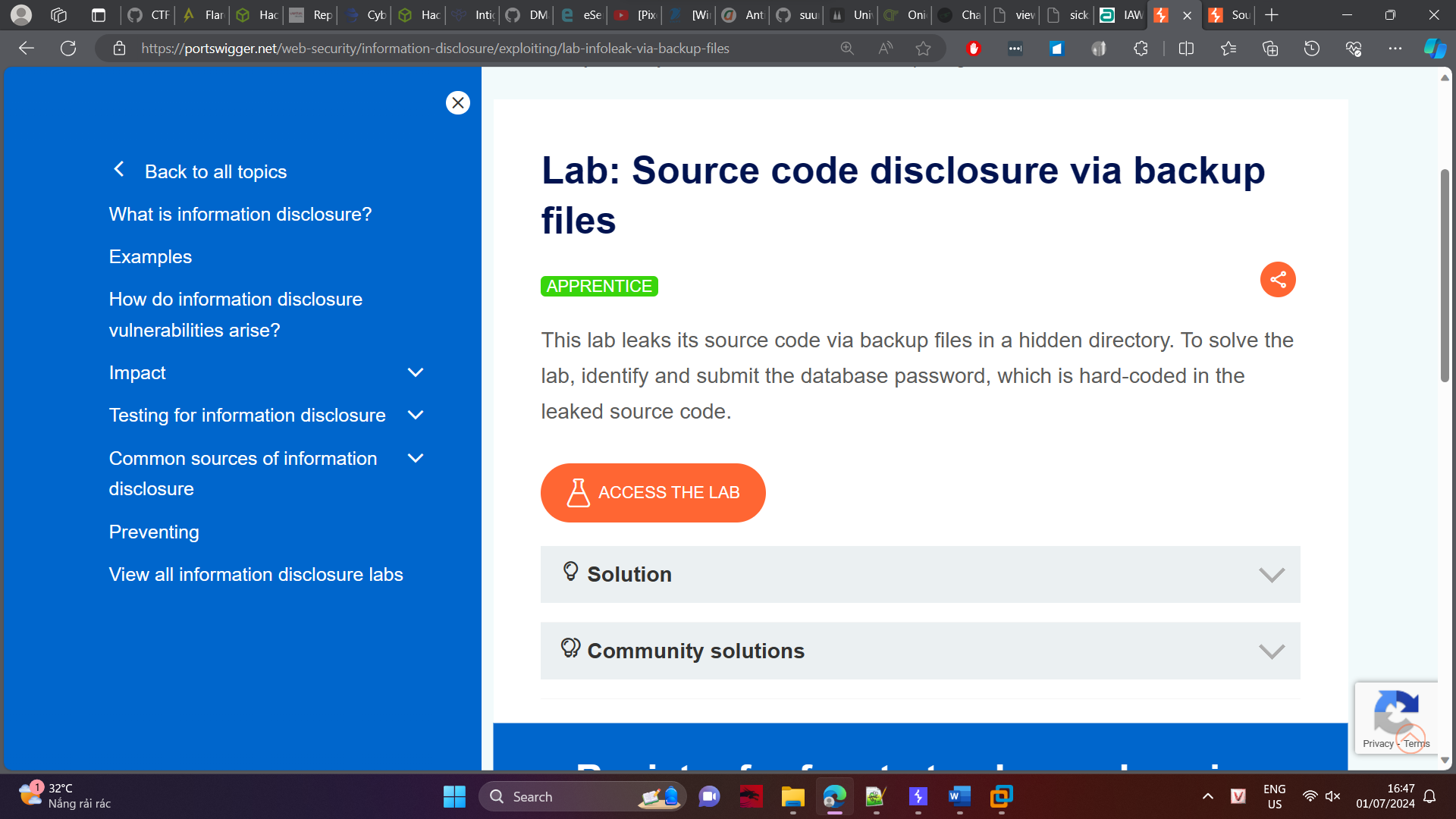
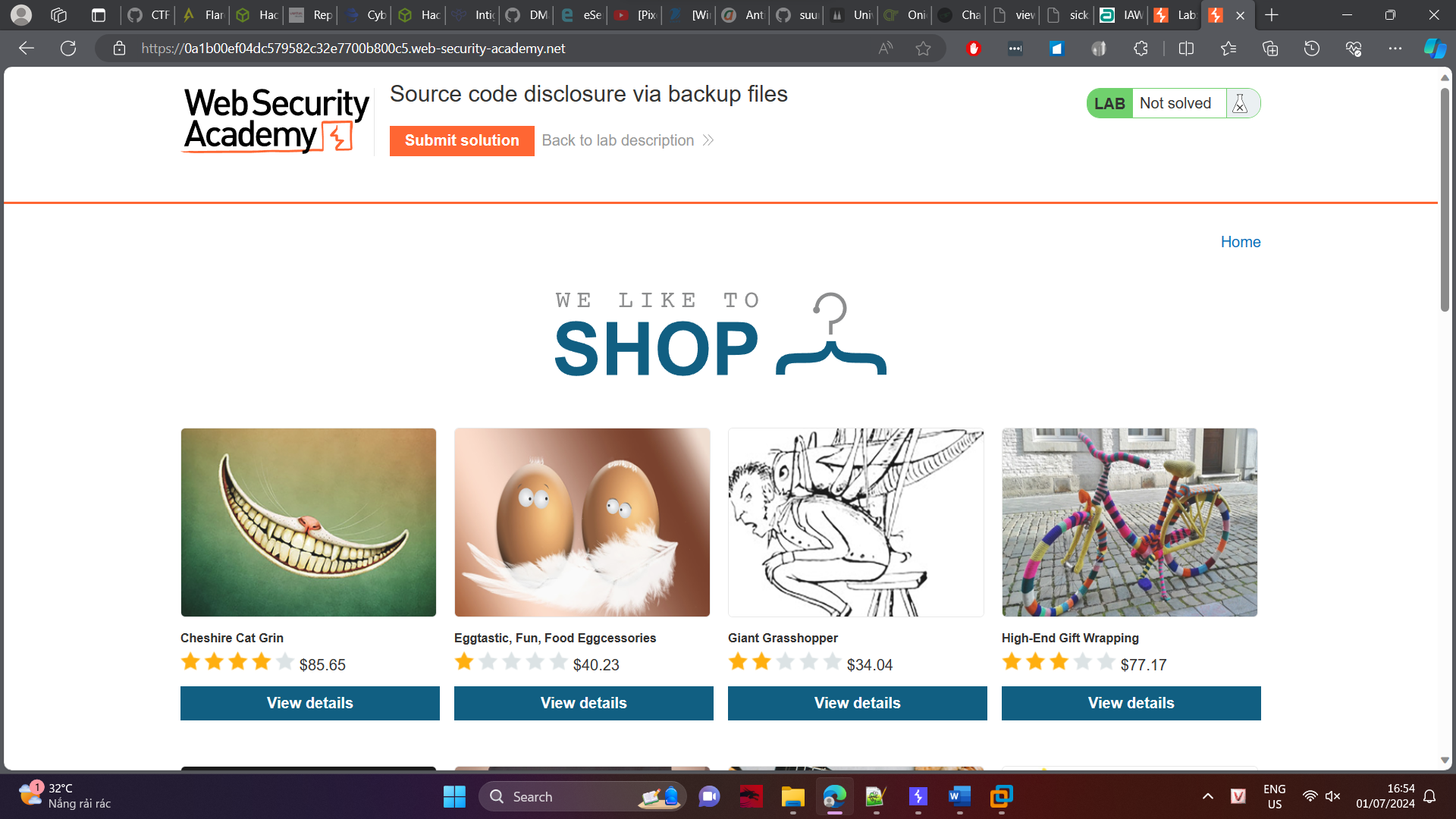
|  |  |
| --- | --- |
| **Lab 2:** **Information Disclosure** | |
| **Name** | Tran Minh Triet |
| **Student ID** | SE172241 |

