

User ID controlled by request parameter with data leakage in redirect

LAB Solved

[Back to lab description >>](#)

Congratulations, you solved the lab!

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

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

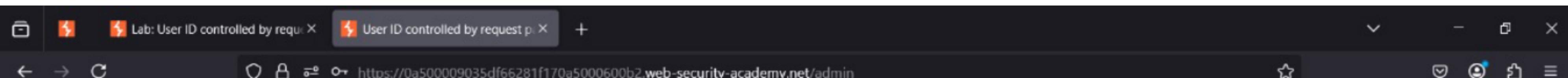
Login

Username

Password

[Log in](#)





User ID controlled by request parameter with password disclosure

[Back to lab description >](#)

LAB Solved

Congratulations, you solved the lab!

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

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

User deleted successfully!

Users

wiener - [Delete](#)

The screenshot shows the Firefox Developer Tools Inspector tab. The DOM tree on the left displays the HTML structure of the page, including scripts and a 'body' element. The right side shows the CSS Styles panel for the 'body' element, with properties like background-color (#fff), color (#333332), font-size (16px), and font-family ('Arial', 'Helvetica Neue', 'Helvetica', 'sans-serif'). The 'Computed' tab in the sidebar is selected. The status bar at the bottom shows system information and the date/time.

```
<!DOCTYPE html>
<html> (scroll)
  <head> (empty) </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js"></script>
    <div id="academyLabHeader"> (empty) </div>
    <section id="notification-labsolved" class="notification-labsolved"> (empty) </section>
    <script src="/resources/labheader/js/completedLabHeader.js"></script>
    <div theme=""> (empty) </div>
  </body>
</html>
```

html > body

Watchlist +0.91%

23:19 05-03-2025

A screenshot of a web browser window. The address bar shows the URL: <https://0ad00020048c22a181225c5f001b008d.web-security-academy.net/my-account?id=carlos>. The page content is from 'Web Security Academy' and displays the message 'Insecure direct object references'. A green button labeled 'LAB Solved' with a checkmark icon is visible. The browser interface includes standard navigation buttons and a toolbar.

Congratulations, you solved the lab!

Share your skills! Continue learning >

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

My Account

Your username is: carlos

Email

[Update email](#)



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

The browser tabs show three instances of the same lab: "Lab: User role can be modified in user profile".

The address bar shows the URL: <https://0ae500d5043a82bf81a93408001e00ec.web-security-academy.net/admin>

The main content area displays the title "User role can be modified in user profile" and a "Solved" badge with a checkmark icon.

A banner at the bottom says "Congratulations, you solved the lab!" and includes links for "Share your skills!" (Twitter and LinkedIn), "Continue learning >>", and navigation links "Home | Admin panel | My account".

A message "User deleted successfully!" is displayed.

The page title is "Users".

The Windows taskbar at the bottom shows the date "05-03-2025" and time "20:19".

A screenshot of a web browser window. The title bar shows three tabs: "Lab: HTTP/2 request splitting via CRLF", "HTTP/2 request splitting via CRLF", and "My Account - PortSwigger". The main content area displays the "Web Security Academy" logo and the title "HTTP/2 request splitting via CRLF injection". A green button indicates the task is "Solved". Below this, a message says "Congratulations, you solved the lab!" and "User deleted successfully!". The page footer includes links for "Share your skills!", "Home", "Admin panel", and "My account". The system tray at the bottom shows the date as 07-03-2025, the time as 11:12, and various system icons.

