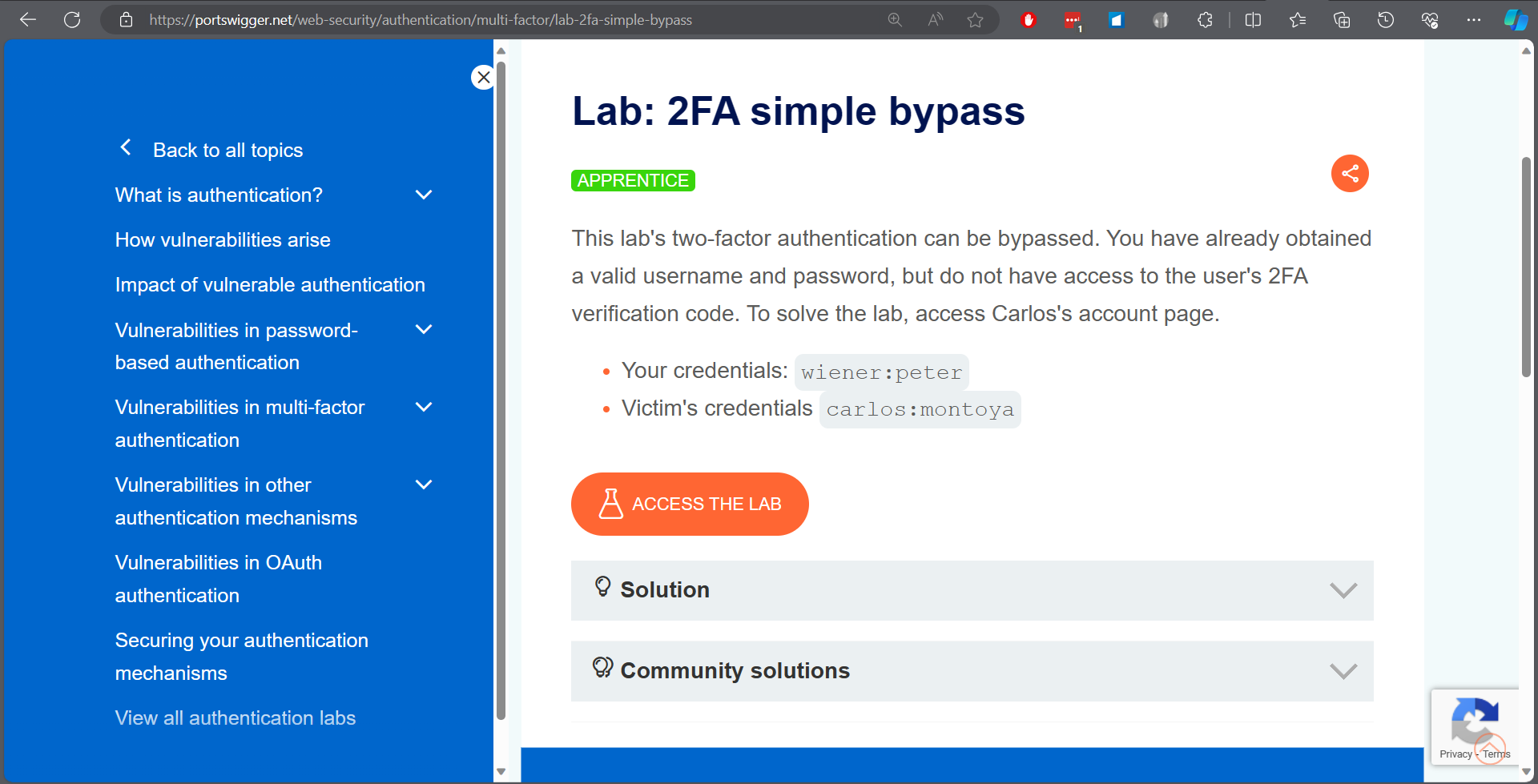
|  |  |
| --- | --- |
| **Lab 4 - Authentication-Vulnerabilities (multi-factor authentication)** | |
| **Name** | Tran Minh Triet |
| **Student ID** | SE172241 |

