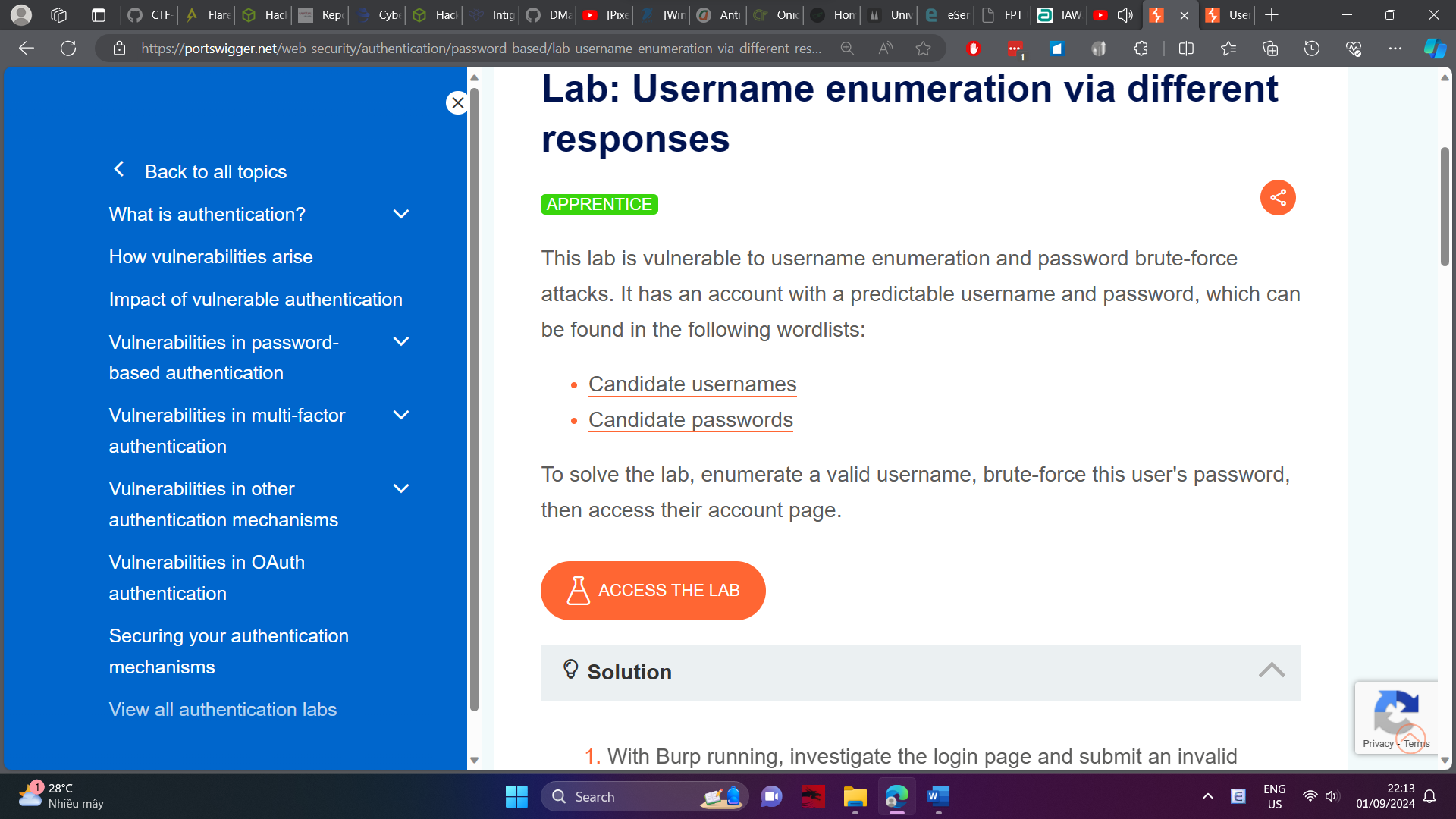
|  |  |
| --- | --- |
| **Lab 3: Authentication Vulnerabilities** | |
| **Name** | Tran Minh Triet |
| **Student ID** | SE172241 |

