

Screenshot of a web browser showing a solved lab on the Web Security Academy platform.

The browser tabs show completed labs: "Lab: Username enumeration via account lock", "Username enumeration via account lock", "Username enumeration via account lock", "Authentication lab usernames", and "Authentication lab passwords".

The address bar shows the URL: <https://0a3a001803c899b185cb0d5d00d000fa.web-security-academy.net/login>.

The main content area displays the "Web Security Academy" logo and the title "Username enumeration via account lock". A green button indicates the task is "Solved".

A banner at the bottom says "Congratulations, you solved the lab!" and includes links for "Share your skills!", "Continue learning", "Home", "My account", and "Log out".

The "My Account" section shows the user's details: "Your username is: mysql" and "Your email is: mysql@normal-user.net". There is a form to update the email, with an "Update email" button.

The system tray at the bottom shows weather (31°C Haze), system icons (Windows, Search, File Explorer, etc.), and system status (ENG IN, 01-03-2025).

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Expired license)

Player | || | ⌂ | 1 2 3 4 | 🔍 | 🔍

Lab: Brute-forcing a stay-logged-in cookie | My Account - PortSwigger | +

https://0a4d00de0430f3528319aff500ac003a.web-security-academy.net/my-account?id=wiener

Burp Project Dashboard 1 x 2 Positions Payloads Payloads This pay... P... L... Re... C... Deda... Add fi... Event log (1)

Web Security Academy  Brute-forcing a stay-logged-in cookie

Back to lab description >

LAB Solved 

Congratulations, you solved the lab!

Share your skills!   Continue learning >

Home | My account | Log out

My Account

Your username is: wiener

Email

Update email



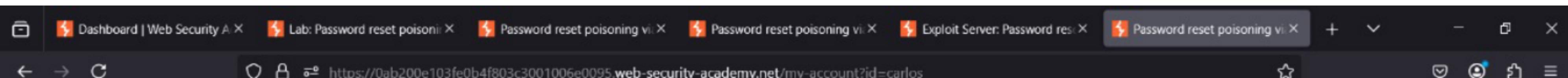
9+ Gold -0.78%  Search              ENG IN 28-02-2025 14:22

Screenshot of a web browser showing a solved lab on the Web Security Academy platform.

The browser tabs show multiple instances of "Offline password cracking". The active tab is titled "Offline password cracking" and has the URL <https://0a8a007c03e363da808c0d2000a90086.web-security-academy.net>.

The page content includes:

- WebSecurity Academy** logo with a red lightning bolt icon.
- Offline password cracking** heading.
- Back to lab description >>** link.
- LAB Solved** button with a green checkmark icon.
- Congratulations, you solved the lab!** message.
- Share your skills!** button with icons for Twitter and LinkedIn.
- Continue learning >>** link.
- WE LIKE TO BLOG** section with a purple graphic.
- A photograph of four people (three men and one woman) with white duct tape over their mouths, standing in front of a background filled with colorful balloons.
- Bottom navigation bar with various application icons (Nifty bank, Search, File Explorer, Edge, etc.) and system status indicators (ENG IN, 27-02-2025, 13:09).



Password reset poisoning via middleware

[Back to lab description >>](#)

LAB Solved



Congratulations, you solved the lab!

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

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

My Account

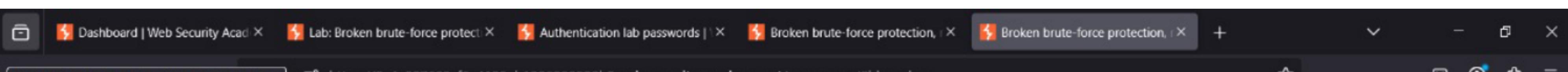
Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

[Update email](#)





Broken brute-force protection, multiple credentials per request

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: carlos

Email

[Update email](#)



Lab: Broken brute-force protect | X Authentication lab passwords | X Broken brute-force protection, | X Broken brute-force protection, | X

View recent browsing across windows and devices

https://0a3b00f7032d612a809af3cb00210049.web-security-academy.net/my-account?id=carlos

WebSecurity Academy  Broken brute-force protection, IP block

Back to lab description » LAB Solved 

Congratulations, you solved the lab!

Share your skills!   Continue learning »

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

My Account

Your username is: carlos

Email

Update email

Dashboard | Web Security Acad X Lab: Password brute-force via p... Authentication lab passwords | X Password brute-force via passw... +

https://0a1e00a60303815a803f49ea00da002a.web-security-academy.net/my-account?id=carlos

WebSecurity Academy Password brute-force via password change

Back to lab description >

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account | Log out

My Account

Your username is: carlos

Email

Update email

Current password

New password

Confirm new password

Trending videos Dog gets head s... ENG IN 27-02-2025 11:25

A screenshot of a web browser window. The address bar shows the URL: <https://0aaf007f035464af807117fd0072007e.web-security-academy.net/my-account?id=announcements>. The page content is from 'Web Security Academy' and displays the title 'Username enumeration via subtly different responses'. A green button labeled 'LAB Solved' with a checkmark icon is visible. The browser's tab bar shows multiple tabs related to the lab.

Congratulations, you solved the lab!

