

Cyber Security and Digital
Forensics Internship

ASSIGNMENT 6
BROKEN
AUTHENTICATION

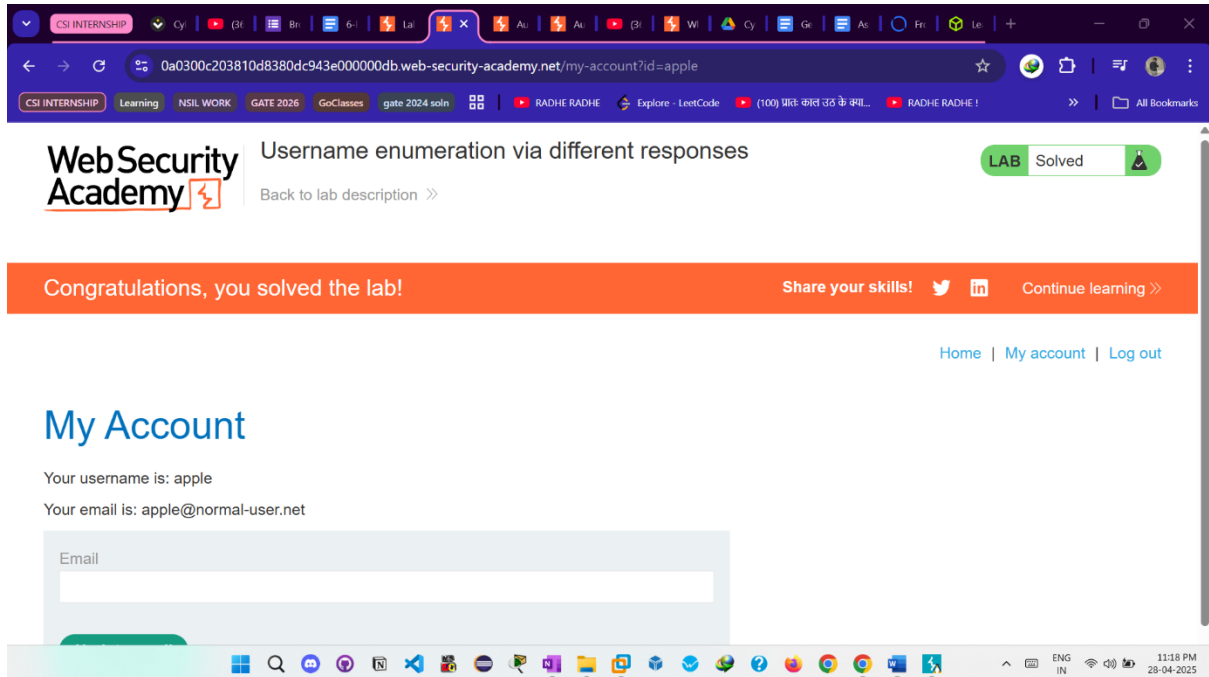
SWASTIK GONDHI

DOON UNIVERSITY

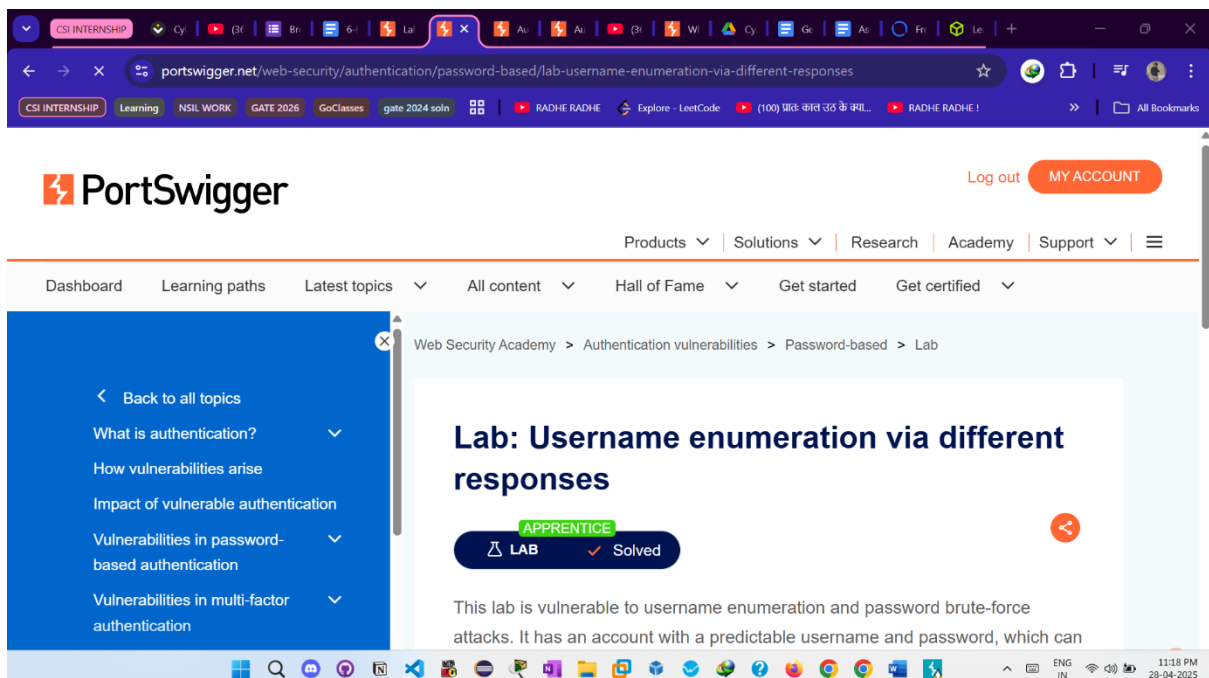
Drive Link -

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

PORTSWIGGER LAB - Username enumeration via different responses



This screenshot shows the completion page of a lab on the Web Security Academy website. The browser's address bar displays the URL: `0a0300c203810d8380dc943e000000db.web-security-academy.net/my-account?id=apple`. The page header includes the Web Security Academy logo and the lab title "Username enumeration via different responses", which is marked as "LAB Solved". 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 displays the user's details: "Your username is: apple" and "Your email is: apple@normal-user.net". There is an input field for the email address. The bottom of the page shows a Windows taskbar with various application icons and a system clock indicating 11:18 PM on 28-04-2025.



This screenshot shows the lab page on the PortSwigger website. The browser's address bar shows the URL: `portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses`. The PortSwigger logo is at the top left, with "Log out" and "MY ACCOUNT" buttons at the top right. A navigation bar contains 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 features a sidebar on the left with a list of topics under "Web Security Academy > Authentication vulnerabilities > Password-based > Lab". The main title is "Lab: Username enumeration via different responses", with a green "APPRENTICE" tag and a "LAB Solved" badge. The description states: "This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can". The bottom of the page shows a Windows taskbar with various application icons and a system clock indicating 11:18 PM on 28-04-2025.

PORTSWIGGER LAB - Username enumeration via subtly different responses

The screenshot shows the Web Security Academy interface. The browser address bar displays the URL: `0a5d00b30460b90480f2808a008d00e7.web-security-academy.net/my-account?id=app01`. The page title is "Username enumeration via subtly different responses". A green badge in the top right corner indicates "LAB Solved". Below the title, there is a "Back to lab description" link. A large orange banner across the middle of the page reads "Congratulations, you solved the lab!". To the right of this banner are links for "Share your skills!", social media icons for Twitter and LinkedIn, and a "Continue learning" link. Below the banner, there are links for "Home", "My account", and "Log out". The "My Account" section displays the user's details: "Your username is: app01" and "Your email is: app01@normal-user.net". There is an "Email" input field and an "Update email" button. The Windows taskbar at the bottom shows the time as 01:45 PM on 29-04-2025.