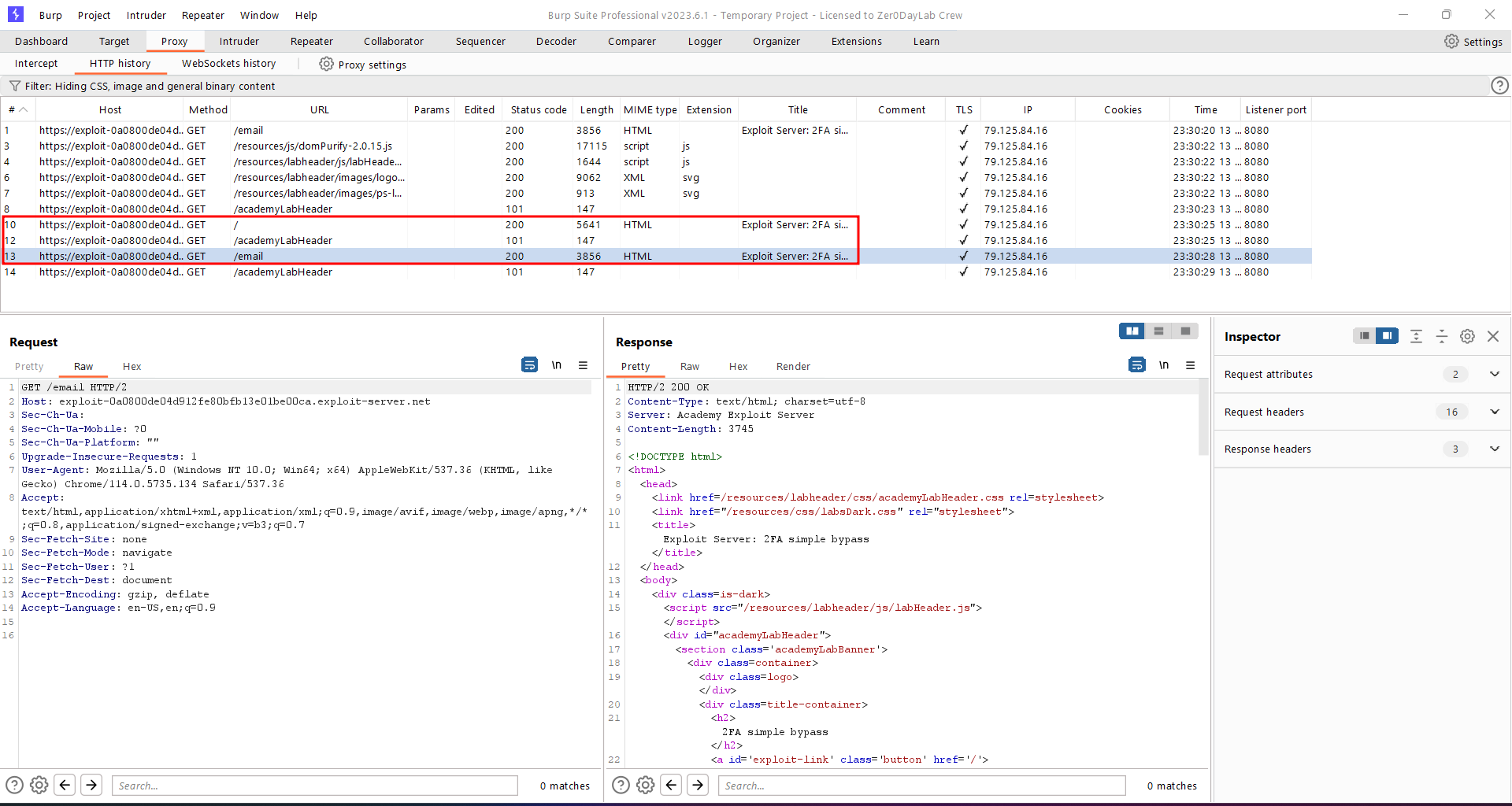
**Giới Thiệu: Trong bài lab này ta sẽ tìm hiểu về lỗ hổng multi-factor authentication**