Lab: URL-based access control

URL-based access control can be circumvented

Back to lab description >

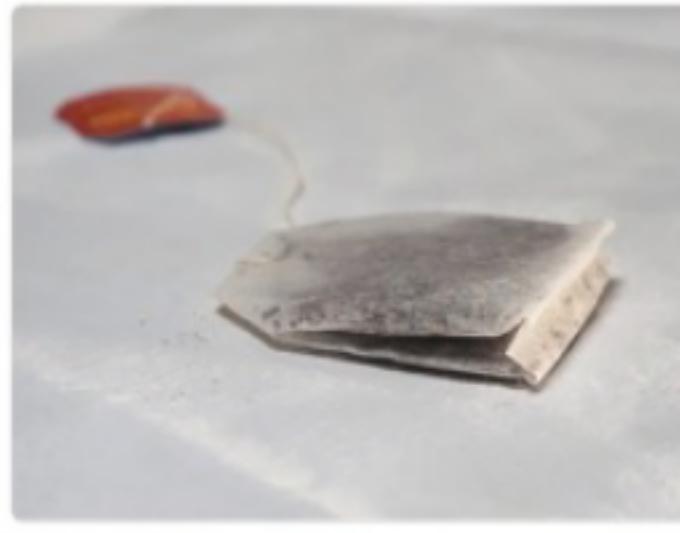
LAB Solved

Congratulations, you solved the lab!

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

Home | Admin panel | My account

WE LIKE TO SHOP 

 Pest Control Umbrella ★★★★★ \$97.69	 Waterproof Tea Bags ★★★★★ \$42.03	 Folding Gadgets ★★★★★ \$13.65	 Eco Boat ★★★★★ \$79.07
--	---	---	--

View details View details View details View details

24°C Haze

Search    Search         ENG IN 05-03-2025 23:48

A screenshot of a web browser window. The address bar shows the URL: <https://0ac0006b03416c2a82dc0c5c00170097.web-security-academy.net/admin-802qst>. The page title is "Unprotected admin functionality with unpredictable URL". The "Web Security Academy" logo is on the left. A green button at the top right says "LAB Solved" with a checkmark icon. Below the title, there's a link "Back to lab description >".

Congratulations, you solved the lab!

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

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

User deleted successfully!

Users

wiener - [Delete](#)



Solved

User ID controlled by request parameter, with unpredictable user IDs

Back to lab description >

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account | Log out

My Account

Your username is: carlos

Your API Key is: [JykIkRpK9diMR4zTPhMFc4wRfxATpxaA](#)

Email

Update email

32°C Mostly clear

Search

05-03-2025

Lab: Referer-based access control X Referer-based access control X +

https://0a84005c040ce233c85d37fe00ff00e2.web-security-academy.net

Web Security Academy Referer-based access control LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | My account

WE LIKE TO SHOP

Conversation Controlling Lemon: ★★★★☆ \$55.58

Hexbug Battleground Tarantula Double Pack: ★★★★☆ \$49.71

Cheshire Cat Grin: ★★★★★ \$34.74

Lightbulb Moments: ★★★★☆ \$83.50

View details View details View details View details

20°C Clear Search ENG IN 06-03-2025 22:52

A screenshot of a web browser window. The address bar shows the URL: <https://0ae9007603e9bb498082eedd004700f1.web-security-academy.net/admin>. The page title is "User role controlled by request parameter". A green button at the top right says "LAB Solved" with a checkmark icon. The main content area displays the message "Congratulations, you solved the lab!" and a "Share your skills!" button with social media icons for Twitter and LinkedIn.

Congratulations, you solved the lab!

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

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

User deleted successfully!

Users

wiener - [Delete](#)

A screenshot of the Microsoft Edge DevTools Style Editor. The left sidebar shows two CSS files: "academyLabHeader.css" (31 rules) and "labs.css" (252 rules). The main pane displays the following CSS code:

```
1 #academyLabHeader {  
2     all: initial;  
3     --spacing-base: 0.9em;  
4     --heading-line-height: 24px;  
5     font-family: Arial, Helvetica, sans-serif;  
6     font-size: 16px;  
7 }  
8 #academyLabHeader .academyLabBanner {  
9     background: #fff;  
10    color: #333332;  
11    -webkit-font-smoothing: antialiased;  
12    -moz-osx-font-smoothing: grayscale;  
13    line-height: 1.4;  
14    overflow-wrap: break-word;  
15    display: flex;  
16 }
```

The status bar at the bottom shows system information: 28°C Haze, ENG IN, 04-03-2025, and 23:02.

