

Cyber Security and Digital
Forensics Internship

ASSIGNMENT 7
BROKEN ACCESS
CONTROL

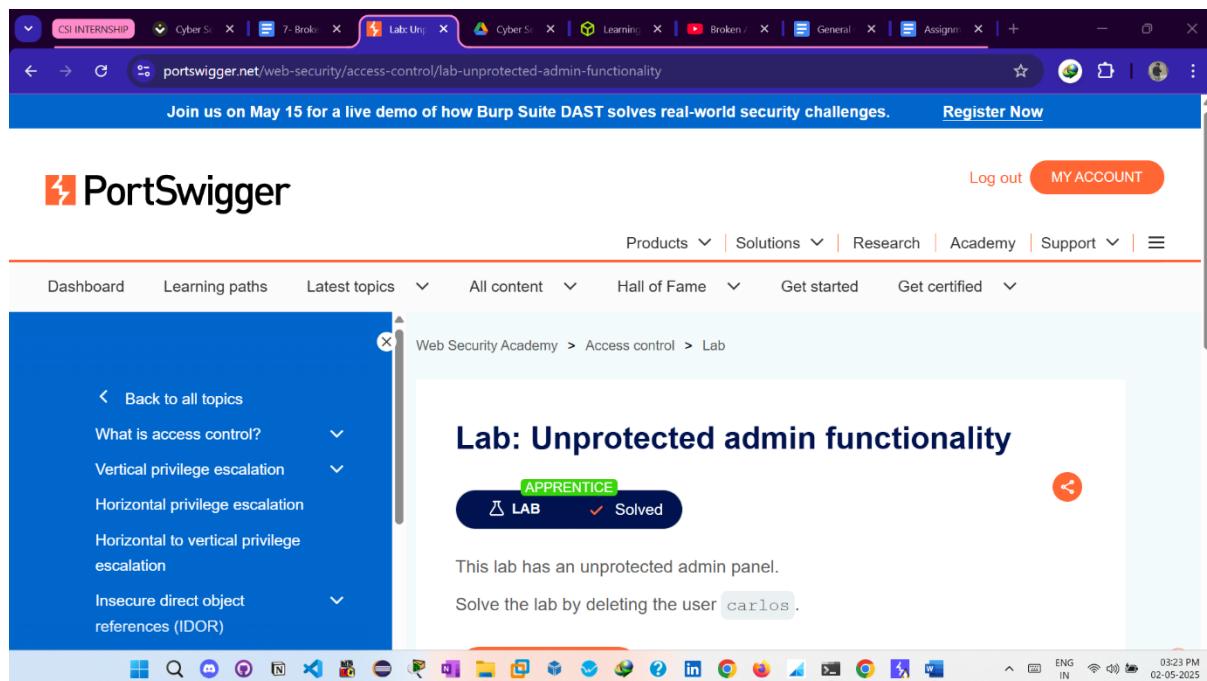
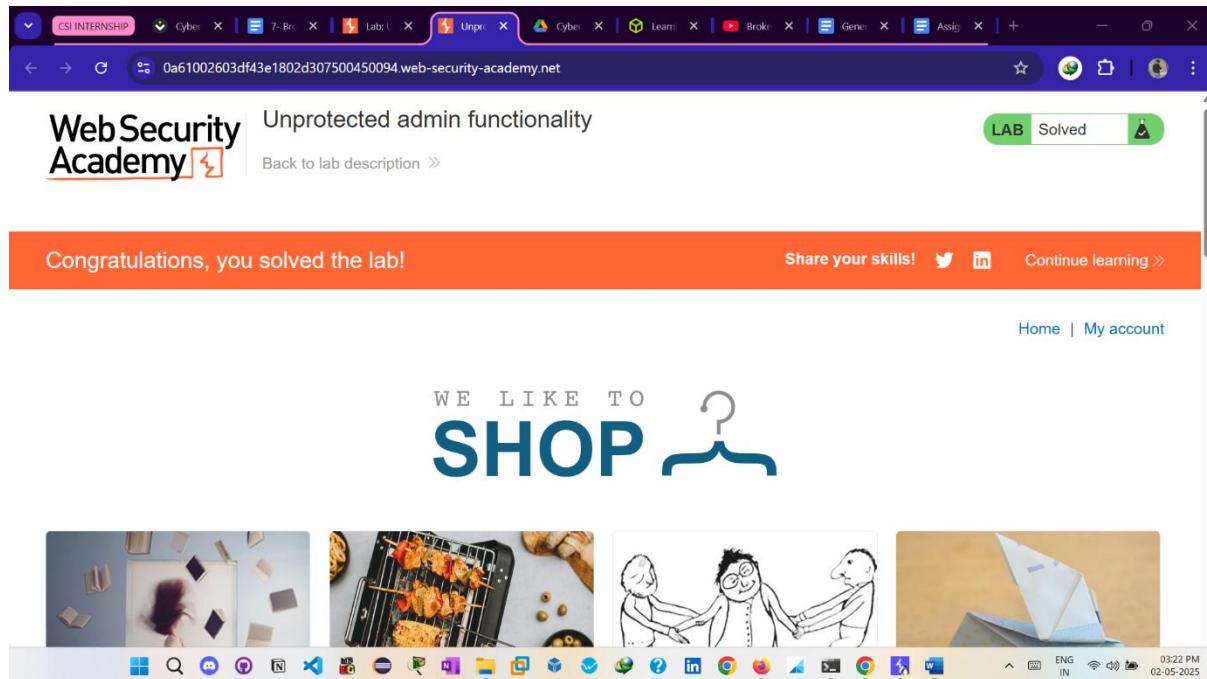
SWASTIK GONDHI

DOON UNIVERSITY

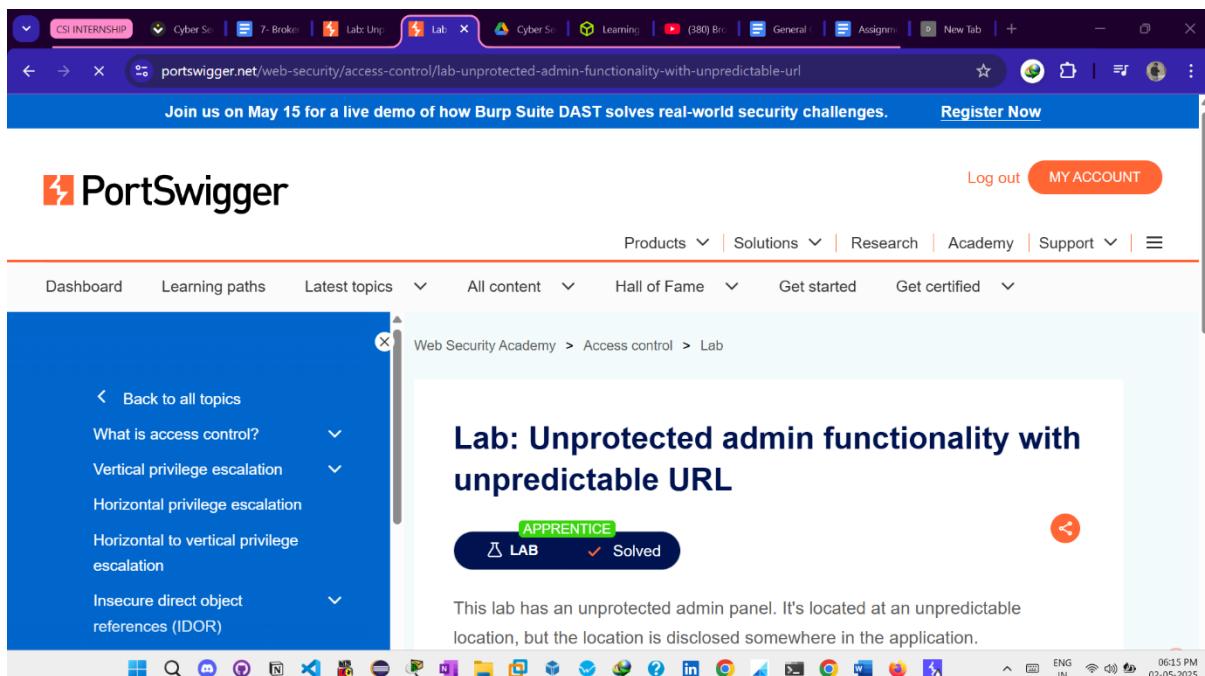
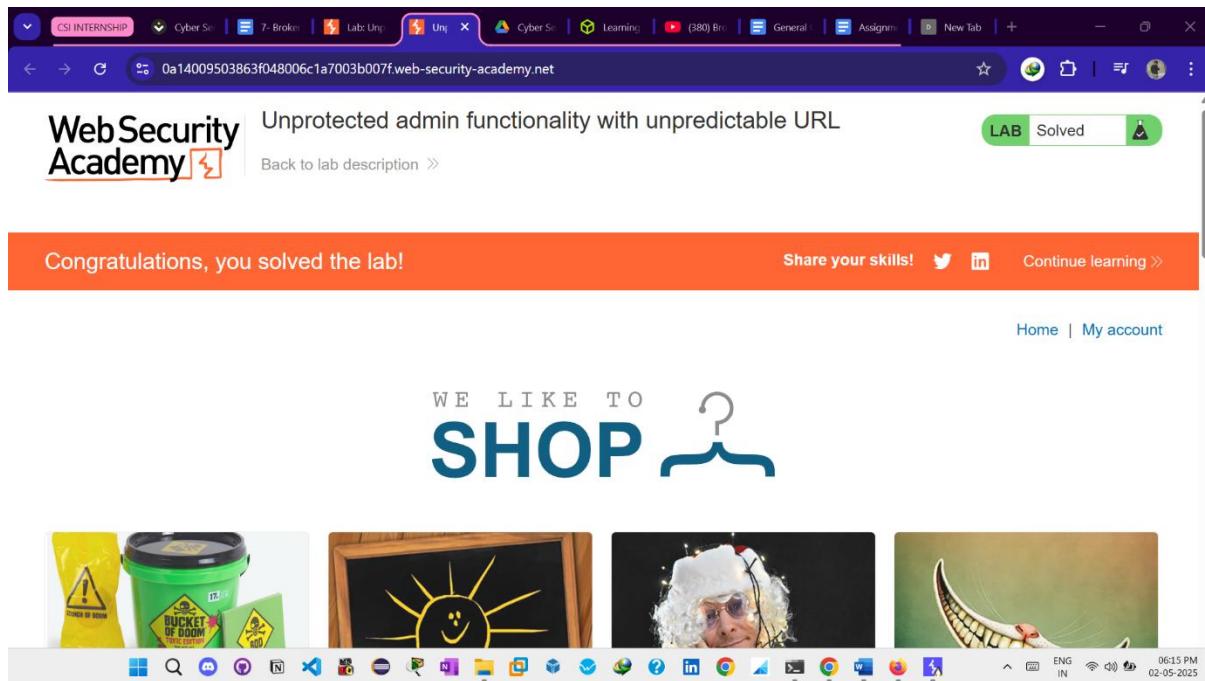
Drive Link -