## **2FA simple bypass <**[**Here**](https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-simple-bypass)**>**

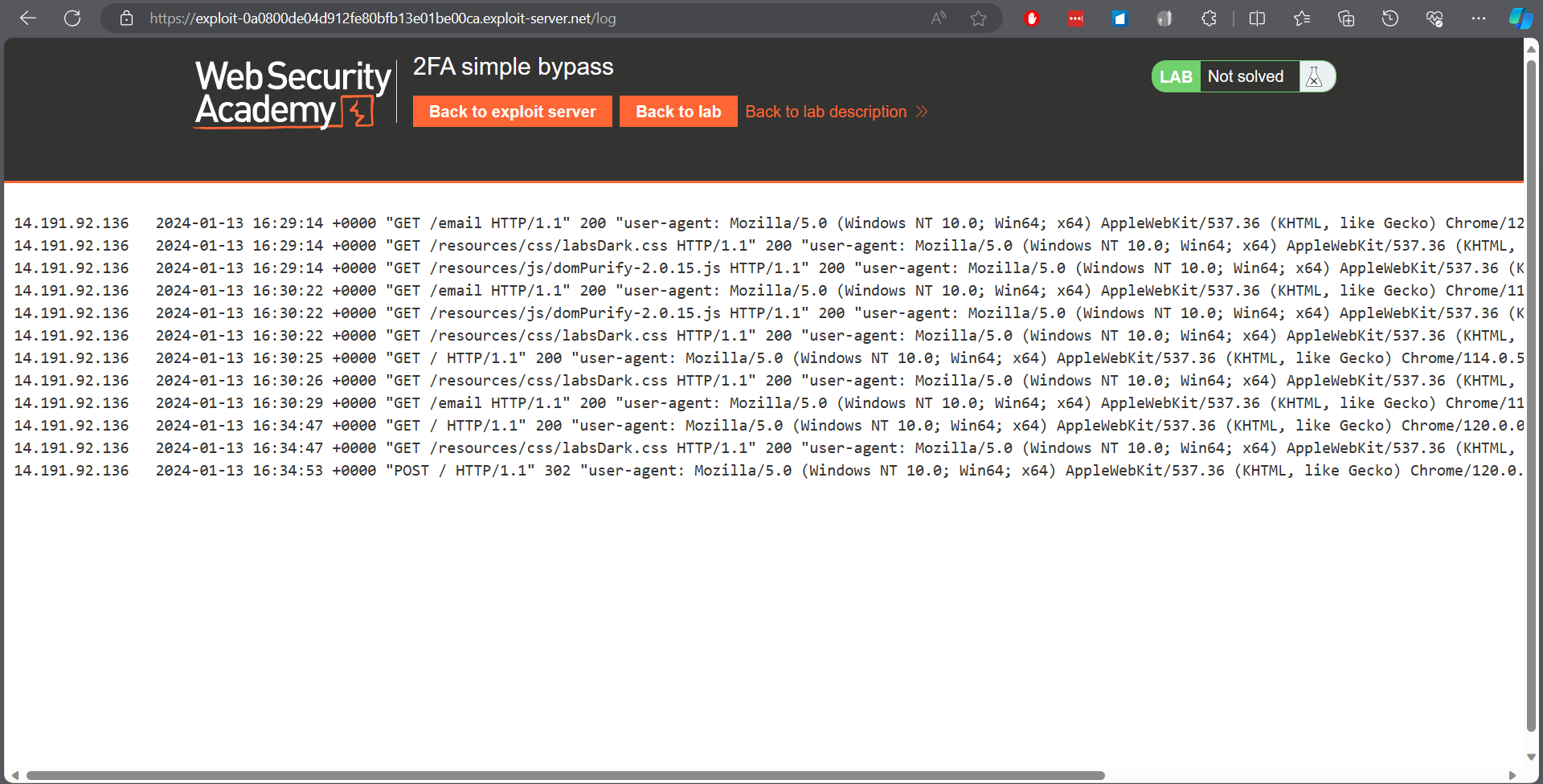


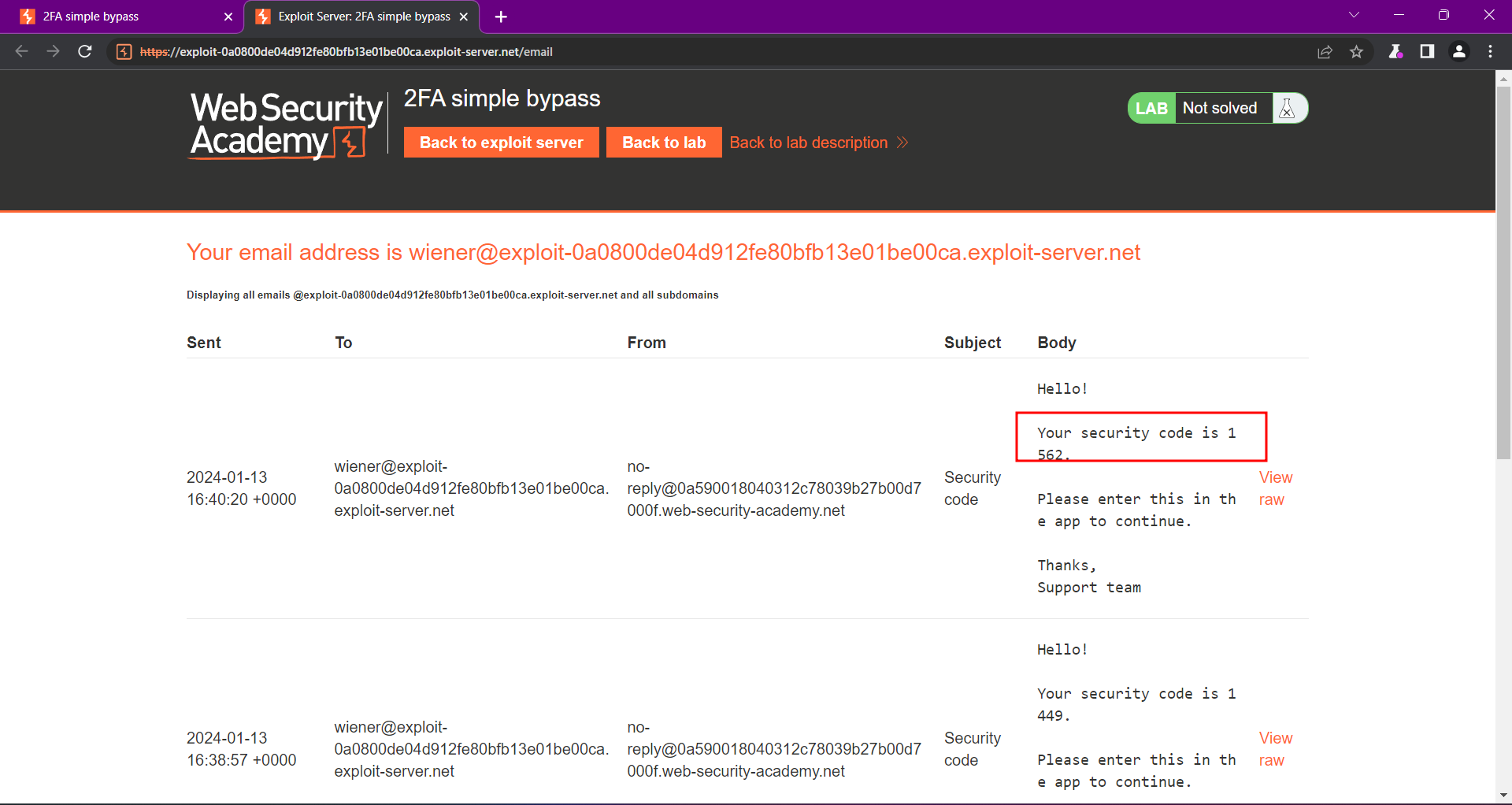
* Mục tiêu của bài lab này là truy cập được vào trang tài khoản của **Carlos**
* Thông tin mà bài lab cung cấp là
  + Account dùng để test: **wiener:peter**
  + Account nạn nhân: **carlos:montoya**