**Giới Thiêu: Trong bài lab này ta sẽ tìm hiểu về lỗ hổng information disclosure**

## **Source code disclosure via backup files: <**[**HERE**](https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-via-backup-files)**>**

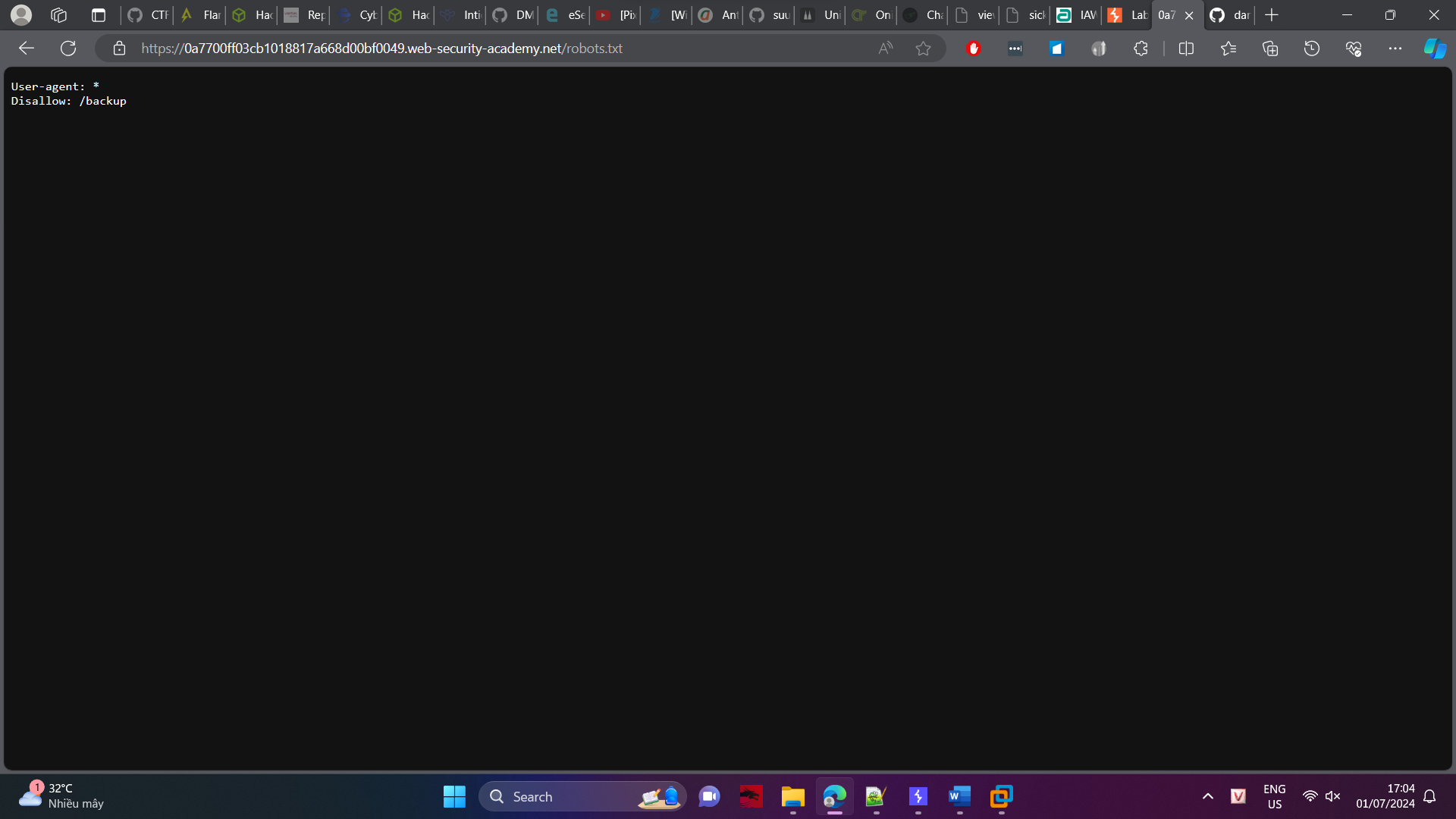


Ở bài lab này ta sẽ khai thác thông tin bị lộ của database từ source code trang web.



