**LAB 10: USER ID CONTROLLED BY REQUEST PARAMETER WITH PASSWORD DISCLOSURE**

**B1:** Mở phần mềm Burp Suite lên, chuyển sang tab Proxy 🡪 HTTP history 🡪 Open browser.

A screenshot of a computer

Description automatically generated

**B2:** Copy và paste link sau vào browser để thực hiện lab10 (nhớ bấm access lab).

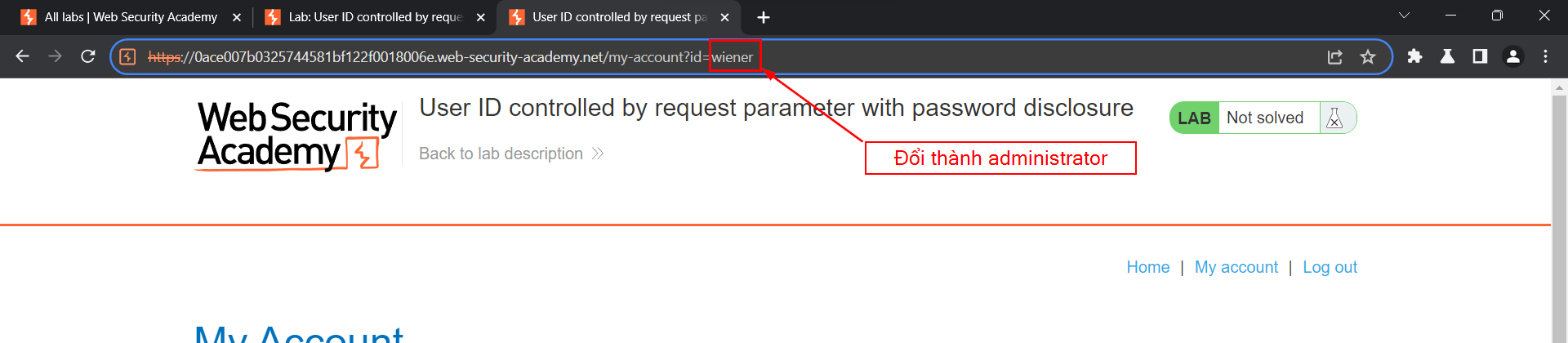
<https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-password-disclosure>

**B3:** Bấm vào My account, nhập tài khoản và mật khẩu đã được gợi ý 🡪 Log in.

A screenshot of a computer

Description automatically generated

**B4:** Trong thanh search, đổi giá trị của id từ wiener thành administrator rồi nhấn Enter.

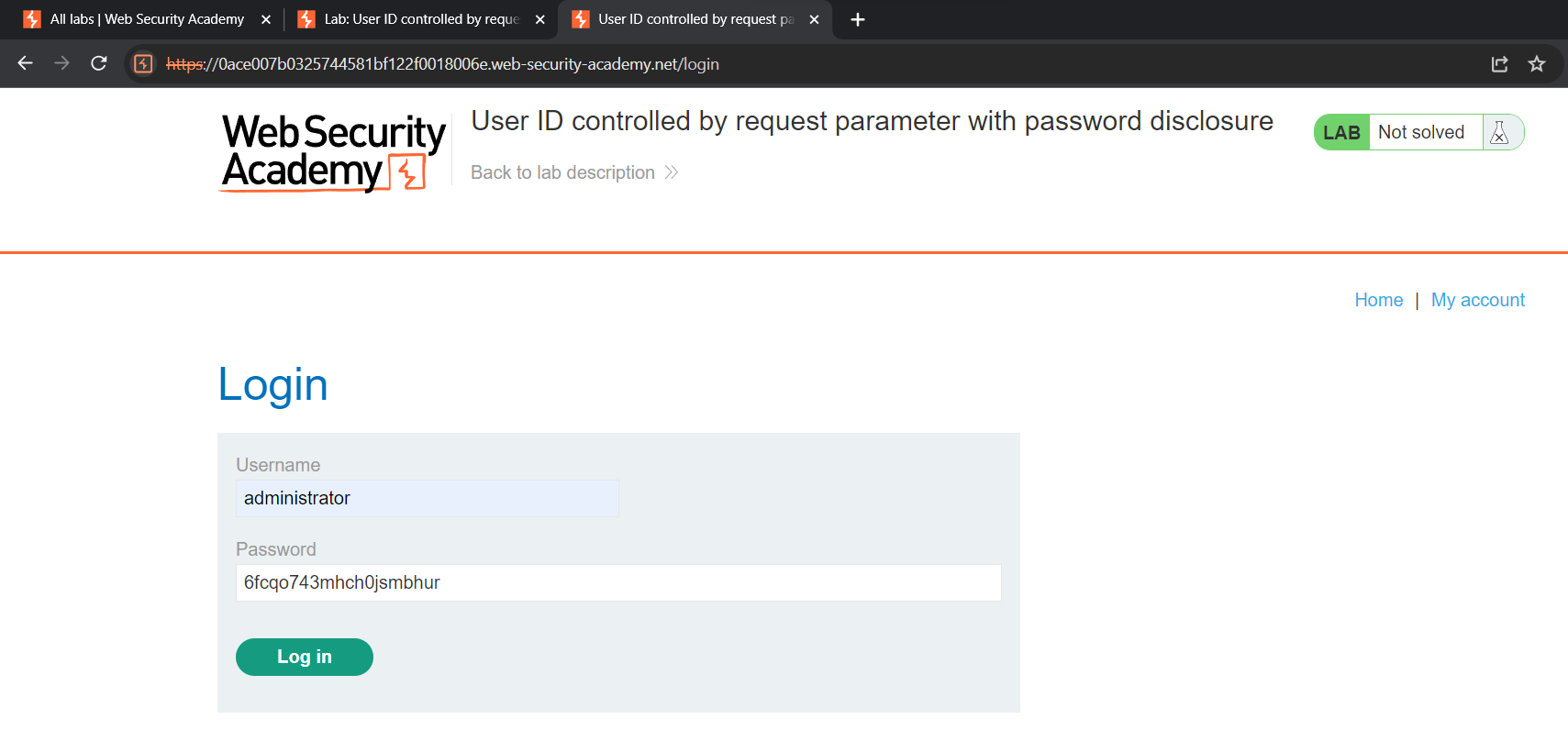


**B5:** Vô lại phần mềm Burp Suite, dò URL nào mà là “/my-account?id=administrator” (có dấu tick bên cạnh). Quan sát phần Response ta sẽ thấy được mật khẩu của tài khoản admin. Hãy copy mật khẩu này.

A screenshot of a computer

Description automatically generated

**B6:** Vô lại trang lab, login với username là administrator, password là cái ta vừa copy khi nãy.



**B7:** Bây giờ ta đã vô được tài khoản admin, chọn Admin panel.

A screenshot of a computer

Description automatically generated

**B8:** Tiến hành delete carlos và ta đã hoàn thành xong lab này.

A screenshot of a computer

Description automatically generated

**-- HẾT --**