1. Đầu tiên ta sẽ thử login vào bằng tài khoản dùng để test

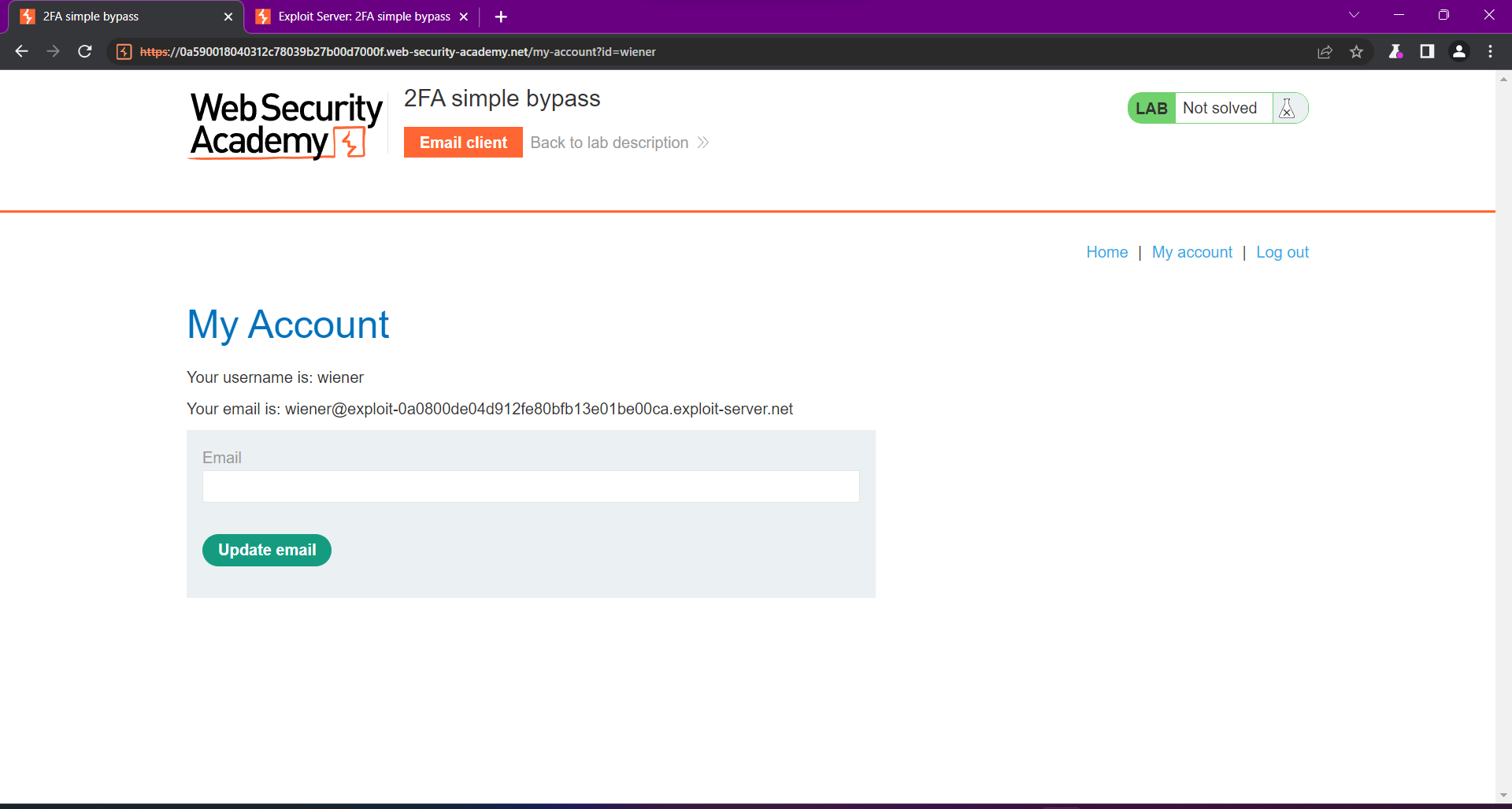


1. Tiếp theo bấm vào nút **Email client**





1. Giờ ta quay lại trang nhập security code và nhập “**1562**”



* Có thể thấy sau khi nhập xong code thì nó sẽ được redirect đến trang quản account bằng đường dẫn “**/my-account**”