<https://drive.google.com/drive/folders/1WCK00ki1F3lFPTo7y5tdSmeKcrDeWjvs?usp=sharing>

PORTSWIGGER LAB 1 – Unprotected admin functionality



PORTSWIGGER LAB 2 – Unprotected admin functionality with unpredictable URL

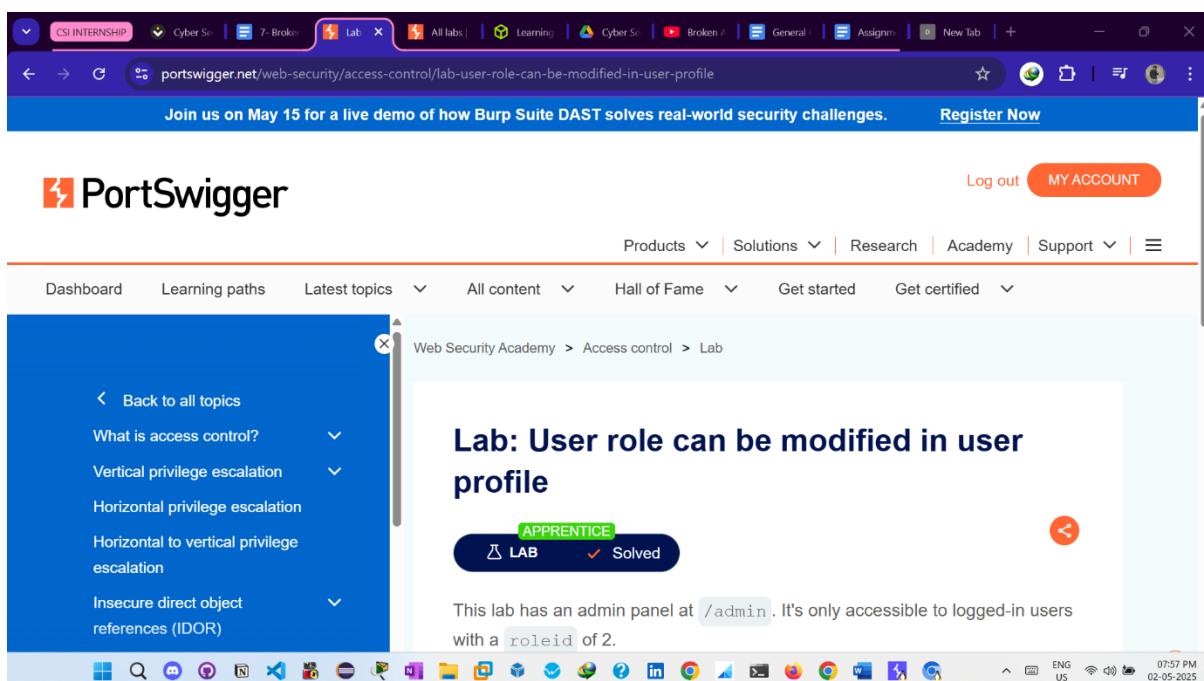
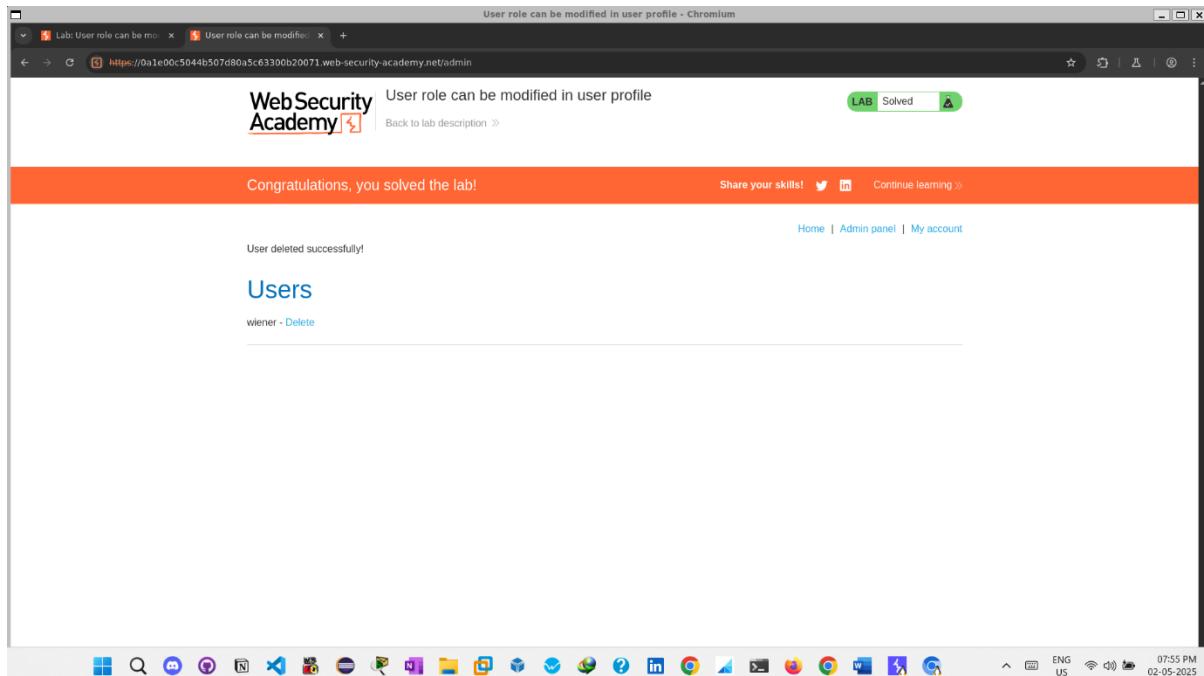