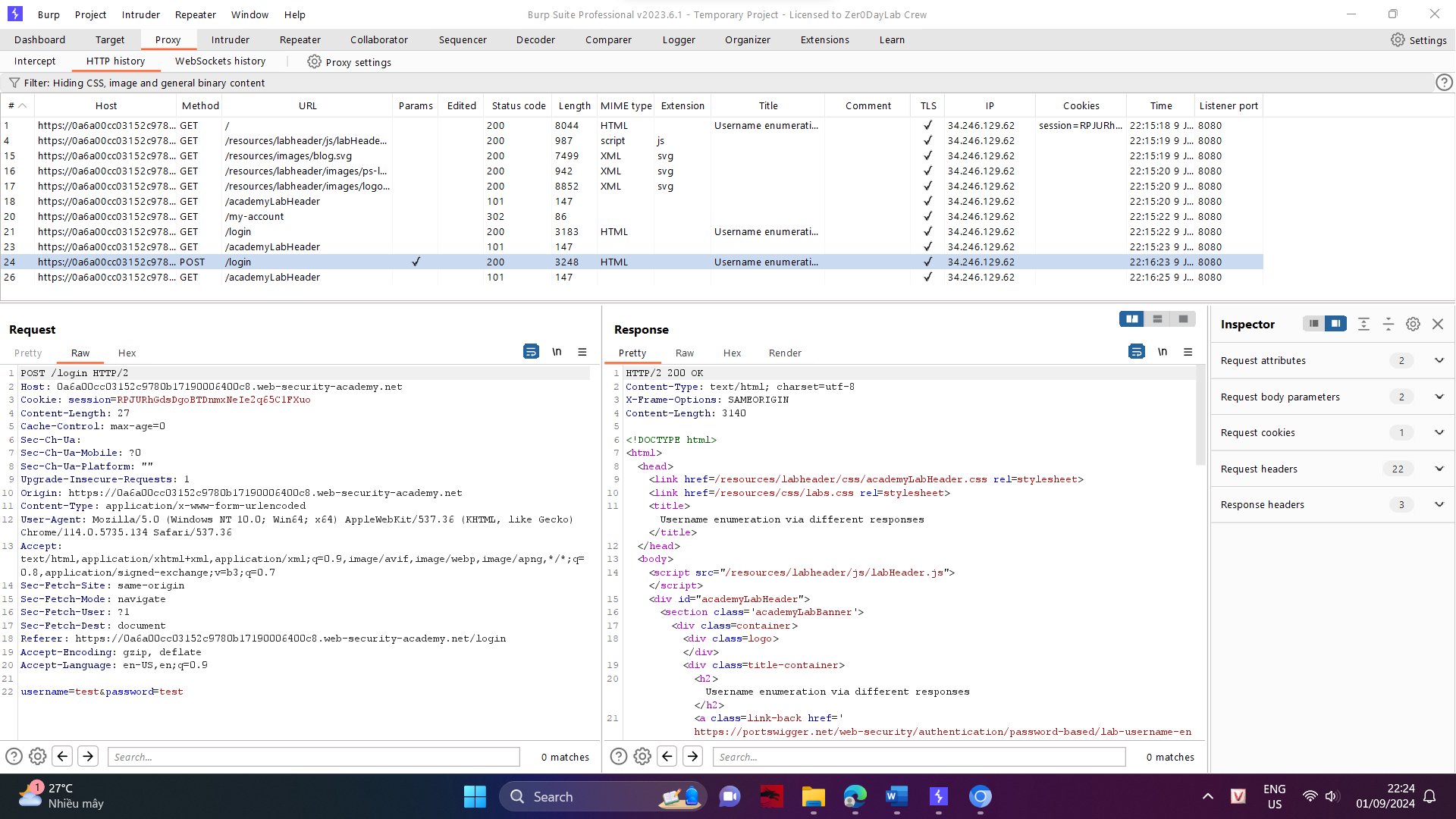
**Giới Thiêu: Trong bài lab này ta sẽ tìm hiểu về lỗ hổng Authentication Vulnerabilities**

## **Source