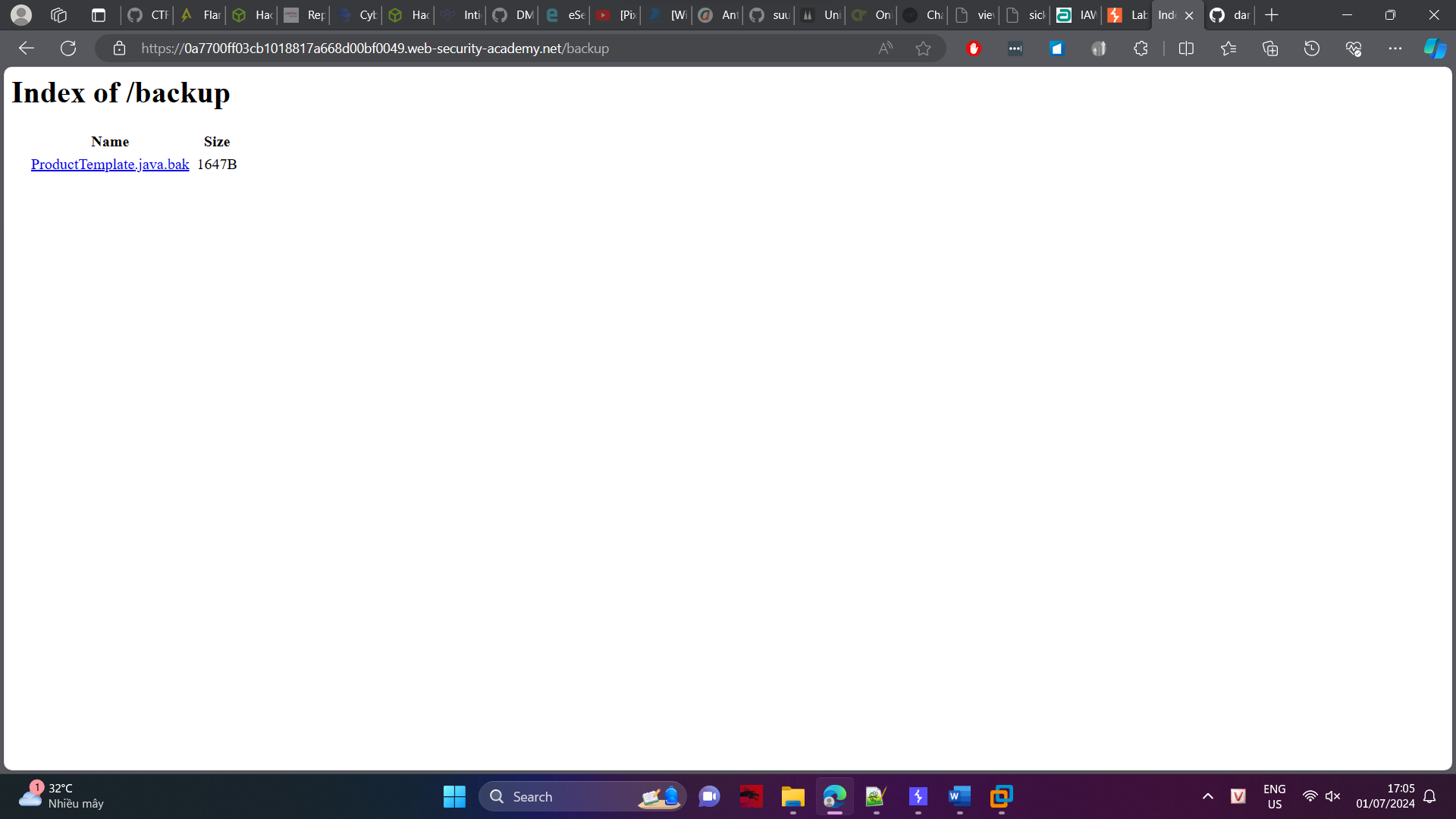
Đây là giao diện trang web một trang web bán hàng bình thường.

Trước tiên, ta chỉnh sửa url để xem content file robots.txt, thông thường khi pentest web ta nên xem file này đầu tiên để xem bên dev có lộ thông tin source code gì ở đây không.

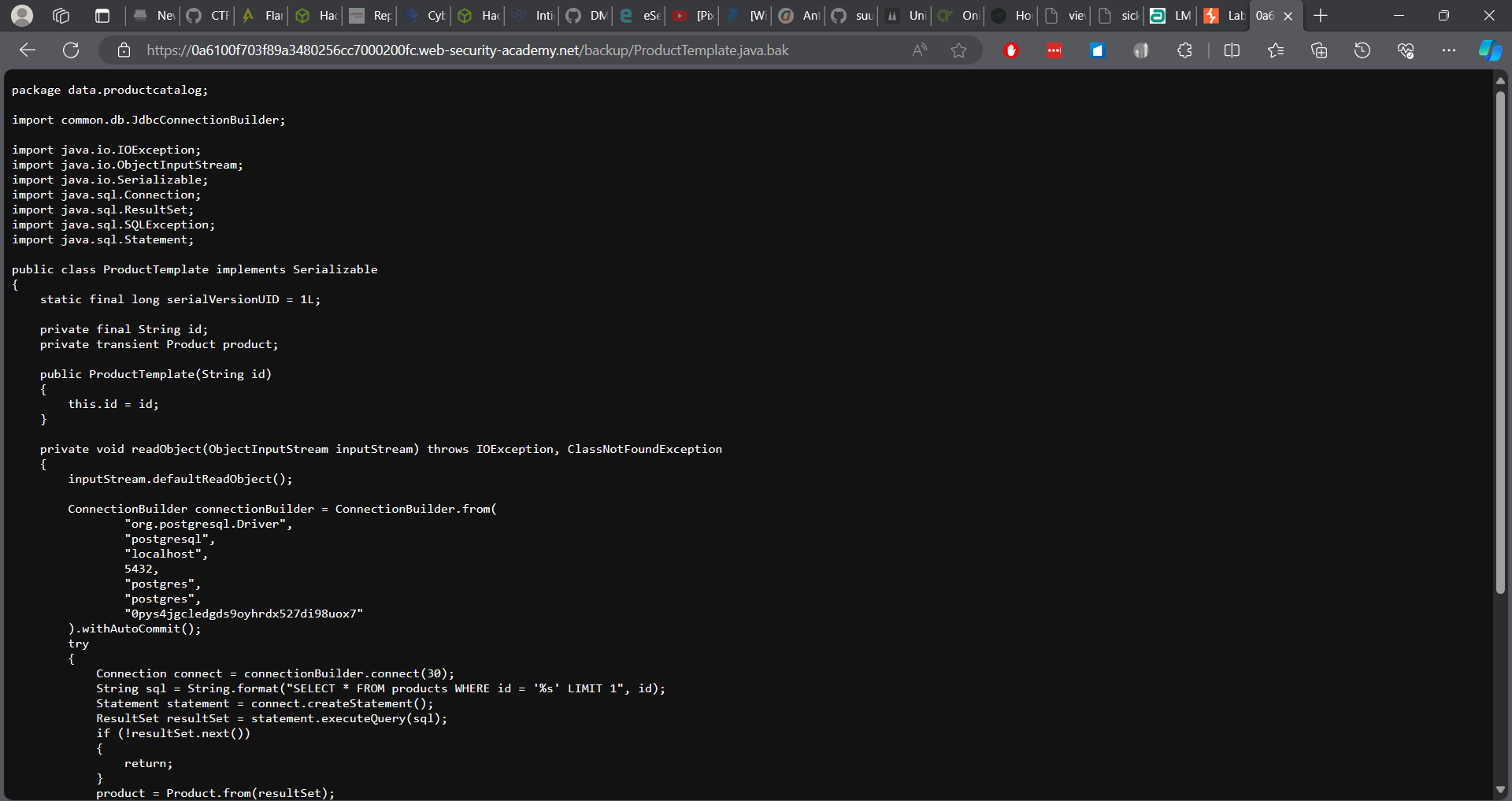


Ta thấy có một folder tên là `backup` ở đây. Vào xem thử nó là gì.