PORTSWIGGER LAB 3 – User role controlled by request parameter

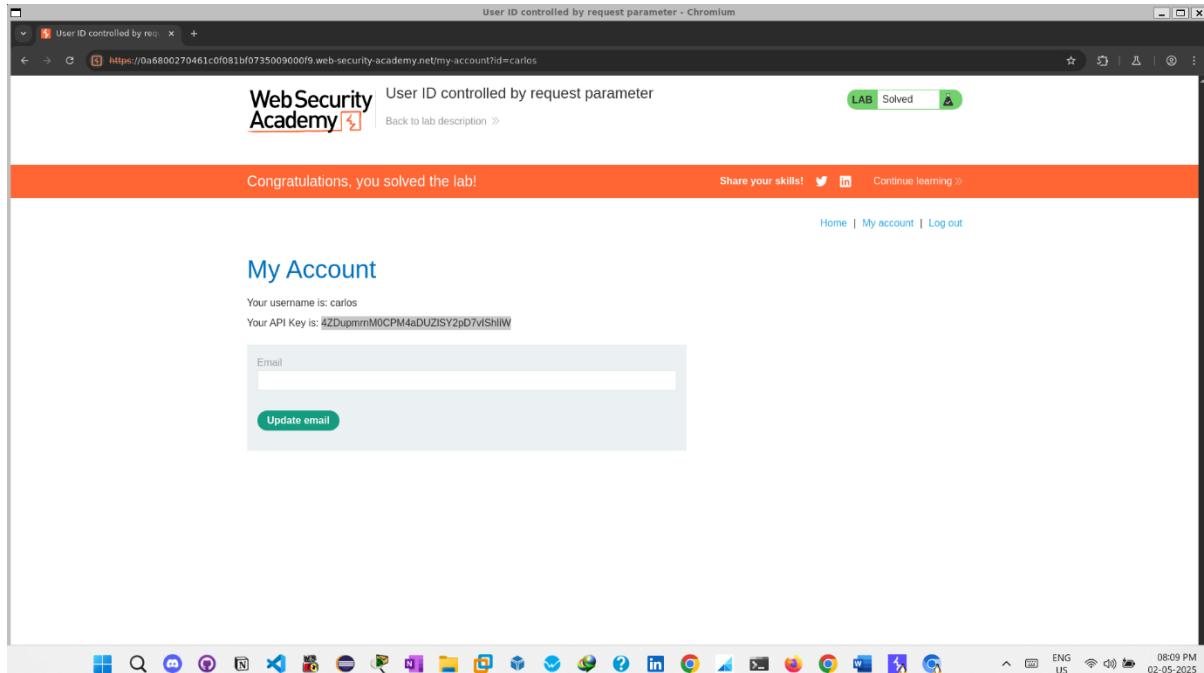
A screenshot of a web browser window. The address bar shows the URL: `oaba0ce04ca1466831ba15500f800c1.web-security-academy.net/admin`. The main content area displays the "WebSecurity Academy" logo and the title "User role controlled by request parameter". A green button labeled "LAB Solved" with a checkmark icon is visible. Below the title, a message says "Congratulations, you solved the lab!". At the bottom of the page, there are links for "Share your skills!" (with Twitter and LinkedIn icons), "Continue learning >", and navigation links for "Home | Admin panel | My account". A success message "User deleted successfully!" is also present.

A screenshot of a web browser window showing the PortSwigger website. The address bar shows the URL: `portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter`. The main content area displays the title "Lab: User role controlled by request parameter". A green button labeled "APPRENTICE" with a "LAB" icon and a "Solved" status is visible. Below the title, a note states: "This lab has an admin panel at `/admin`, which identifies administrators using a forgeable cookie." The browser's taskbar at the bottom shows various open tabs and system status indicators.

PORTSWIGGER LAB 4 – User role can be modified in user profile

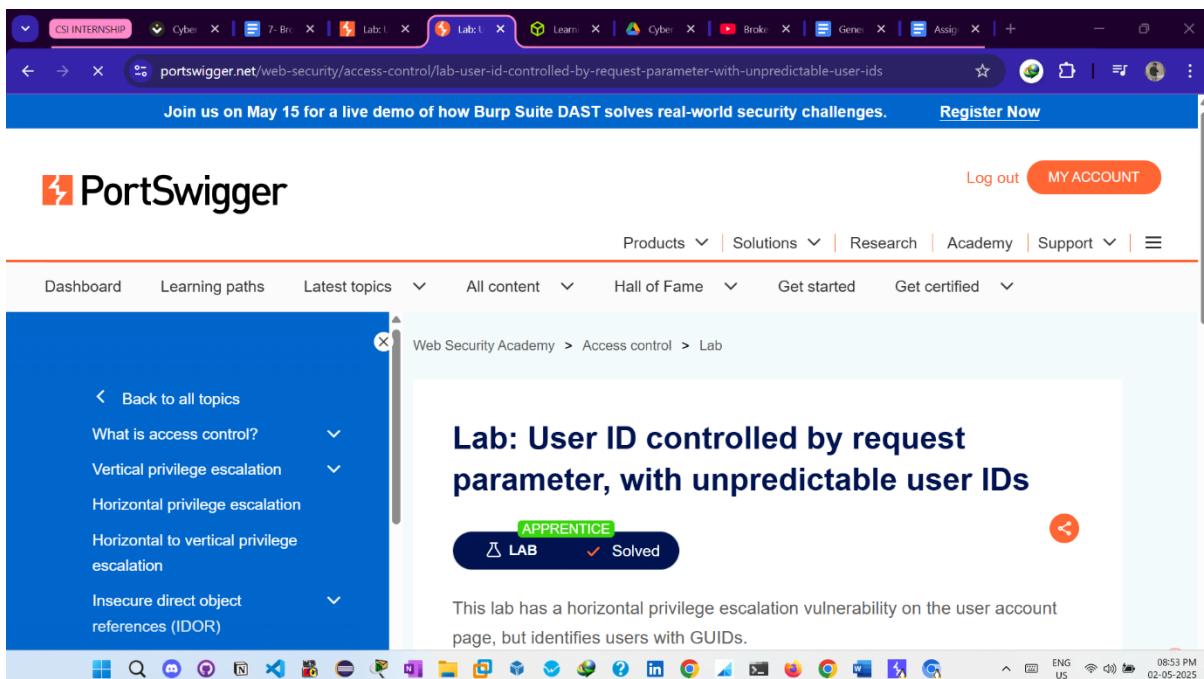
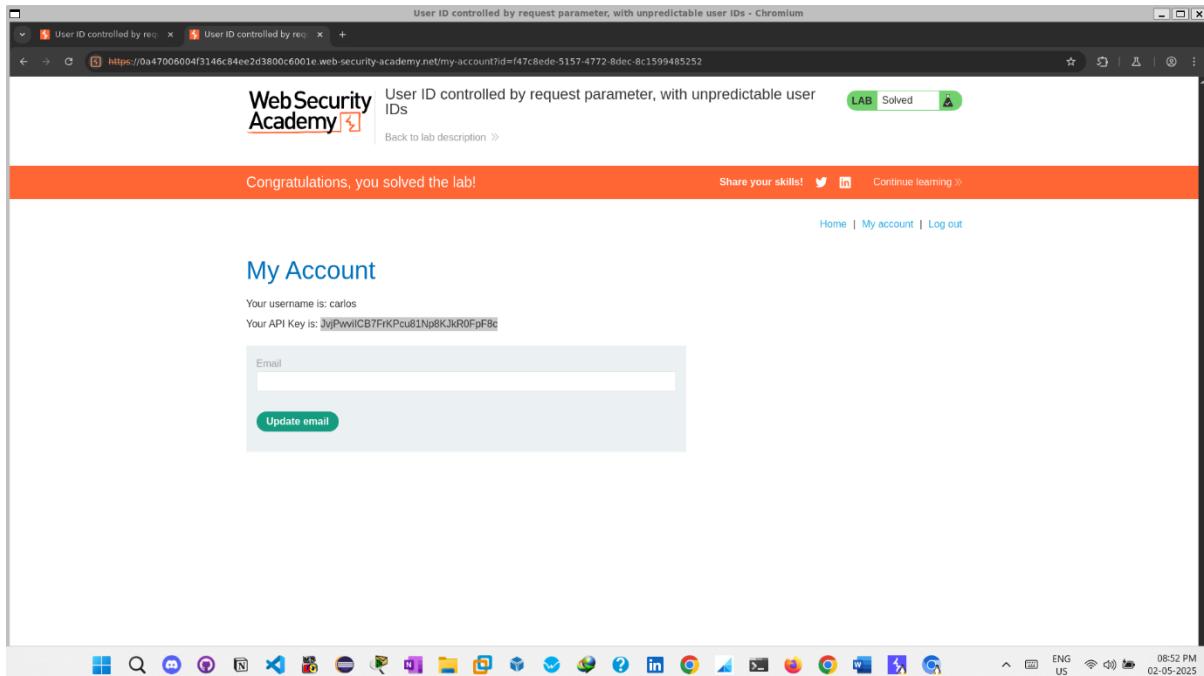