A screenshot of a web browser window. The address bar shows the URL: <https://0a7b00f8049c397f8140f23000a400aa.web-security-academy.net/administrator-panel>. The page title is "Unprotected admin functionality". The page content includes the "Web Security Academy" logo, a "Solved" badge, and a message saying "Congratulations, you solved the lab!". Below this, a success message states "User deleted successfully!". The browser's taskbar at the bottom shows various pinned icons and the system tray indicates it's 22:50 on 04-03-2025.

My Account - PortSwigger X Lab: Unprotected admin functio X Unprotected admin functionalit X +

https://0a7b00f8049c397f8140f23000a400aa.web-security-academy.net/administrator-panel

Web Security Academy Unprotected admin functionality LAB Solved

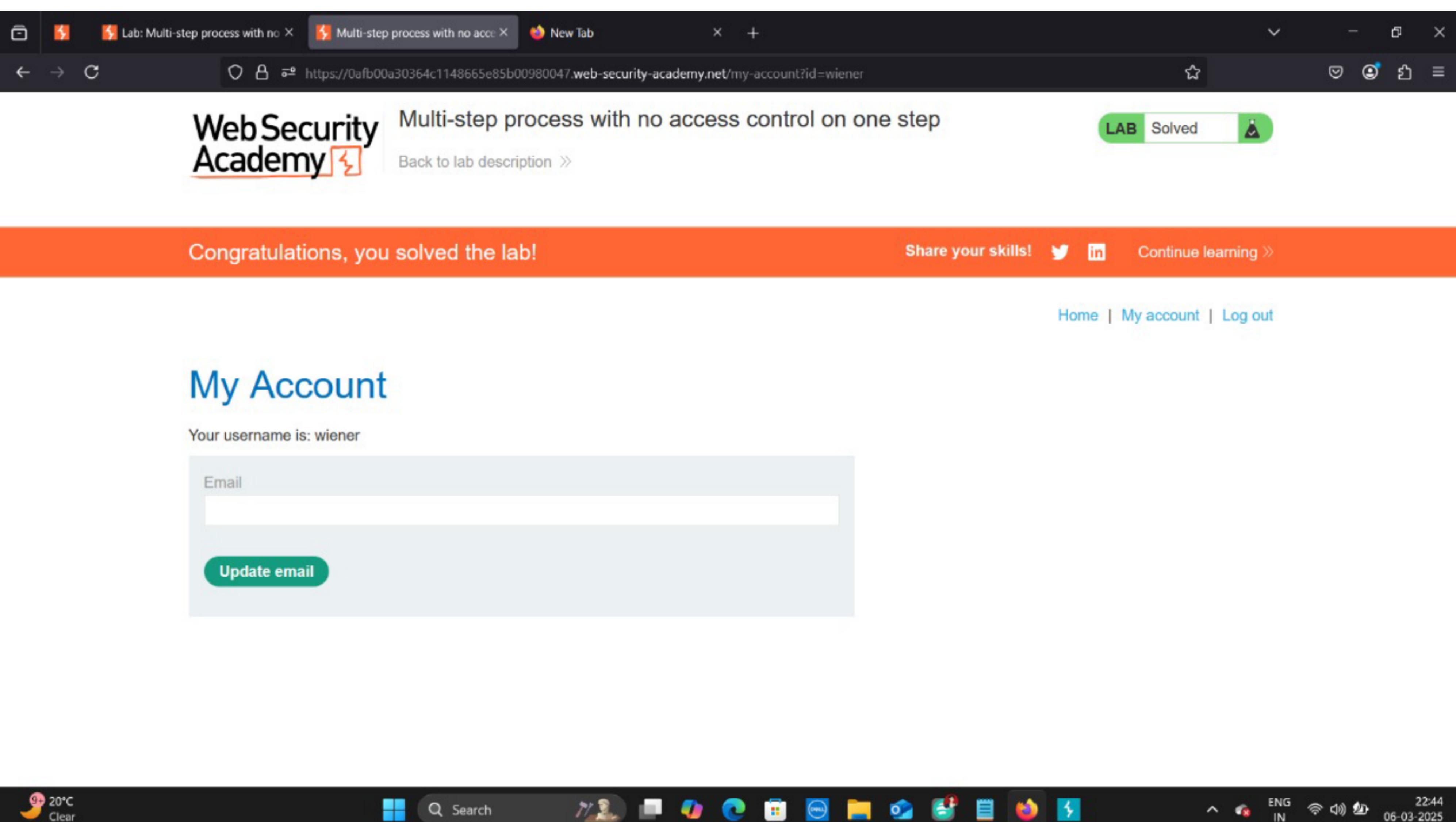
Congratulations, you solved the lab!