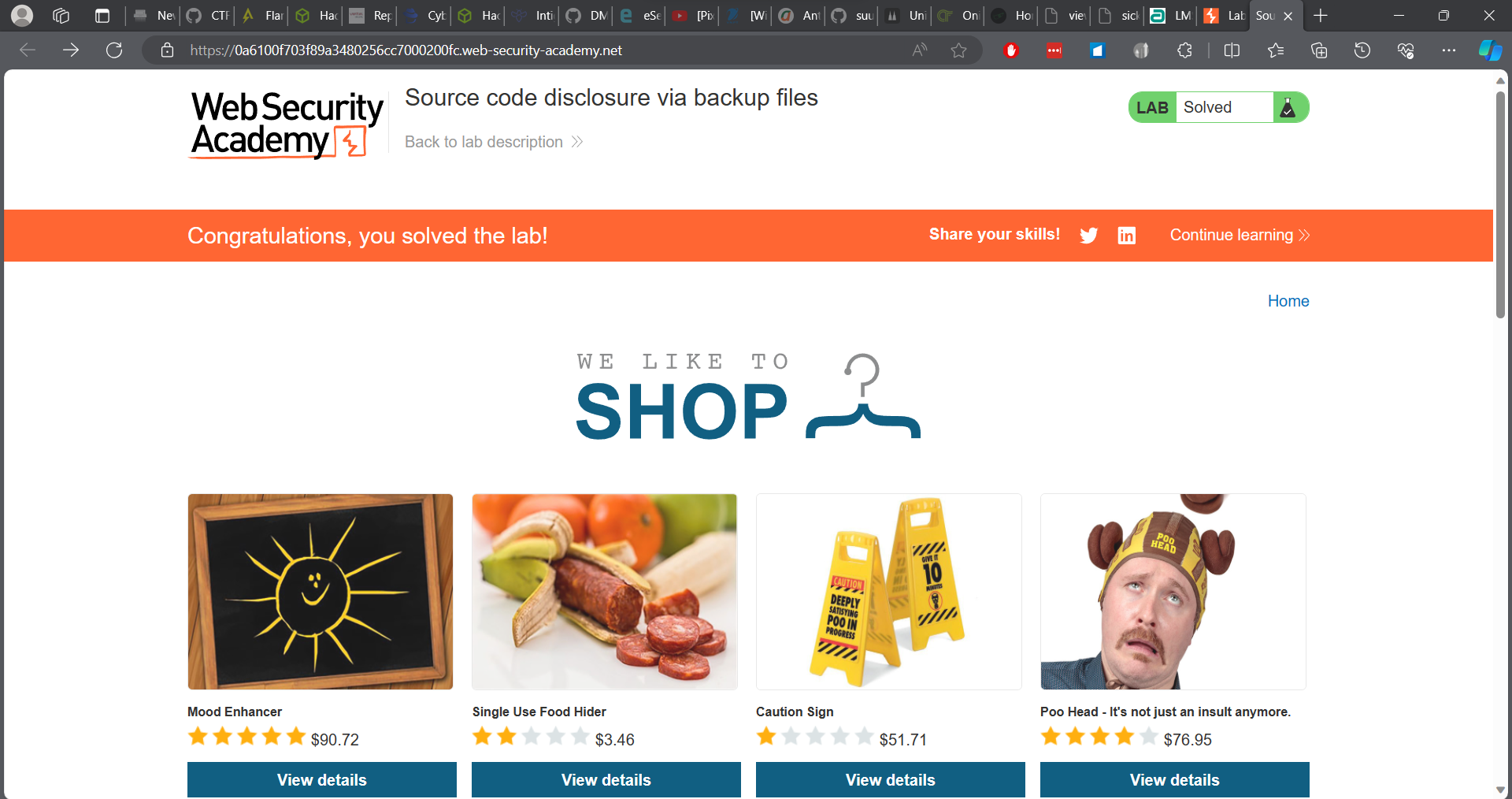
Peekaboo, folder này có chứa một file source code của trang web này.



Đây là một lỗi trong lập trình để lộ file access từ robots.txt, ta có thể đọc source code đẻ khai thác thêm nhưng lô hổng sâu hơn.



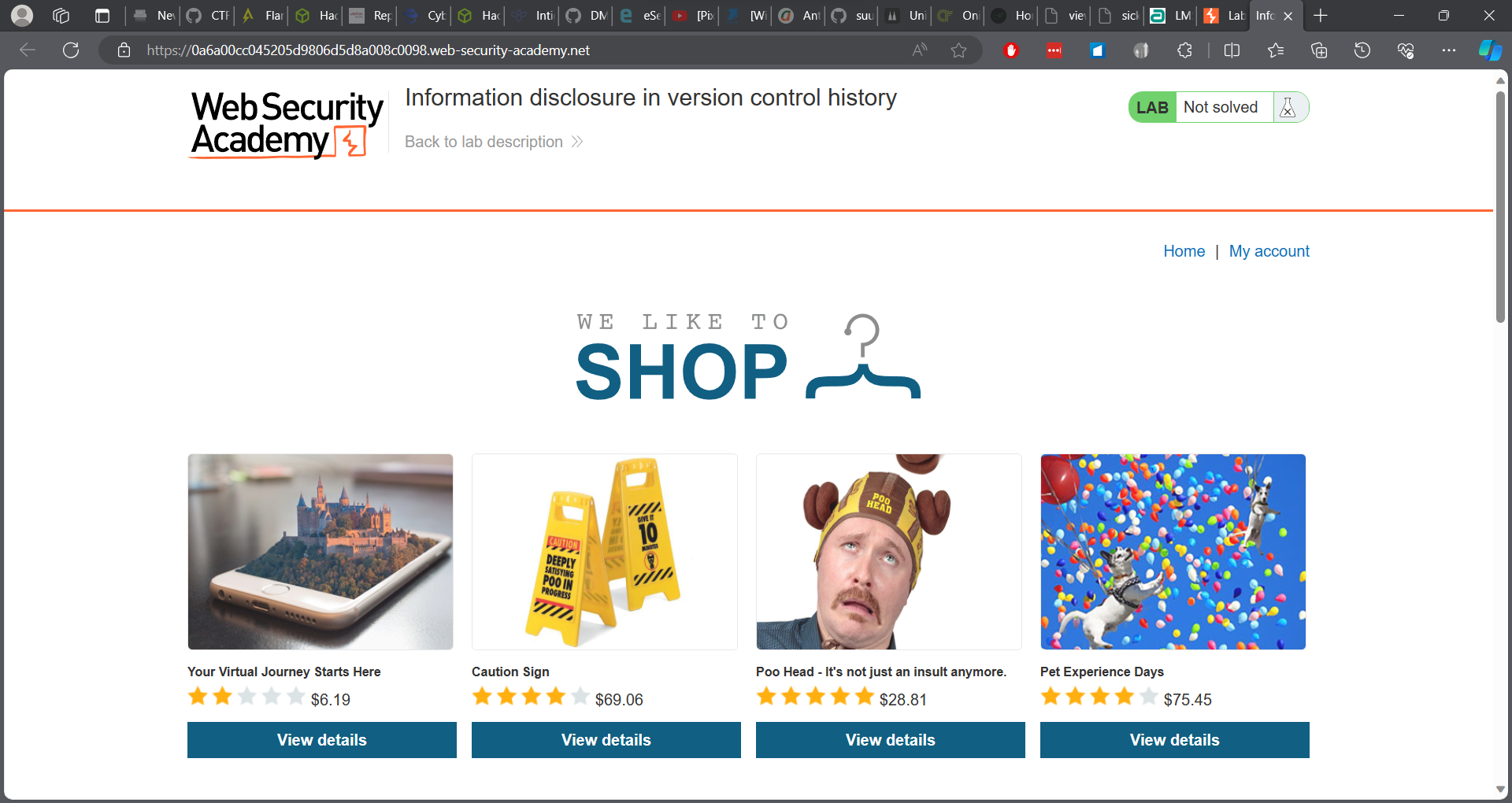
Như hình trên ta thấy password ta cần tìm là 0pys4jgcledgds9oyhrdx527di98uox7.