PORTSWIGGER LAB 5 – User ID controlled by request parameter

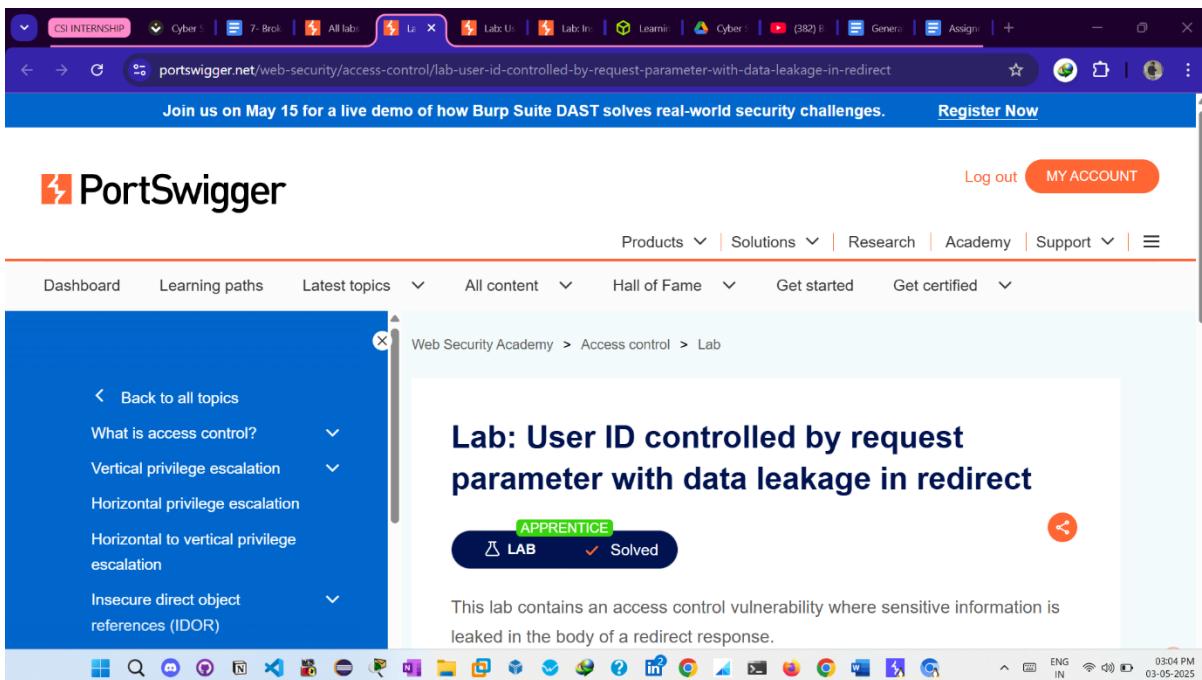
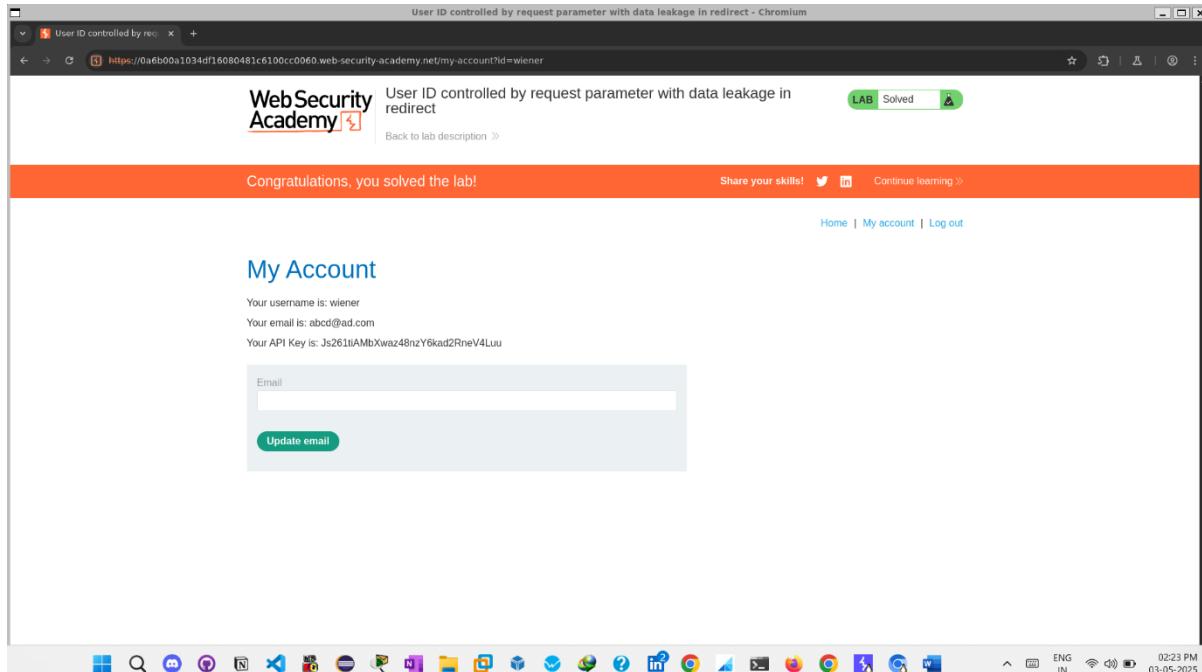


A screenshot of a web browser window showing a PortSwigger lab titled "Lab: User ID controlled by request parameter". The URL is portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter. The page includes a sidebar with navigation links like "Dashboard", "Learning paths", and "Latest topics". The main content area describes the lab as having a horizontal privilege escalation vulnerability on the user account page. A "Solved" badge is visible at the bottom of the page.

