account".

The screenshot shows the PortSwigger Academy website. The top navigation bar includes "Log out" and "MY ACCOUNT". Below this, a secondary navigation bar lists "Products", "Solutions", "Research", "Academy", and "Support". The main content area is titled "Lab: Blind SQL injection with time delays" and includes a "PRACTITIONER" badge and a "LAB Solved" status. A sidebar on the left lists various topics under "Web Security Academy > SQL injection > Blind > Lab", including "What is SQL injection?", "What is the impact of SQL injection?", "Detecting SQL injection vulnerabilities", "Examples of SQL injection", "Examining the database", "UNION attacks", and "Blind SQL injection". The main text describes the lab's vulnerability: "This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs a SQL query containing the value of the submitted cookie. The results of the SQL query are not returned, and the application does not".

PORTSWIGGER LAB-7



This screenshot shows the 'My Account' page on the WebSecurity Academy website. The browser's address bar displays the URL: `0a050027030061c880e21207008a00d4.web-security-academy.net/my-account?id=administrator`. The page header includes the WebSecurity Academy logo, the lab title 'SQL injection with filter bypass via XML encoding', and a 'LAB Solved' status indicator. A green banner at the top of the main content area reads 'Congratulations, you solved the lab!' and includes links to 'Share your skills!', 'Continue learning >>', and 'Back to lab description >>'. Below this, the 'My Account' section shows the username 'administrator' and an email update form with an 'Update email' button. The Windows taskbar at the bottom shows the time as 10:08 PM on 24-04-2025.




This screenshot shows the PortSwigger website's lab page. The browser's address bar displays the URL: `portswigger.net/web-security/sql-injection/lab-sql-injection-with-filter-bypass-via-xml-encoding`. The page header features the PortSwigger logo, a 'Log out' button, and a 'MY ACCOUNT' button. A navigation bar includes links for 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. Below this, a secondary navigation bar lists 'Dashboard', 'Learning paths', 'Latest topics', 'All content', 'Hall of Fame', 'Get started', and 'Get certified'. The main content area is titled 'Lab: SQL injection with filter bypass via XML encoding' and includes a 'PRACTITIONER' badge, a 'LAB Solved' status, and a description: 'This lab contains a SQL injection vulnerability in its stock check feature. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables.' A left sidebar contains a list of topics, including 'What is SQL injection?', 'What is the impact of SQL injection?', 'Detecting SQL injection vulnerabilities', 'Examples of SQL injection', 'Examining the database', 'UNION attacks', and 'Blind SQL injection'. The Windows taskbar at the bottom shows the time as 10:08 PM on 24-04-2025.

TRYHACKME ROOM-1

tryhackme.com/room/sqlinjectionlm

Woop woopl! Your answer is correct



Congratulations on completing SQL Injection!!! 🎉

Points earned 🔥 104	Completed tasks ✅ 10	Room type 👤 Walkthrough	Difficulty 📊 Medium	Streak 🔥 1
------------------------	-------------------------	----------------------------	------------------------	---------------

Leave Feedback Next

tryhackme.com/room/sqlinjectionlm

SQL Injection
Learn how to detect and exploit SQL injection vulnerabilities
Medium 30 min

Share your achievement Start Attackbox Help Save Room 5035 Options

Task 1: Brief
Task 2: What is a Database?
Task 3: What is SQL?
Task 4: What is SQL Injection?
Task 5: In-Band SQLi
Task 6: Blind SQLi - Authentication Bypass
Task 7: Blind SQLi - Boolean Based
Task 8: Blind SQLi - Time Based
Task 9: Out-of-Band SQLi
Task 10: Remediation

How likely are you to recommend this room to others?