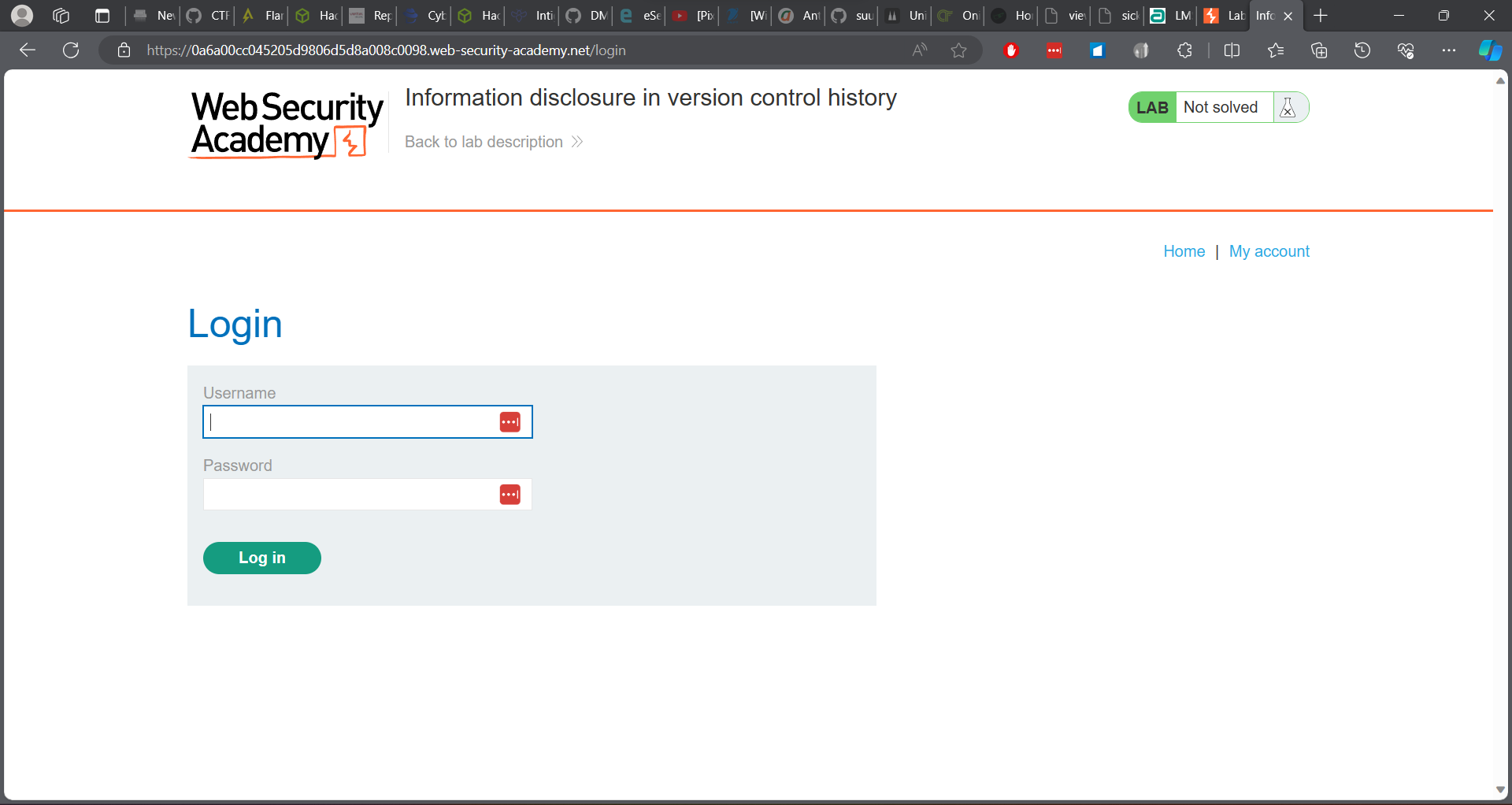
Vậy là ta đã giải xong bài lab đầu tiên.

## **Information disclosure in version control history: <**[**HERE**](https://portswigger.net/web-security/information-disclosure/exploiting/lab-infoleak-in-version-control-history)**>**

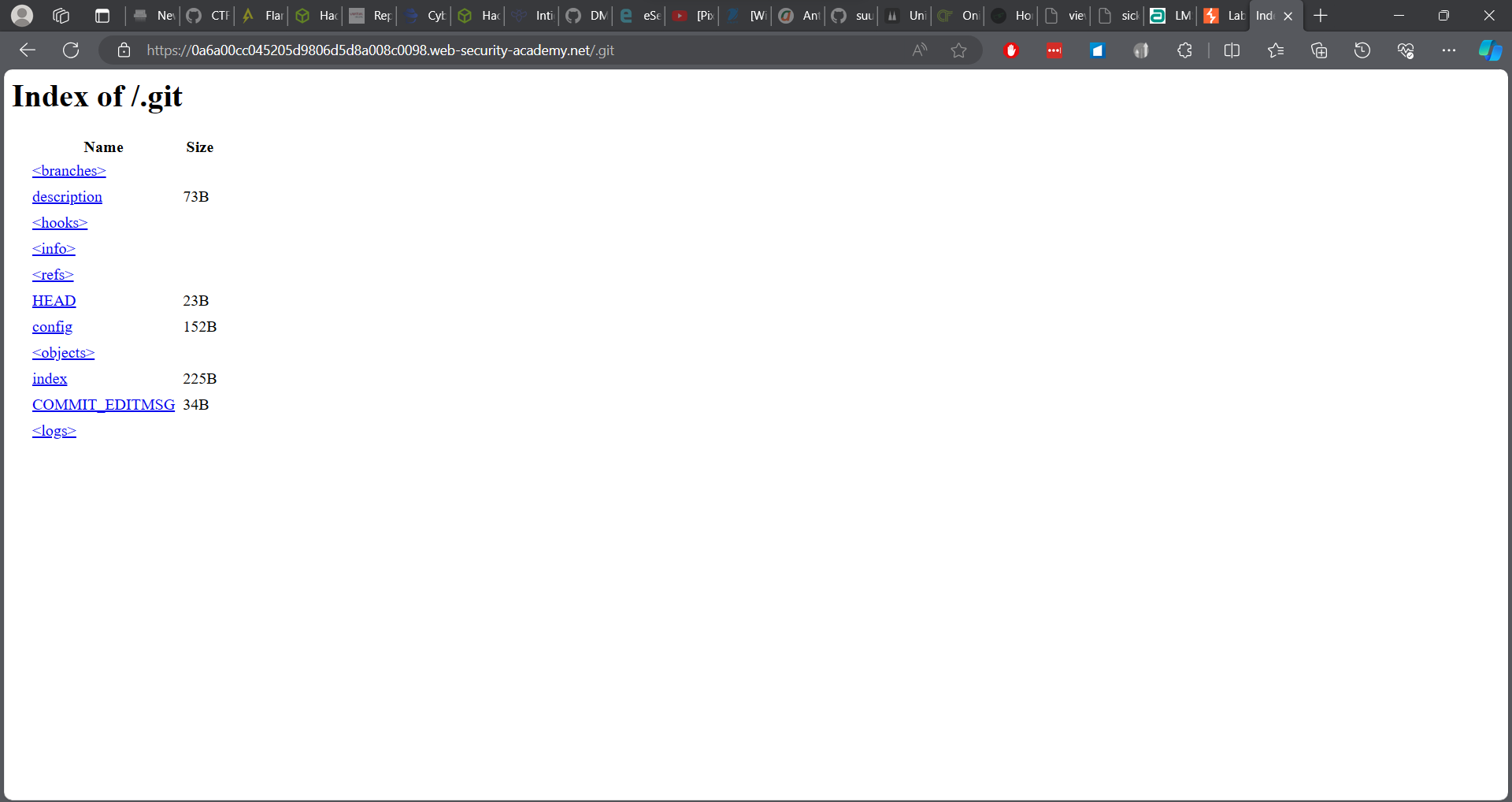
Ở bài này, ta sẽ tìm hiểu về lỗi để lộ mật khẩu ở phần history.