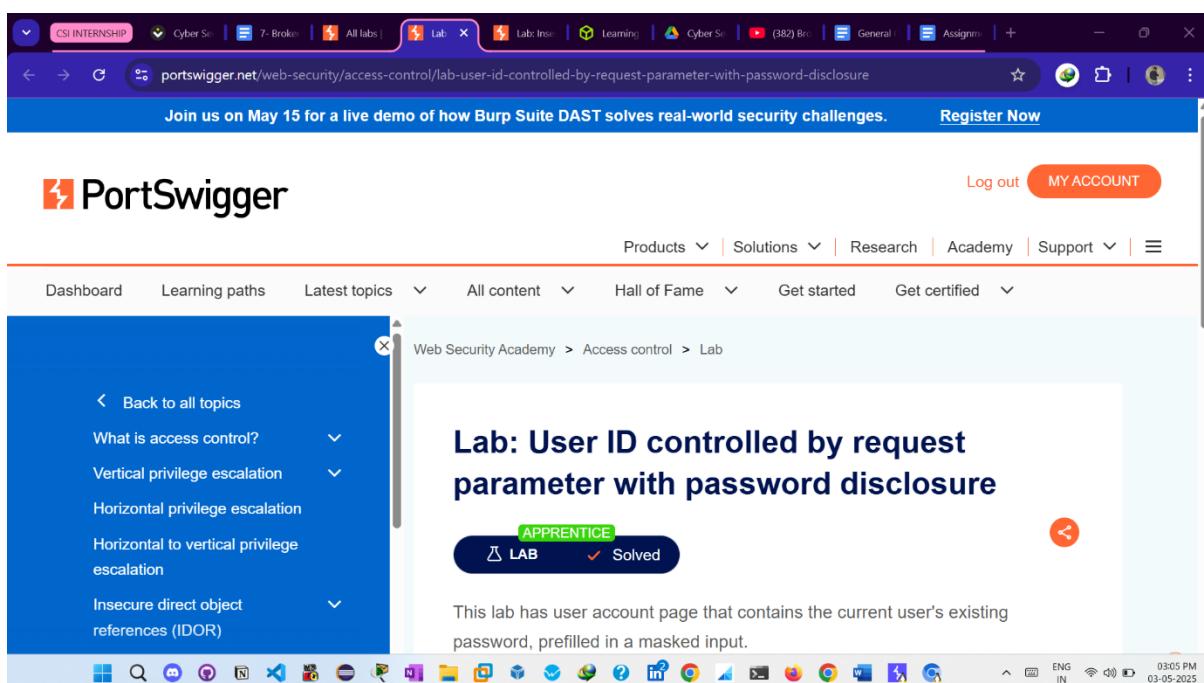
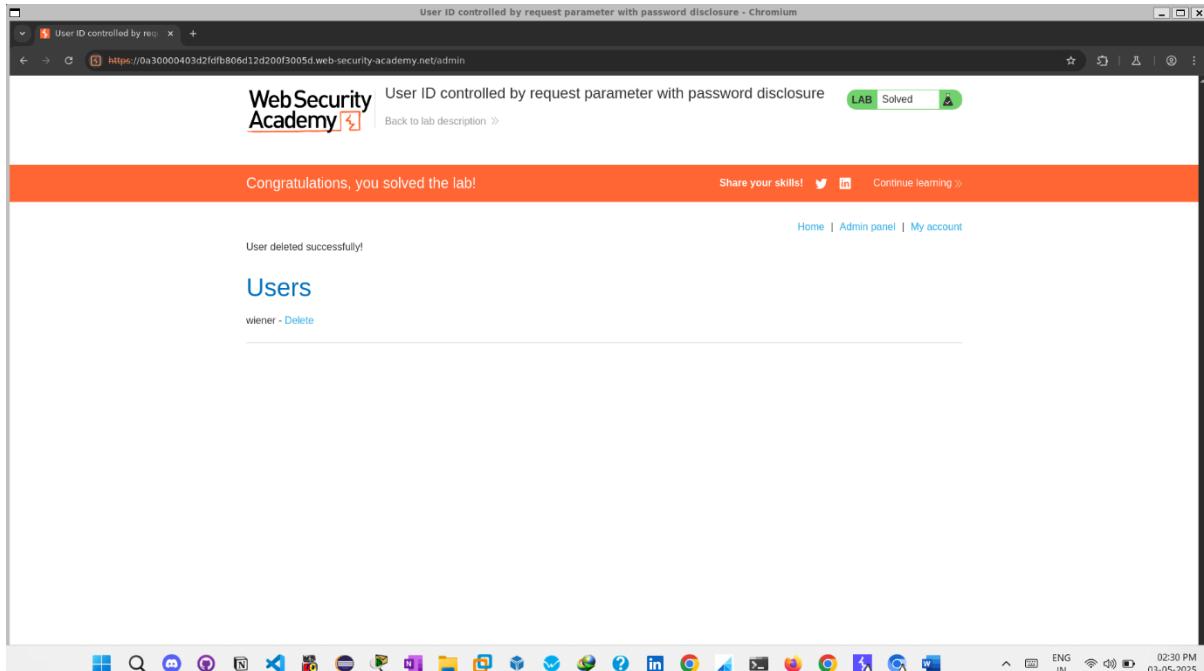
PORTSWIGGER LAB 6 – User ID controlled by request parameter, with unpredictable user IDs



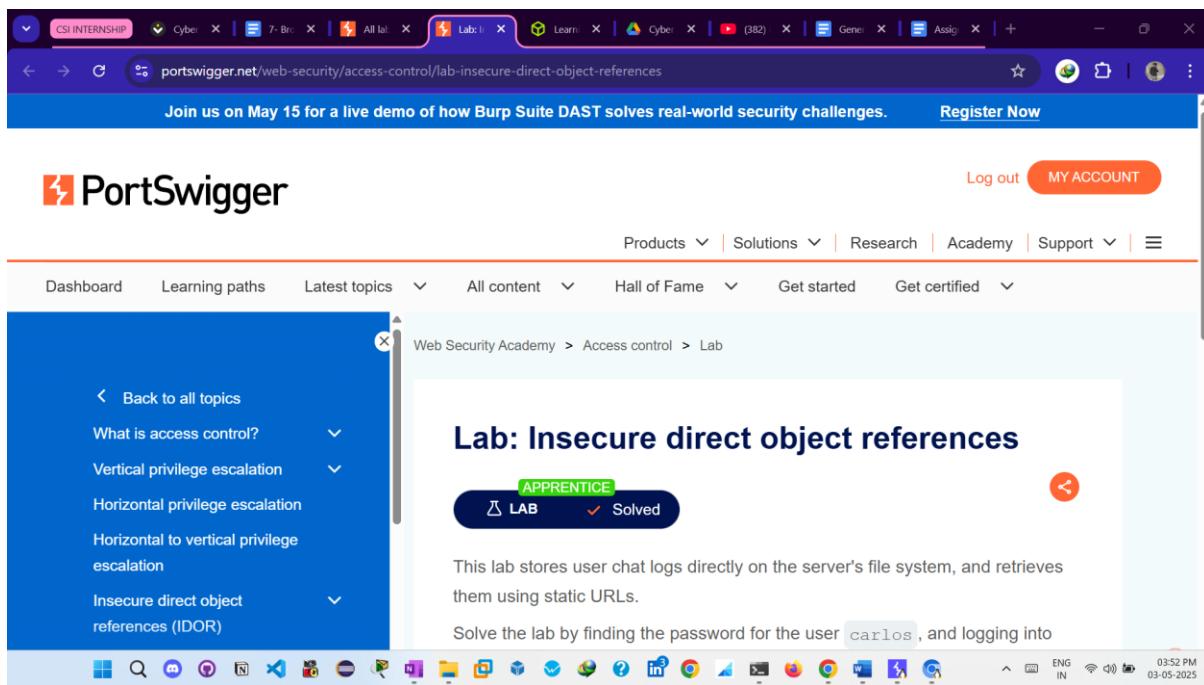
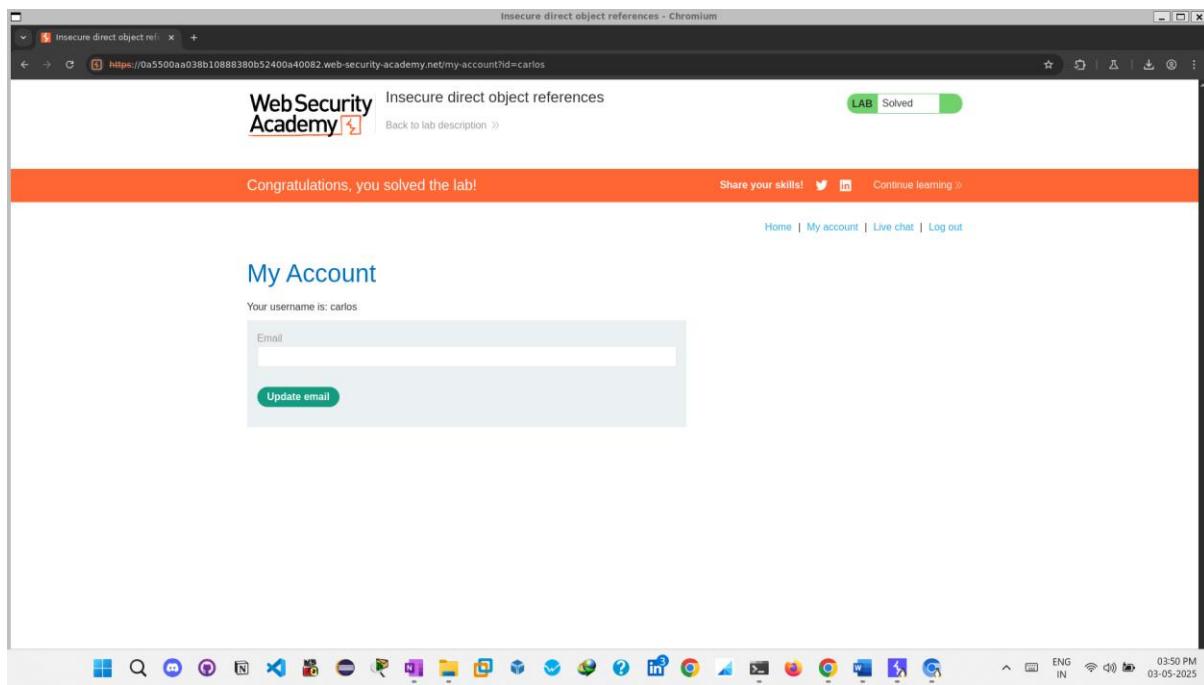
PORTSWIGGER LAB 7 – User ID controlled by request parameter with data leakage in redirect