User deleted successfully!

Share your skills! Continue learning >

Home | My account

wiener - Delete



Lab: OS command injection, sir X OS command injection, simple X +

https://0a0c00fe0306ba00815c9ed3005a0033.web-security-academy.net/product?productId=1

Web Security Academy OS command injection, simple case LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Home

3D Voice Assistants

★★★★★ \$47.65

19°C Mostly clear

Search

23:00

A screenshot of a web browser window showing a completed lab on the "Web Security Academy" platform.

The browser title bar shows two tabs: "Lab: Exploiting XXE using external entities" and "Exploiting XXE using external entities".

The URL in the address bar is <https://0a25007204288c1a81fa114500b40045.web-security-academy.net/product?productId=1>.

The main content area displays the title "Exploiting XXE using external entities to retrieve files" and a "Solved" badge with a checkmark icon.

An orange banner at the bottom of the page says "Congratulations, you solved the lab!" and includes links for "Share your skills!" (Twitter and LinkedIn icons), "Continue learning >>", and "Home".

The main content section features a product listing for "The Lazy Dog" with a price of \$40.60. It includes a 5-star rating icon and a thumbnail image of a pug dog.

The Windows taskbar at the bottom shows various pinned icons and system status indicators like weather (28°C, sunny), battery level, and system date (07-03-2025).

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

The browser window title is "Method-based access control". The URL in the address bar is <https://0a6c000c03cb47ae87c7e70a005c0003.web-security-academy.net/my-account?id=wiener>.

The page header includes the Web Security Academy logo, the title "Method-based access control can be circumvented", a "Solved" badge, and a "Back to lab description" link.

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

The main content area is titled "My Account" and displays the user's username "wiener". It features a form for updating the email address, with an "Email" input field and a green "Update email" button.

The taskbar at the bottom of the screen shows various application icons and system status indicators, including weather (27°C Haze), search, file explorer, and browser icons.

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

The browser title bar shows two tabs: "Lab: User ID controlled by request" and "User ID controlled by request parameter". The URL in the address bar is <https://0ac6002404443cc080683ab500e4009d.web-security-academy.net/my-account?id=carlos>.

The page header includes the "Web Security Academy" logo, the title "User ID controlled by request parameter", a "Solved" badge, and links for "Back to lab description" and "Share your skills!" (with Twitter and LinkedIn icons).

A prominent orange banner at the bottom of the page congratulates the user: "Congratulations, you solved the lab!" and provides links for "Share your skills!", "Continue learning >>", "Home", "My account", and "Log out".

The main content area is titled "My Account". It displays the user's username ("Your username is: carlos") and API key ("Your API Key is: bPmZhskC843QXH1FL1NvfKf0j7RWOKHF"). There is a form for updating the email address, featuring an "Email" input field, a redacted email value, and a green "Update email" button.

The taskbar at the bottom of the screen shows various pinned application icons, including File Explorer, Edge, Task View, File History, Control Panel, File Cabinet, Task Scheduler, and others. The system tray indicates "Air: Moderate Now", "ENG IN", and the date/time "05-03-2025 20:27".