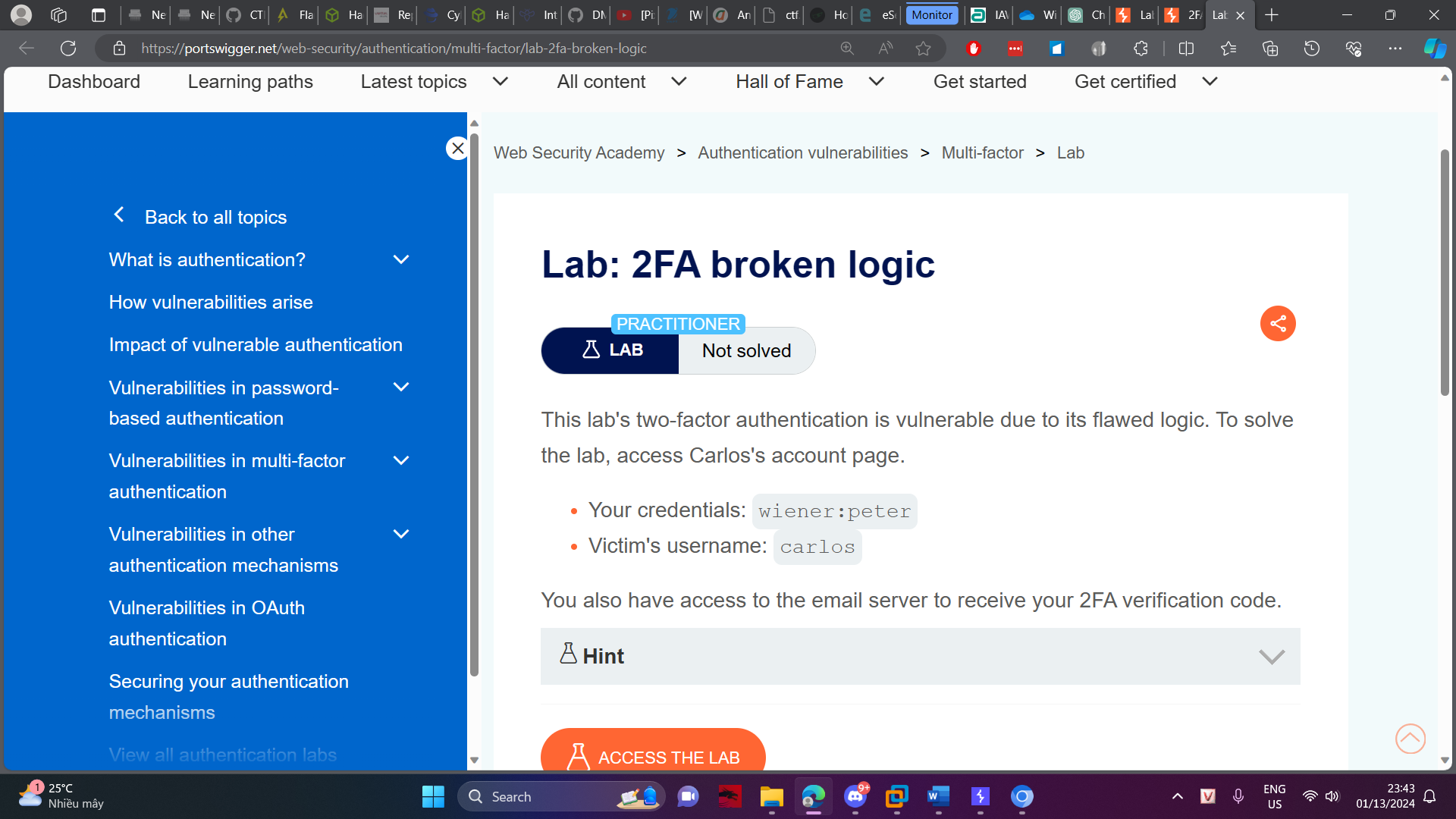
Giờ ta sẽ thử login bằng account của Carlos đã cho sẵn