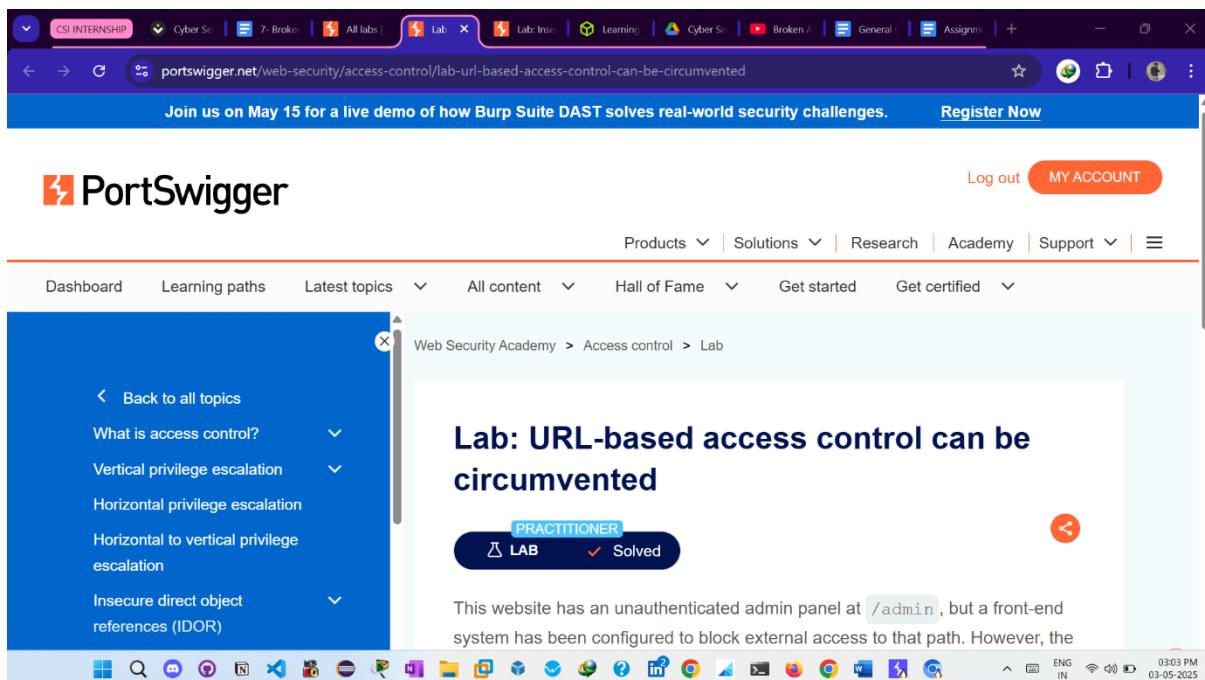
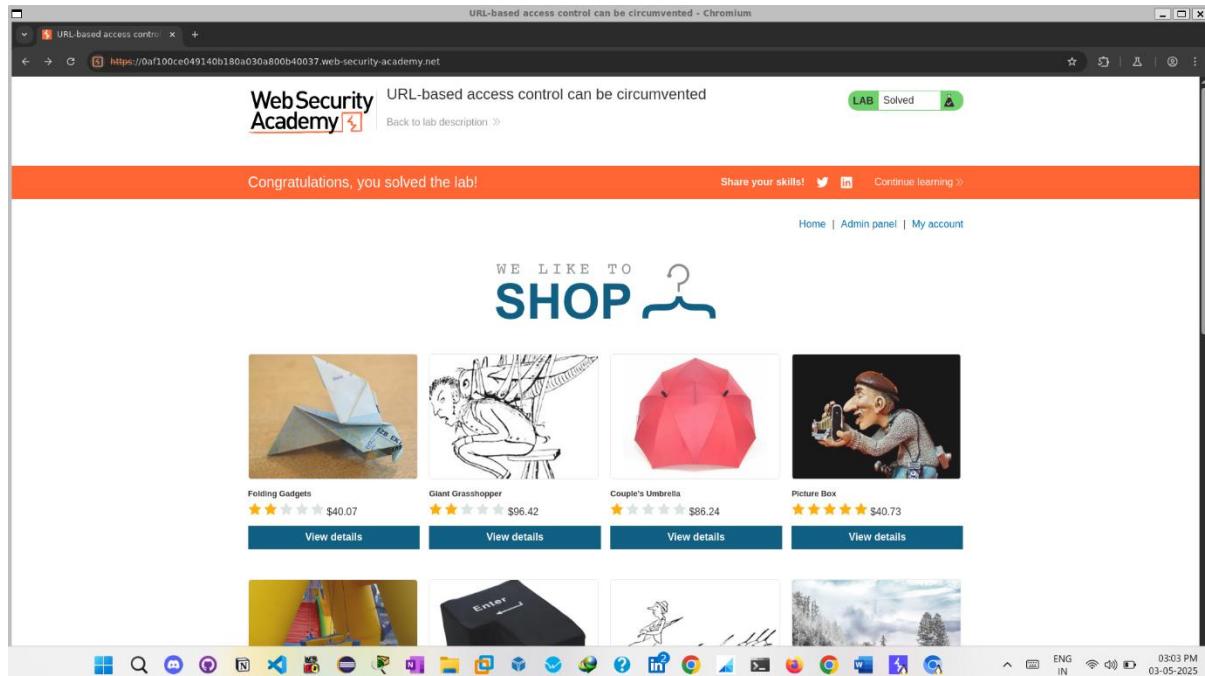
PORTSWIGGER LAB 8 – User ID controlled by request parameter with password disclosure



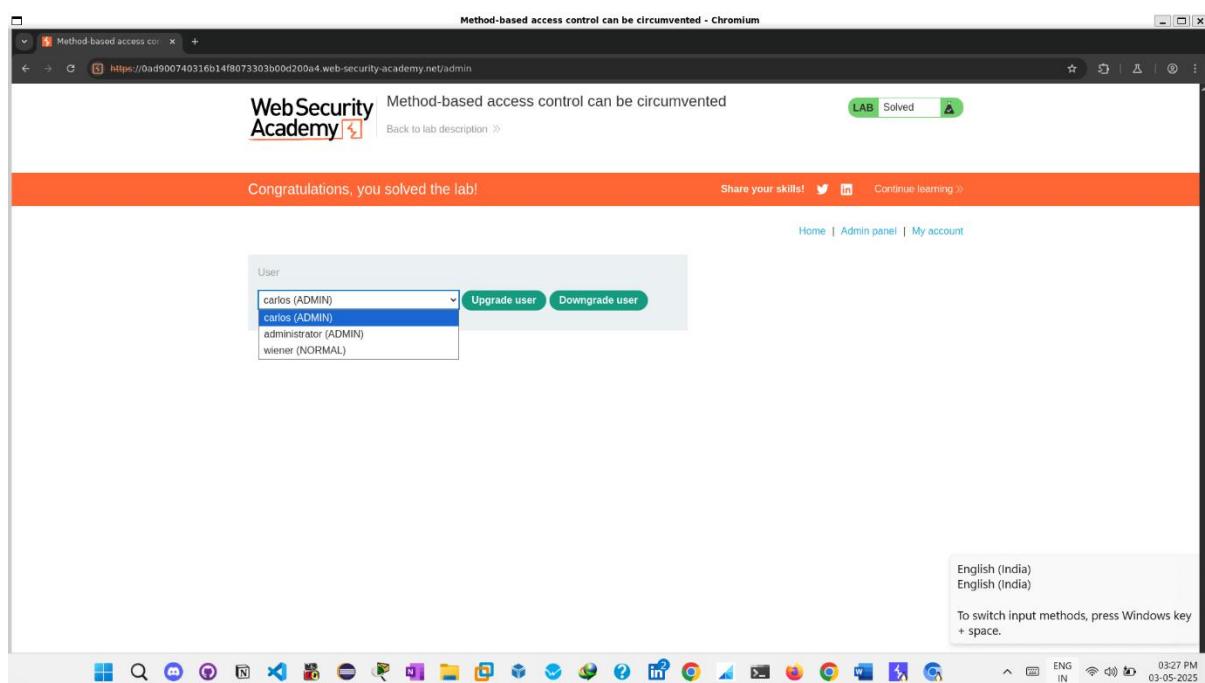
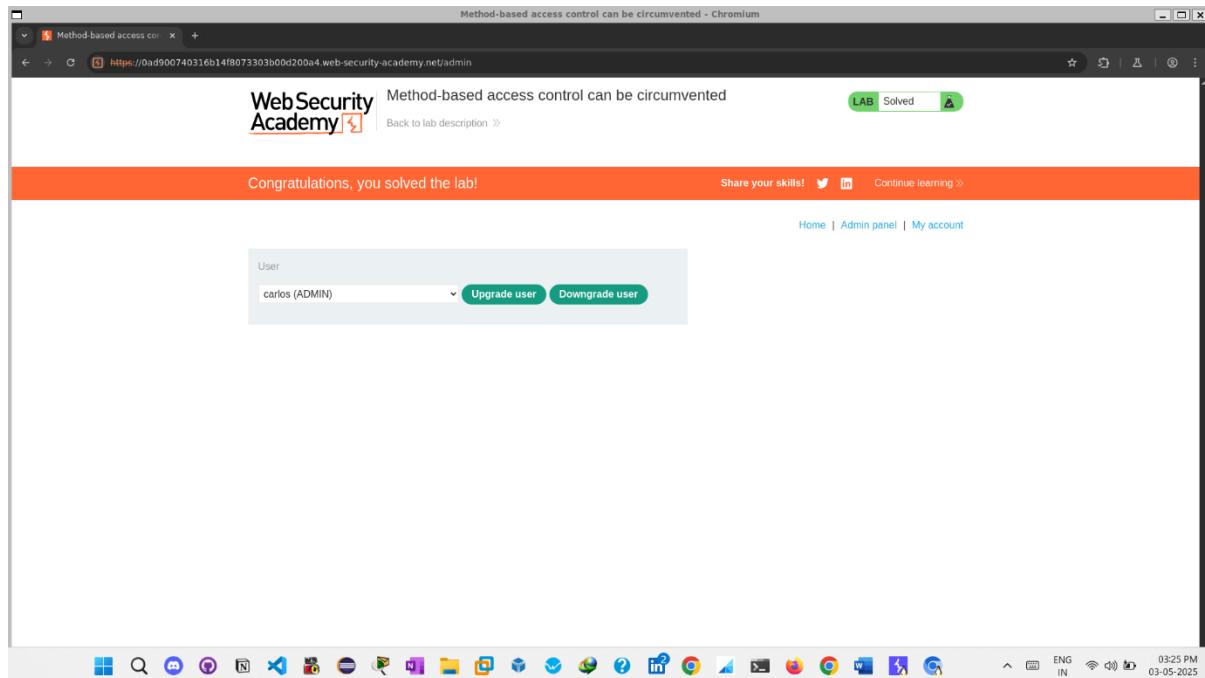
PORTSWIGGER LAB 9 – Insecure direct object references