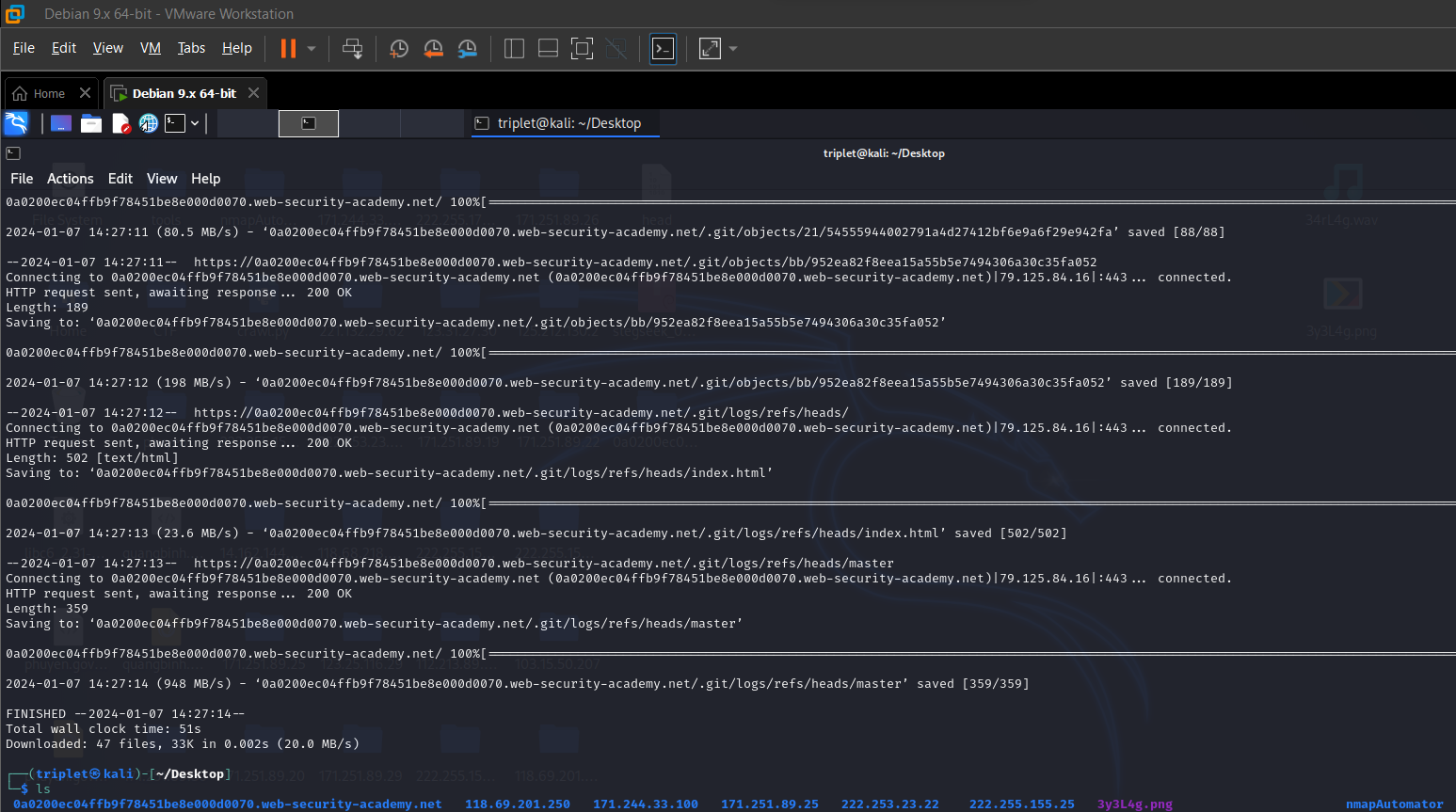
Vẫn là trang web cũ.