A screenshot of a computer

Description automatically generated

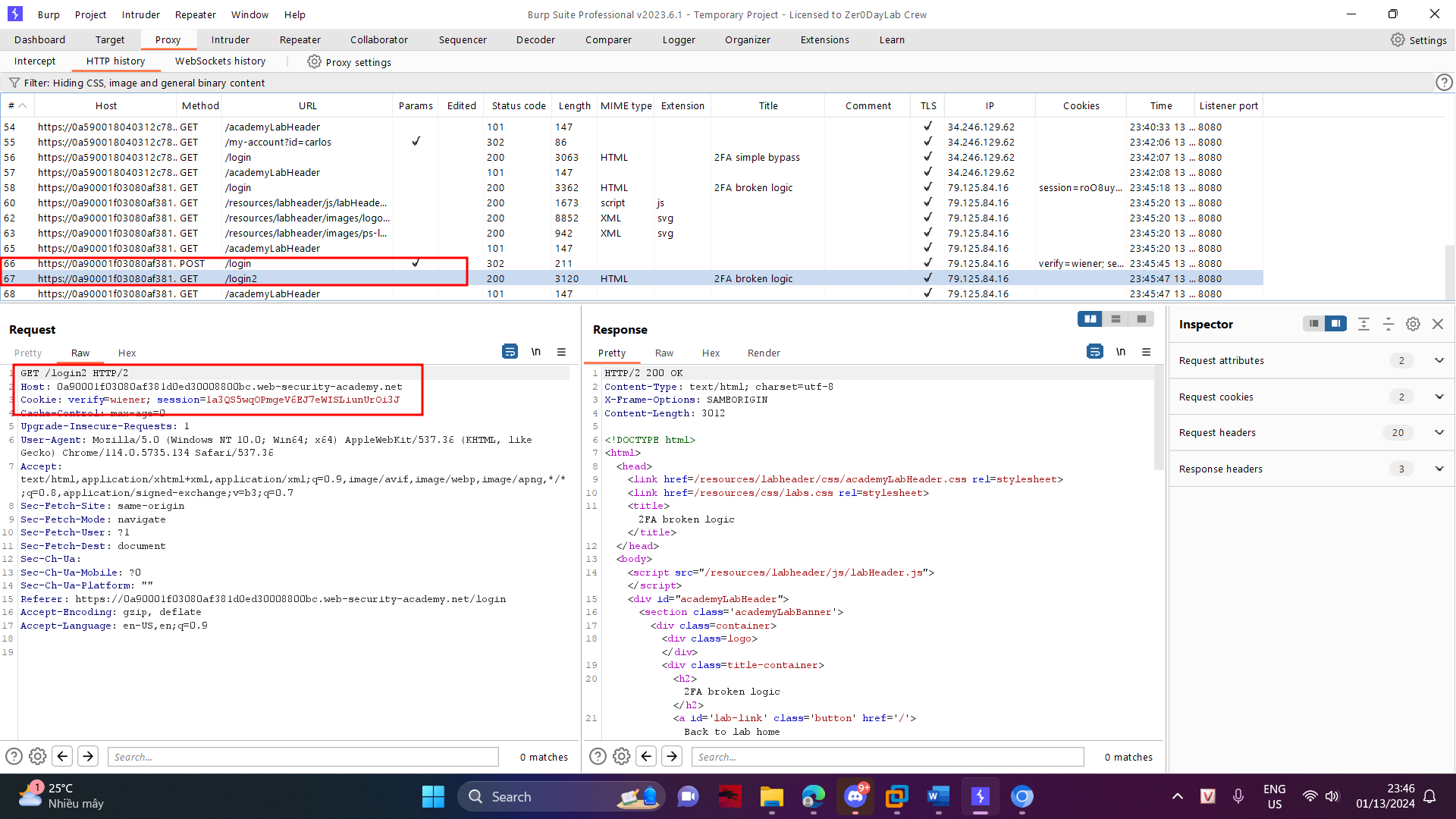
* Có thể thấy rằng khi bị yêu cầu nhập security code “**/login2**” để bỏ qua ta sẽ điều hướng trực tiếp đến “**/my-account**” mà không cần nhập mã code.
* Vậy bài lab này đã được solve

## **2FA broken logic <**[**Here**](https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-broken-logic)**>**



* Mục tiêu của bài lab này tương tự như trên. Tuy nhiên thông tin mà bài lab cung cấp như sau:
  + Account dùng để test: **wiener:peter**
  + Account nạn nhân: **carlos**
  + Khác với bài lab trên là bài lab này không có password của nạn nhân

1. Đầu tiên ta truy cập vào bài lab, sau đó login bằng tài khoản test



* Tuy nhiên có thể thấy rằng ở đường dẫn “**/login2**”, ở header **Cookie** thì có thêm một biến **verify** nữa.