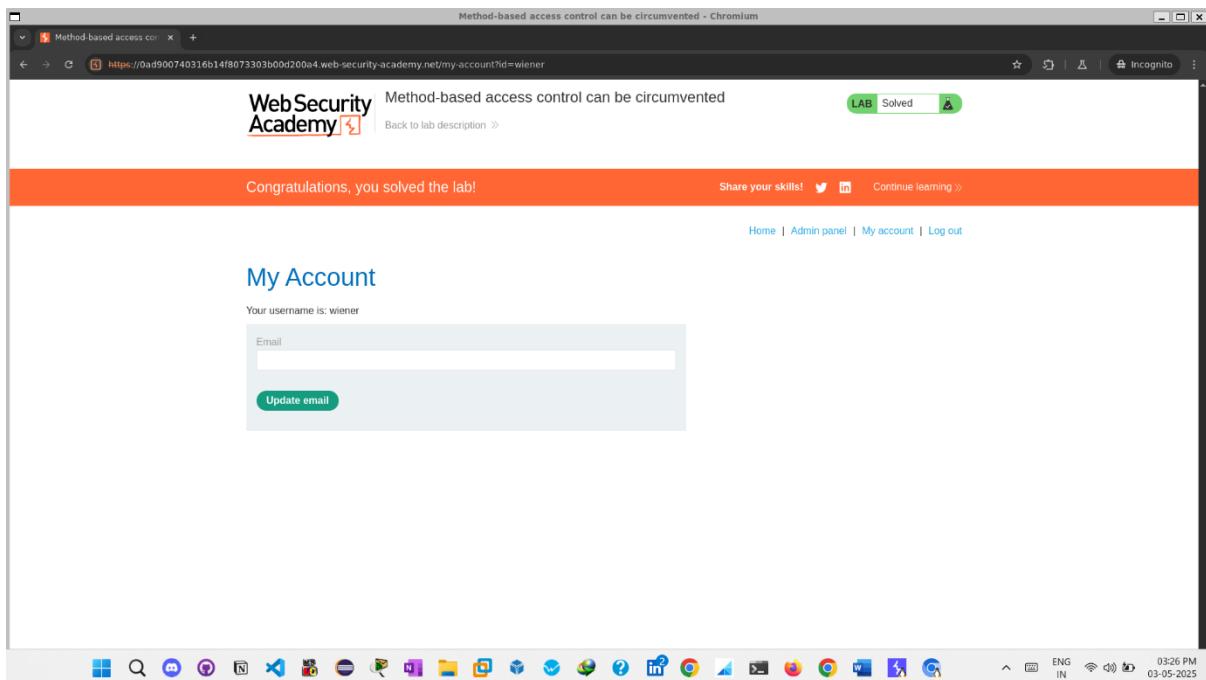


PORTSWIGGER LAB 10 – URL-based access control can be circumvented



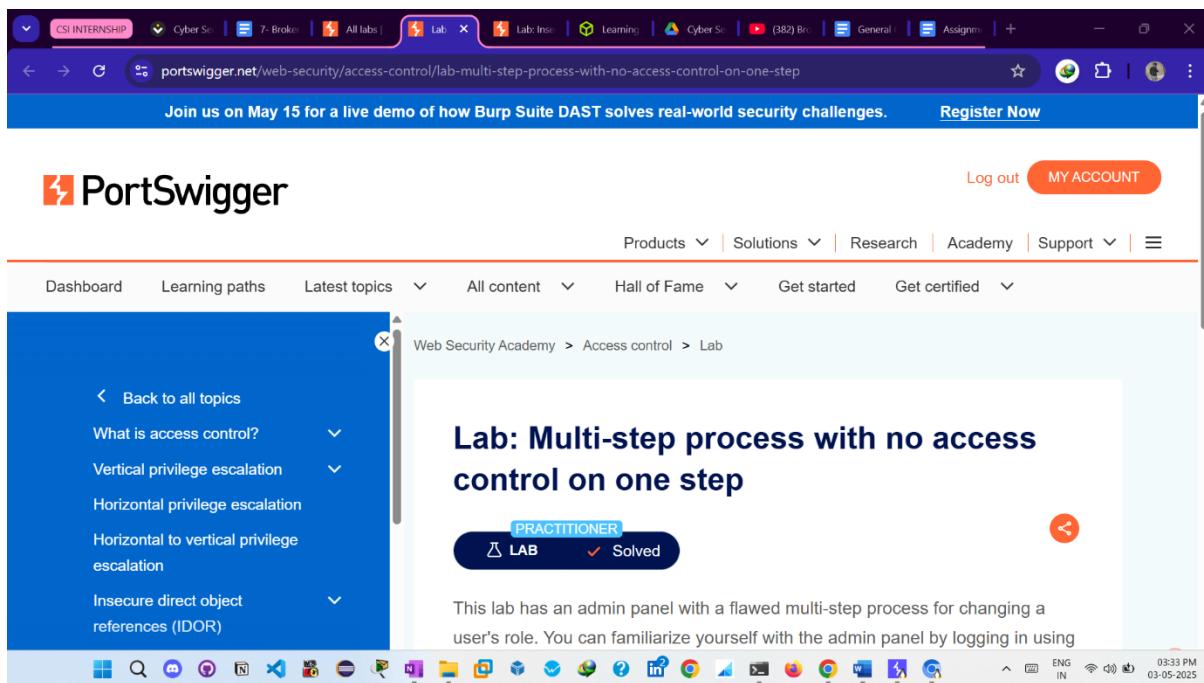
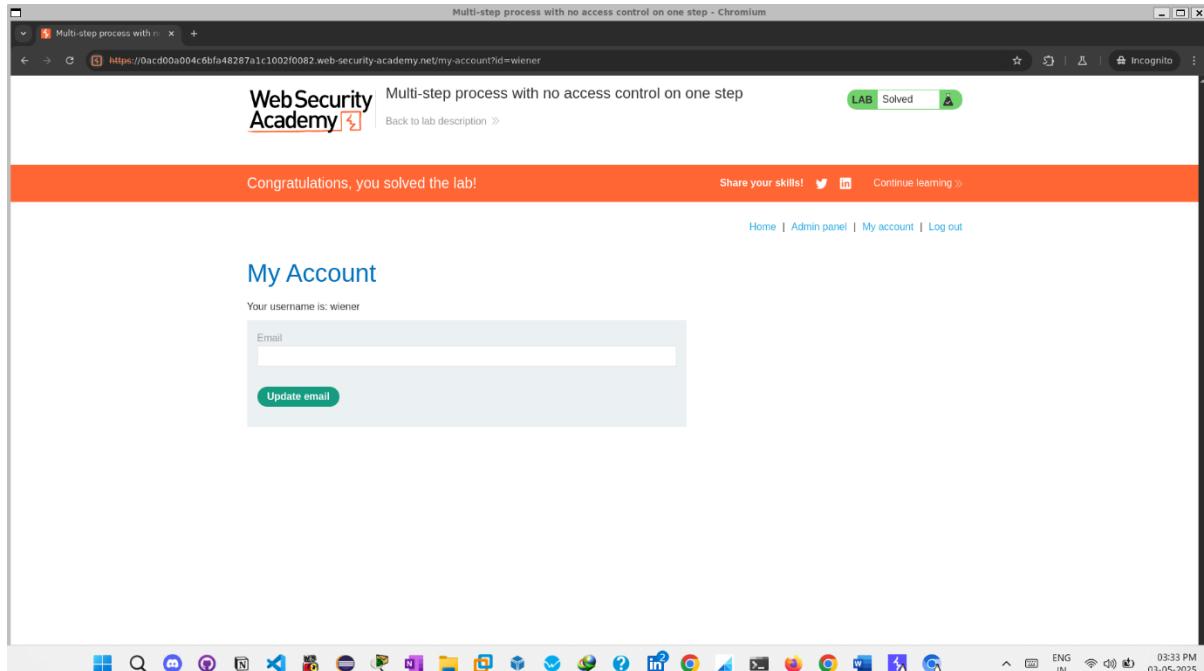
PORTSWIGGER LAB 11 – Method-based access control can be circumvented



