**LAB 5: URL-BASED ACCESS CONTROL CAN BE CIRCUMVENTED**

**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 lab5 (nhớ bấm access lab).

<https://portswigger.net/web-security/access-control/lab-url-based-access-control-can-be-circumvented>

**B3:** Bấm vào mục Admin panel.

A screenshot of a computer

Description automatically generated

**B4:** Có thể thấy sau khi bấm vào mục Admin panel thì chúng ta đang bị từ chối truy cập.

A screenshot of a computer

Description automatically generated

**B5:** Vô lại phần mềm Burp Suite, chọn Host và URL như trong hình và chọn Send to Repeater.

A screenshot of a computer

Description automatically generated

**B6:** Chuyển sang tab Repeater, ở cửa sổ Inspector, ta thay đổi “/admin” sang “/” và thêm X-Original-Url: /admin vào cửa sổ Request. Rồi nhấn Send.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**B7:** Quan sát cửa sổ Response, ta thấy mã 200 OK, vậy có nghĩa là bây giờ ta đã là vô được trang admin.

A screenshot of a computer

Description automatically generated

**B8:** Bây giờ ở mục Request query parameters hãy thêm các giá trị như trong hình. Và thêm X-Original-Url: /admin/delete vào cửa sổ Request. Rồi nhấn Send.

A screenshot of a computer

Description automatically generated

**B9:** Quan sát cửa sổ Response, ta thấy mã 302 Found. Có nghĩa là ta đã xóa thành công user carlos như đề yêu cầu.

A screenshot of a computer

Description automatically generated

**B10:** Vô lại trang làm lab, refresh lại trang và ta đã hoàn thành xong lab này.

A screenshot of a computer

Description automatically generated

**-- HẾT --**