The screenshot shows the PortSwigger website. The browser address bar displays the URL: `portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-subtly-different-responses`. The PortSwigger logo is in the top left, and "Log out" and "MY ACCOUNT" buttons are in the top right. A navigation bar includes links for "Products", "Solutions", "Research", "Academy", and "Support". Below this is a secondary navigation bar with links for "Dashboard", "Learning paths", "Latest topics", "All content", "Hall of Fame", "Get started", and "Get certified". The main content area shows the lab details for "Web Security Academy > Authentication vulnerabilities > Password-based > Lab". The lab title is "Lab: Username enumeration via subtly different responses". A blue badge indicates "PRACTITIONER" and a green badge indicates "LAB Solved". The lab description states: "This lab is subtly vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:". The Windows taskbar at the bottom shows the time as 01:45 PM on 29-04-2025.

PORTSWIGGER LAB- Username enumeration via response timing

The screenshot shows a web browser window with the URL `0a1400f103e40ba081afeda6005b004d.web-security-academy.net/my-account?id=afiliados`. The page header includes the Web Security Academy logo and the lab title "Username enumeration via response timing". A green badge indicates the lab is "Solved". Below the header, an orange banner congratulates the user: "Congratulations, you solved the lab!". Navigation links for "Home", "My account", and "Log out" are present. The "My Account" section displays the user's details: "Your username is: afiliados" and "Your email is: afiliados@normal-user.net". There is an "Email" input field and an "Update email" button.

The screenshot shows the PortSwigger Academy website. The top navigation bar includes links for "Products", "Solutions", "Research", "Academy", and "Support". The "Academy" section is active, showing a breadcrumb trail: "Web Security Academy > Authentication vulnerabilities > Password-based > Lab". The lab title "Lab: Username enumeration via response timing" is prominently displayed. A badge indicates the lab is "Solved". The lab description states: "This lab is vulnerable to username enumeration using its response times. To solve the lab, enumerate a valid username, brute-force this user's password,". A sidebar on the left lists various topics under "Latest topics", including "What is authentication?", "How vulnerabilities arise", "Impact of vulnerable authentication", "Vulnerabilities in password-based authentication", and "Vulnerabilities in multi-factor authentication".