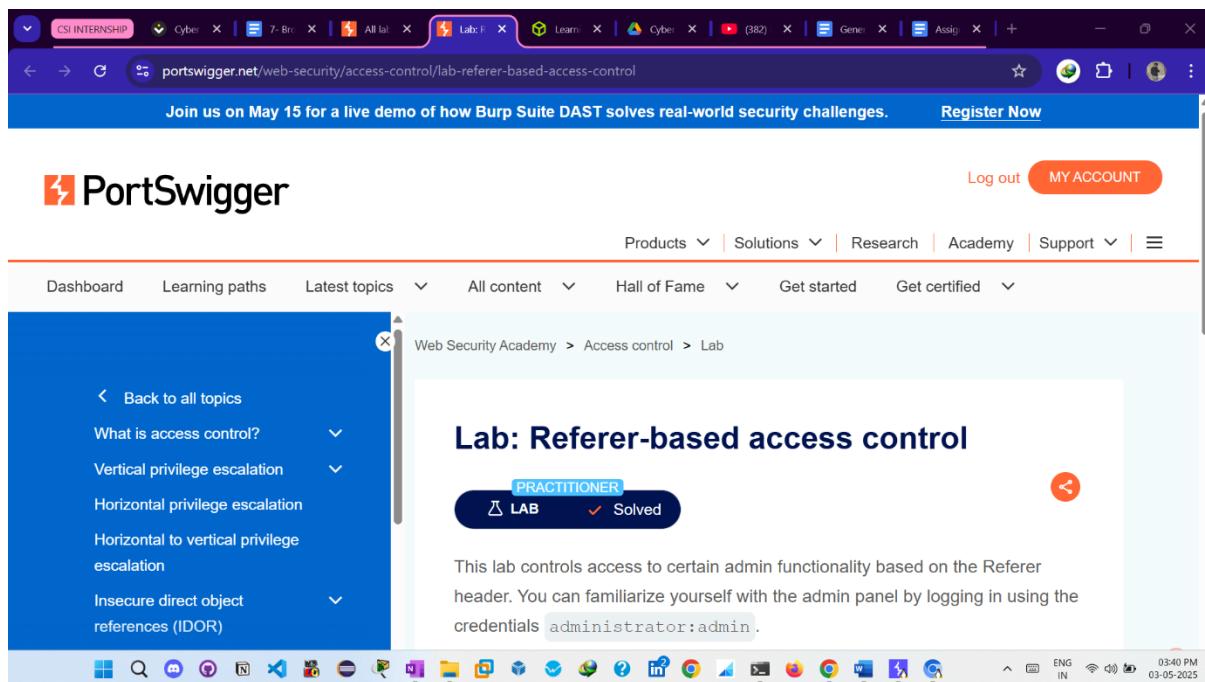
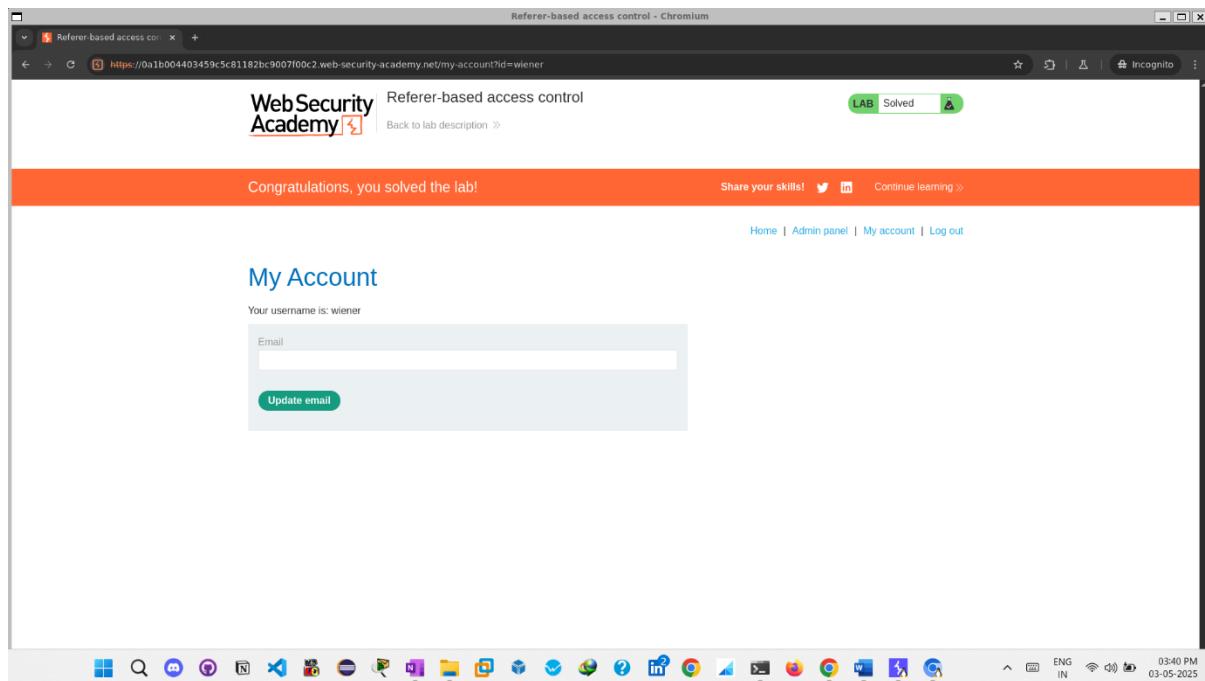


A screenshot of a web browser window showing the PortSwigger Lab page for the challenge "Lab: Method-based access control can be circumvented". The browser's address bar shows the URL "portswigger.net/web-security/access-control/lab-method-based-access-control-can-be-circumvented". The page features the PortSwigger logo and navigation menu. The main content area displays the lab title and a brief description. The bottom status bar shows various icons and the date/time "03:26 PM 03-05-2025".

PORTSWIGGER LAB 12– Multi-step process with no access control on one step



PORTSWIGGER LAB 13– Referer-based access control



PS: Really happy to solve all labs this time, learned a lot more. Thankyou for this internship