Nhưng lần này đề bài bảo chúng ta tìm password của user administrator

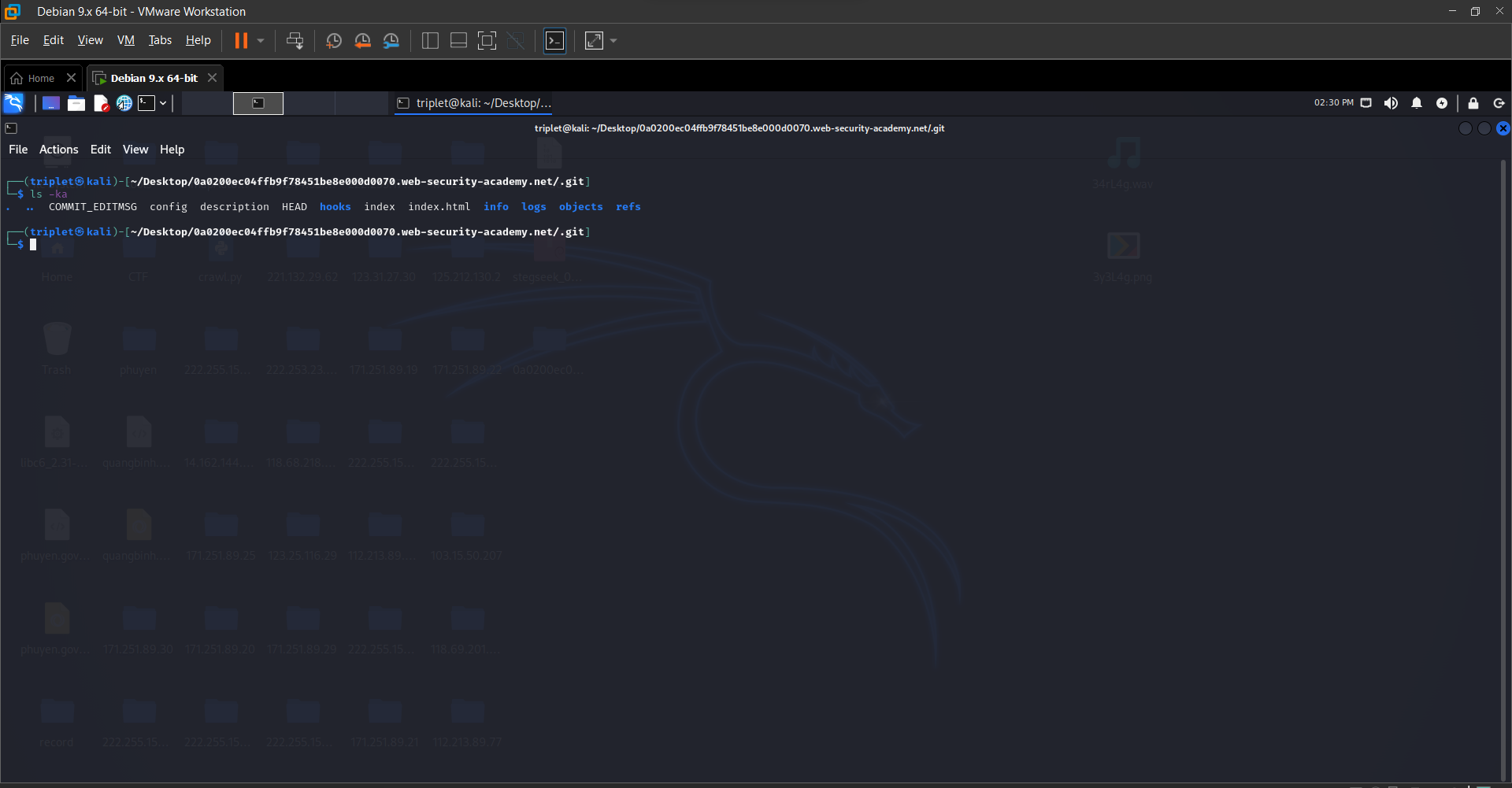
Sau khi truy cập vào đường dẫn .git thì ta phát hiện có một repo ở đây.



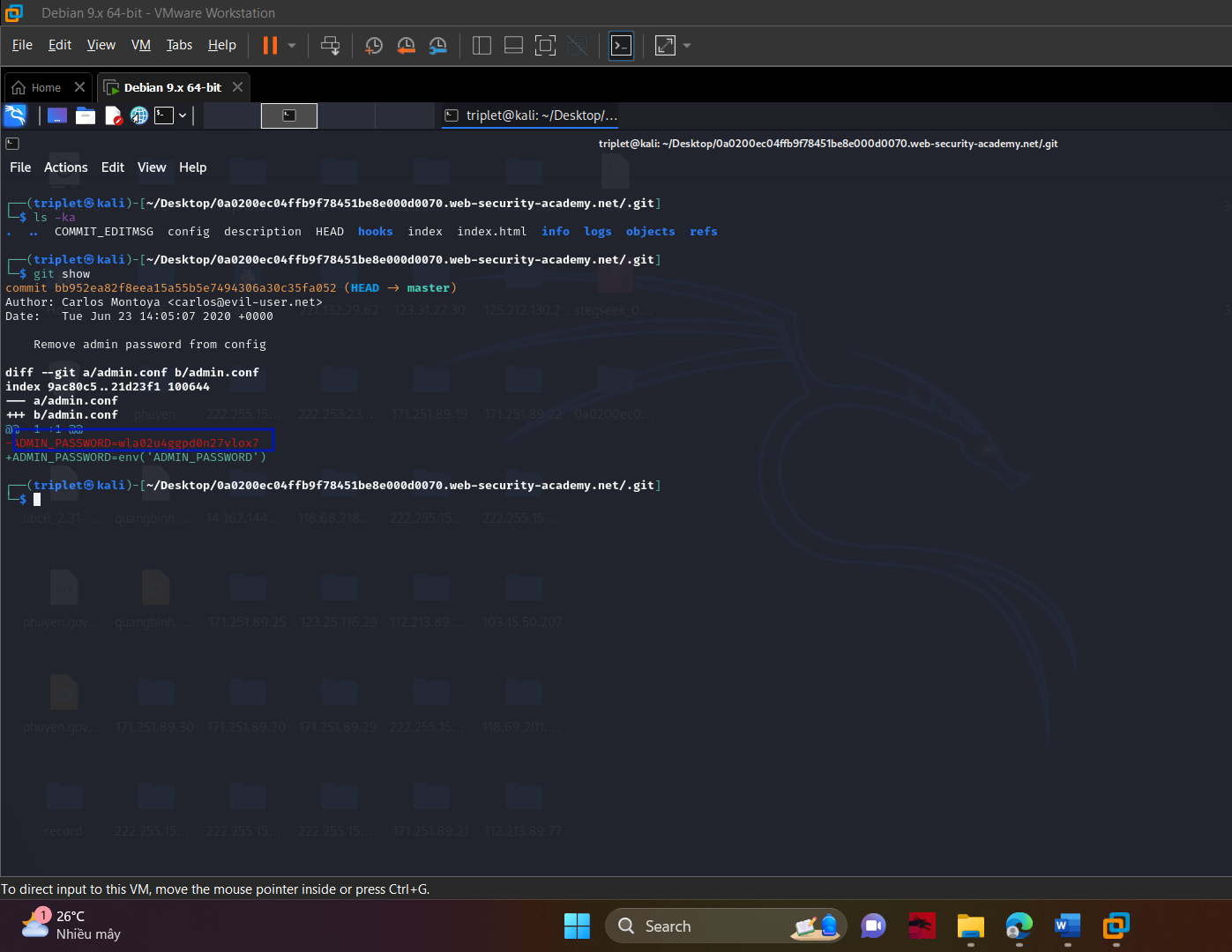
Thực hiện câu lệnh wget để tiến hành download repo này về máy.