PORTSWIGGER LAB- 2FA SIMPLE BYPASS

The screenshot shows the '2FA simple bypass' lab page on the Web Security Academy website. The browser's address bar displays the URL: `0a99003604294d4c81db75c700ce0093.web-security-academy.net/my-account`. The page header includes the Web Security Academy logo and the lab title '2FA simple bypass'. A green badge in the top right corner indicates 'LAB Solved'. Below the header, an orange banner reads 'Congratulations, you solved the lab!' with links to 'Share your skills!', 'Continue learning >>', and 'Back to lab description >>'. The 'My Account' section shows the username 'carlos' and email 'carlos@carlos-montoya.net', with an 'Update email' button. The bottom of the page shows a Windows taskbar with various application icons and a system tray with the time '07:38 PM' and date '29-04-2025'.

The screenshot shows the 'Lab: 2FA simple bypass' page on the PortSwigger website. The browser's address bar displays the URL: `portswigger.net/web-security/authentication/multi-factor/lab-2fa-simple-bypass`. The page header includes the PortSwigger logo and a 'Log out MY ACCOUNT' button. The navigation bar lists 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. The main content area shows the lab title 'Lab: 2FA simple bypass' with an 'APPRENTICE' badge and a 'LAB Solved' status. The lab description states: 'This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.' A hint section shows 'Your credentials: wiener:peter'. The bottom of the page shows a Windows taskbar with various application icons and a system tray with the time '07:39 PM' and date '29-04-2025'.

PORTSWIGGER LAB- 2FA Broken Logic

This screenshot shows the '2FA broken logic' lab page on the Web Security Academy website. The browser's address bar displays the URL '0aba00950407af6e8013f8c400e000b6.web-security-academy.net'. The page header includes the 'Web Security Academy' logo, the lab title '2FA broken logic', and a 'LAB Solved' badge. A green banner at the top of the main content area reads 'Congratulations, you solved the lab!' and includes links to 'Share your skills!' and 'Continue learning >>'. Below this, there are links for 'Home' and 'My account'. The main content area features a large heading 'WE LIKE TO BLOG' with a stylized face icon, followed by a blurred image of a smartphone screen. The Windows taskbar at the bottom shows various application icons and the system clock indicating 08:54 PM on 29-04-2025.

This screenshot shows the 'My Account' page on the Web Security Academy website. The browser's address bar shows the URL '0aba00950407af6e8013f8c400e000b6.web-security-academy.net/my-account?id=carlos'. The page header includes the 'Web Security Academy' logo, the lab title '2FA broken logic', and a 'LAB Solved' badge. A green banner at the top of the main content area reads 'Congratulations, you solved the lab!' and includes links to 'Share your skills!' and 'Continue learning >>'. Below this, there are links for 'Home', 'My account', and 'Log out'. The main content area is titled 'My Account' and displays the user's details: 'Your username is: carlos' and 'Your email is: carlos@carlos-montoya.net'. There is a form with an 'Email' label and a text input field, followed by an 'Update email' button. The Windows taskbar at the bottom shows various application icons and the system clock indicating 08:54 PM on 29-04-2025.

PRACTITIONER
 LAB **Solved**

• Your credentials: wiener:peter

PORTSWIGGER LAB- Password reset broken logic

This screenshot shows the 'Password reset broken logic' lab page on the Web Security Academy website. The browser's address bar displays the URL: `0aae00a6031791378013df910045000b.web-security-academy.net/my-account?id=carlos`. The page header includes the 'Web Security Academy' logo and a 'LAB Solved' badge. A green banner at the top reads 'Congratulations, you solved the lab!' with links to 'Share your skills!', 'Continue learning >>', 'Home', 'My account', and 'Log out'. The 'My Account' section shows the user's details: 'Your username is: carlos' and 'Your email is: carlos@carlos-montoya.net'. Below this is an email update form with an 'Update email' button. The Windows taskbar at the bottom shows the time as 09:18 PM on 29-04-2025.

This screenshot shows the 'Lab: Password reset broken logic' page on the PortSwigger website. The browser's address bar displays the URL: `portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-broken-logic`. A blue banner at the top promotes a live demo of Burp Suite DAST. The page header includes the PortSwigger logo, a 'Log out' button, and a 'MY ACCOUNT' button. The navigation menu includes 'Products', 'Solutions', 'Research', 'Academy', and 'Support'. The main content area shows the lab title 'Lab: Password reset broken logic' with an 'APPRENTICE' badge and a 'LAB Solved' status. The lab description states: 'This lab's password reset functionality is vulnerable. To solve the lab, reset Carlos's password then log in and access his "My account" page.' Below this, the credentials 'Your credentials: wiener:peter' are displayed. The Windows taskbar at the bottom shows the time as 09:19 PM on 29-04-2025.

PS: Could have solved all the remaining labs also, but could manage this much only..will give my best to submit the remaining ones also in the next checkpoint for sure. I really gave my best to solve these much also, it was tough to manage with college work , but I am happy to do this much also. Thanks to Cyber Secured India for such an amazing internship.