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

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

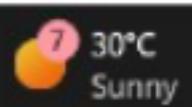
My Account

Your username is: announcements

Your email is: announcements@normal-user.net

Email

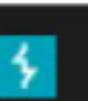
[Update email](#)



30°C
Sunny



Search



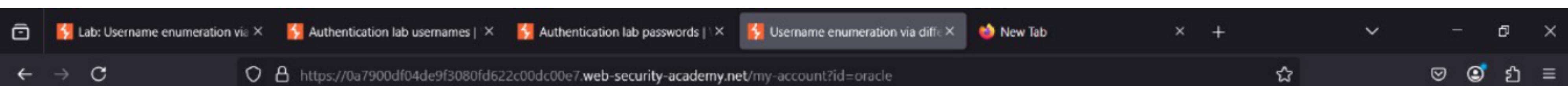
ENG
IN



26-02-2025



12:36



Username enumeration via different responses

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >>

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

My Account

Your username is: oracle

Your email is: oracle@normal-user.net

Email

user

[Update email](#)

25°C
Haze



ENG IN 25-02-2025 10:52

Screenshot of a web browser showing a solved lab on the Web Security Academy platform.

The browser window title is "Lab: Password reset broken logic". The URL in the address bar is "https://0a3e002403de3a3f966f95fa00fc00dd.web-security-academy.net/my-account?id=carlos".

The page header includes the "Web Security Academy" logo, the title "Password reset broken logic", and a "Solved" badge with a green border and a person icon.

A banner at the top of the page says "Congratulations, you solved the lab!" and includes links for "Share your skills!" (with Twitter and LinkedIn icons), "Continue learning >", "Home", "My account", and "Log out".

My Account

Your username is: carlos
Your email is: carlos@carlos-montoya.net

Email:
[Update email](#)

The taskbar at the bottom of the screen shows various application icons and system status indicators, including weather (23°C Haze), search, file explorer, and network status.

A screenshot of a web browser window. The address bar shows the URL: <https://0ad6000c04f4b86280eff89400440029.web-security-academy.net/my-account?id=carlos>. The page title is "2FA simple bypass". The main content area displays the "Web Security Academy" logo and the text "2FA simple bypass". A green button labeled "LAB Solved" with a checkmark icon is visible. Below the logo, there is a link "Back to lab description >". The message "Congratulations, you solved the lab!" is prominently displayed in white text on an orange background. To the right, there are links for "Share your skills!" (with icons for Twitter and LinkedIn), "Continue learning >", and "Home | My account | Log out". At the bottom of the browser window, the taskbar shows various pinned icons and the system tray indicates it's 25-02-2025 at 19:43, with a weather forecast of 27°C and partly cloudy conditions.

Screenshot of a web browser showing a solved lab page on the Web Security Academy platform.

The browser tabs show multiple instances of "2FA broken logic" and "Exploit Server: 2FA broken logic".

The main content area displays:

- WebSecurity Academy** logo and "2FA broken logic" title.
- A green button labeled "LAB Solved" with a trophy icon.
- A message: "Congratulations, you solved the lab!"
- Links: "Share your skills!" (with Twitter and LinkedIn icons), "Continue learning >>".
- A "Home | My account" link.
- A form field placeholder: "Please enter your 4-digit security code" with a corresponding input field.
- A blue "Login" button.

The taskbar at the bottom shows various application icons and system status indicators, including:

- Air: Moderate Now
- Search bar
- File Explorer
- PowerShell
- Microsoft Edge
- OneDrive
- Windows File Explorer
- Task View
- File History
- Windows Update
- System
- Network
- Taskbar icons for Mail, Photos, and Settings
- Language: ENG IN
- Wi-Fi signal
- Battery level
- Date and time: 01-03-2025

Screenshot of a web browser showing a solved lab on the Web Security Academy platform.

The browser tabs show completed labs: "Lab: Username enumeration via account lock", "Username enumeration via account lock", "Username enumeration via account lock", "Authentication lab usernames", and "Authentication lab passwords".

The address bar shows the URL: <https://0a3a001803c899b185cb0d5d00d000fa.web-security-academy.net/login>.

The main content area displays the "Web Security Academy" logo and the title "Username enumeration via account lock". A green button indicates the task is "Solved".

A banner at the bottom says "Congratulations, you solved the lab!" and provides 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: mysql" and "Your email is: mysql@normal-user.net". There is a form to update the email, with an "Update email" button.

The system tray at the bottom shows weather (31°C Haze), system icons (Windows, Search, File Explorer, etc.), and system status (ENG IN, 01-03-2025).

Screenshot of a web browser showing a solved lab on the Web Security Academy platform.

The browser tabs show:

- Lab: CSRF vulnerability with no defenses
- CSRF vulnerability with no defer
- Exploit Server: CSRF vulnerability

The address bar shows the URL: <https://exploit-0a51006f04817c0c80100c1201c7005a.exploit-server.net>.

The page content includes:

- Web Security Academy** logo
- CSRF vulnerability with no defenses
- [Back to lab description >>](#)
- LAB Solved** badge
- Congratulations, you solved the lab!
- Share your skills! (Twitter, LinkedIn)
- Continue learning >>
- Home | My account | Log out

The Windows taskbar at the bottom shows various pinned icons and the date/time: 01-03-2025 14:56.