Ta xem được một số content của repo này như sau

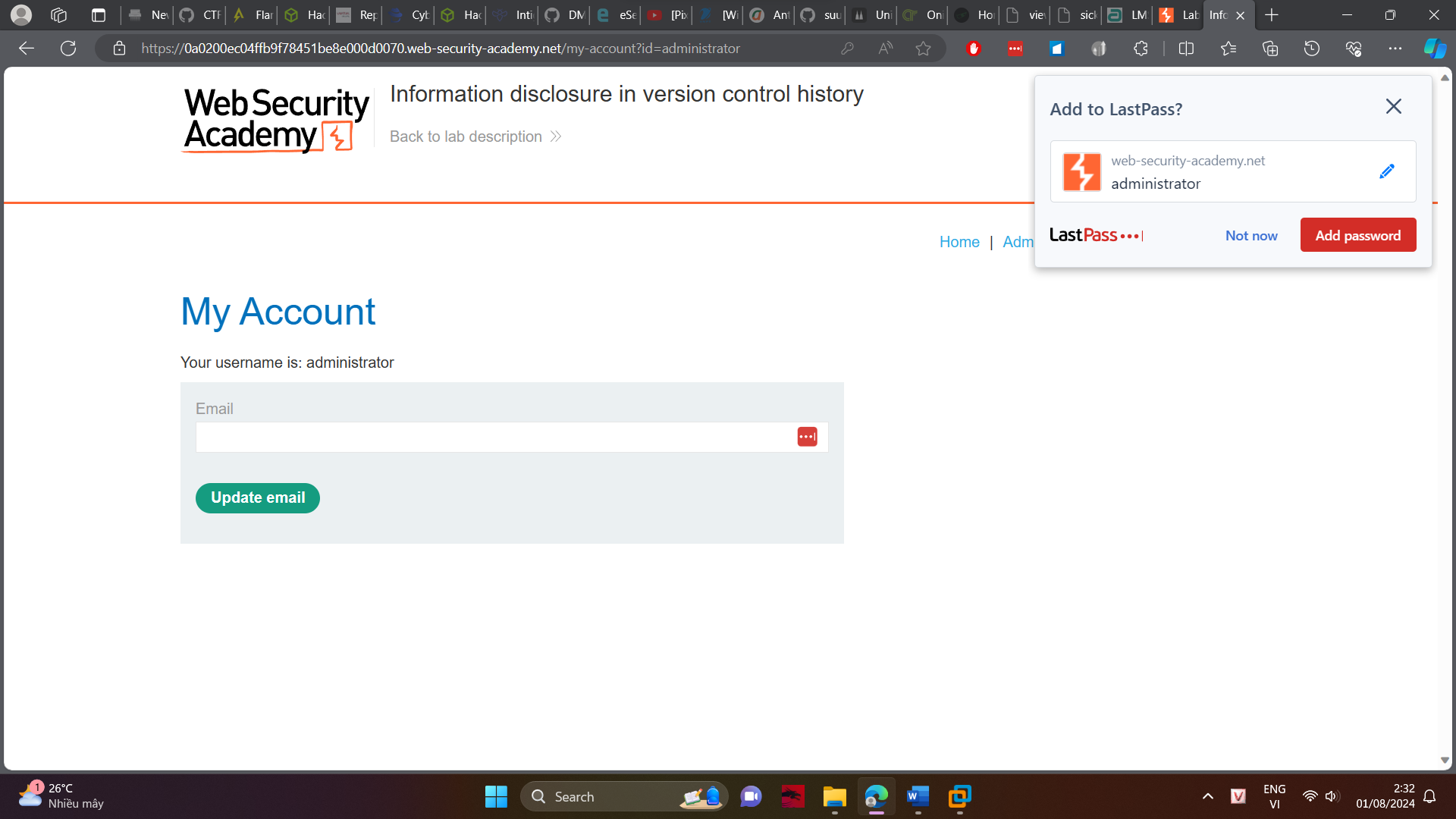


Dùng lệnh git show để xem lịch sử commit

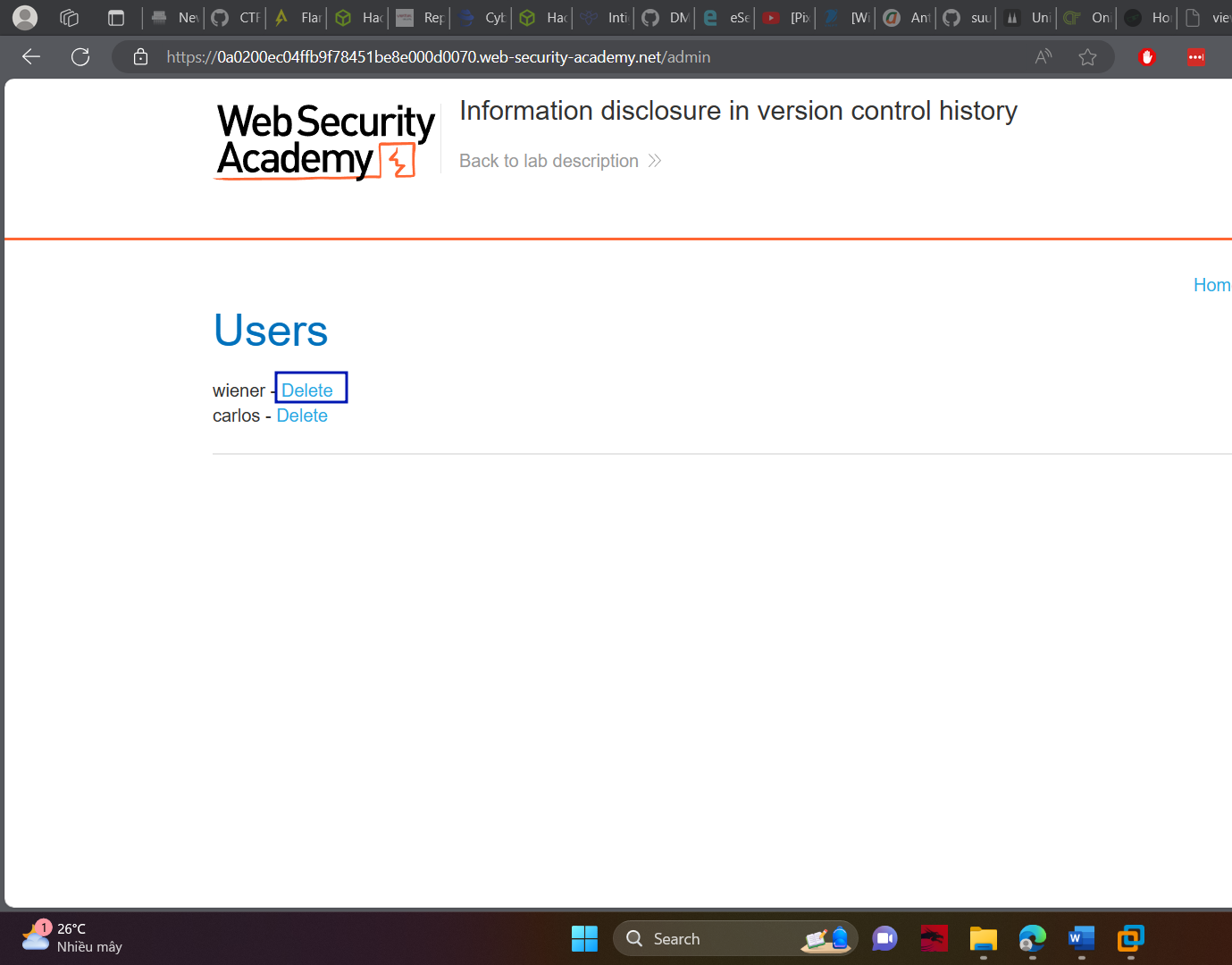


Ta thu được password bị xóa là wla02u4ggpd0n27vlox7

Tiến hành đăng nhập và xóa user như đề bài yêu cầu



Đã đăng nhập thành công



Vậy là ta đã xong bài lab thứ 2 roi.

**---END---**