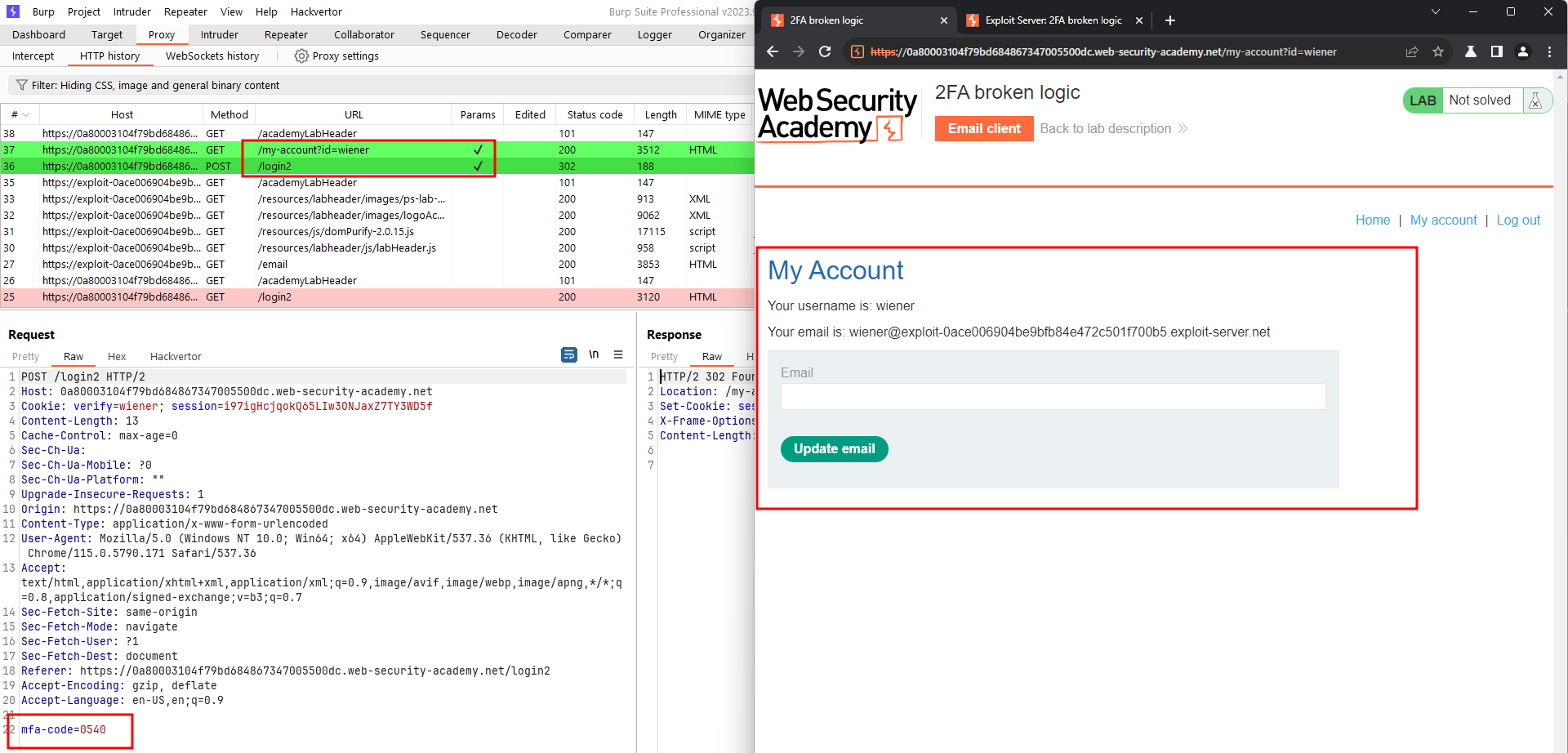
1. Tiếp theo bấm vào nút **Email client**

A screenshot of a computer

Description automatically generated

* Giờ ta sẽ thử nhập security code đó để xem quá trình diễn ra như thế nào

1. Sau khi nhập security code



* Sau khi nhập security code thì quá trình diễn ra vẫn giống như vậy
* Cái khác ở đây đó là biến verify ở header Cookie.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Sau đó quay lại **Proxy** gửi request “**POST /login2**” đến **Intruder**

A screenshot of a computer

Description automatically generated

Ta sửa thông tin như sau:

A screenshot of a computer

Description automatically generated

Về Payloads, ta cấu hình như sau

A screenshot of a computer

Description automatically generated

Sau đó **Start attack**, khi xong thì tìm request có HTTP **Status code** là **302**. Để dễ dàng hơn ta sẽ áp dụng filter

A screenshot of a computer

Description automatically generated

Sau khi chờ được một lúc thì ta đã tìm được code

A screenshot of a computer

Description automatically generated

Giờ ta sẽ truy cập vào trang web bằng session bằng cách

A screenshot of a computer

Description automatically generated

A screenshot of a computer error message

Description automatically generated

Sau đó dán vào trình duyệt

A screenshot of a computer

Description automatically generated

**---END---**