code disclosure via backup files: <**[**HERE**](https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses)**>**

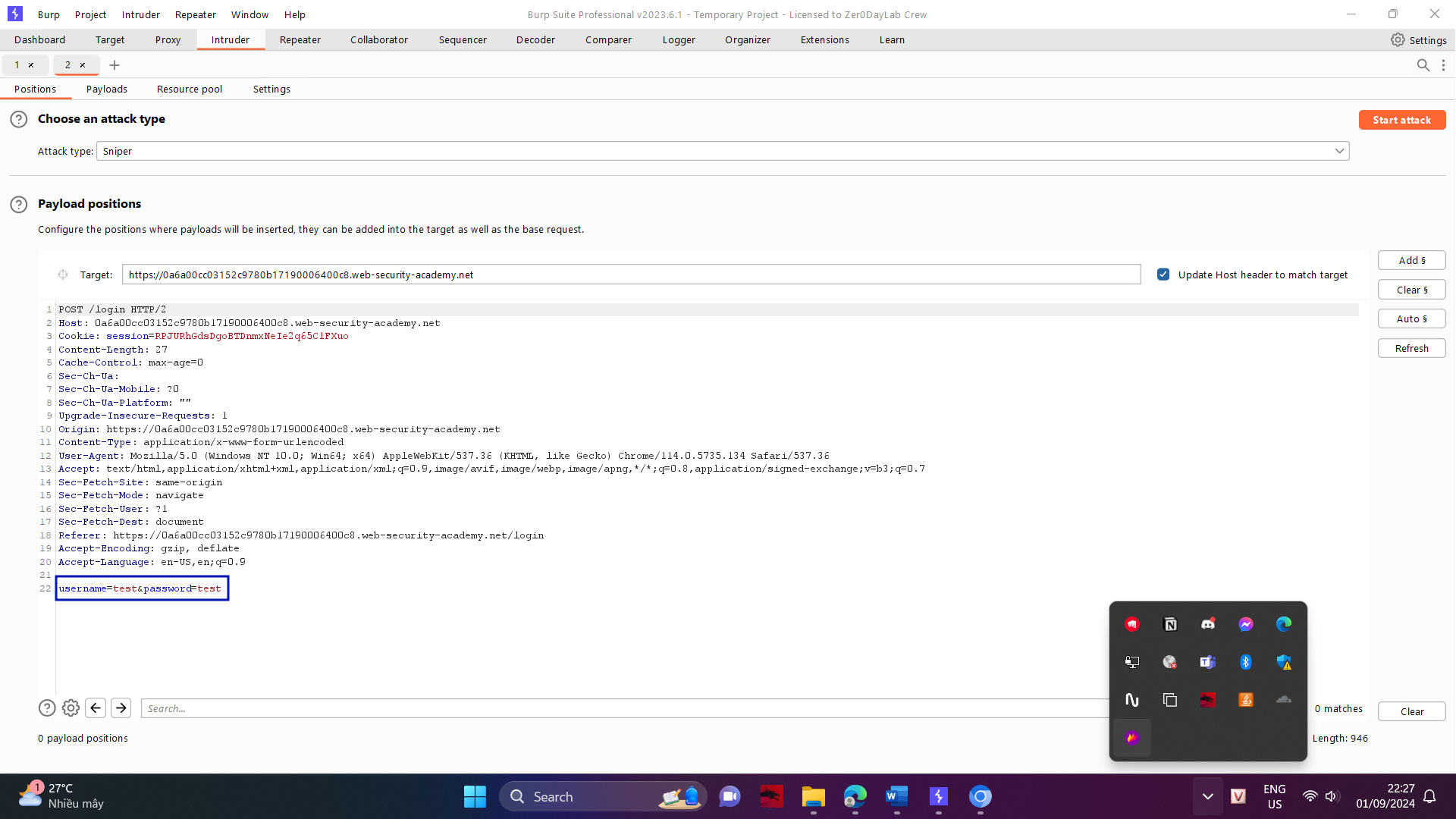
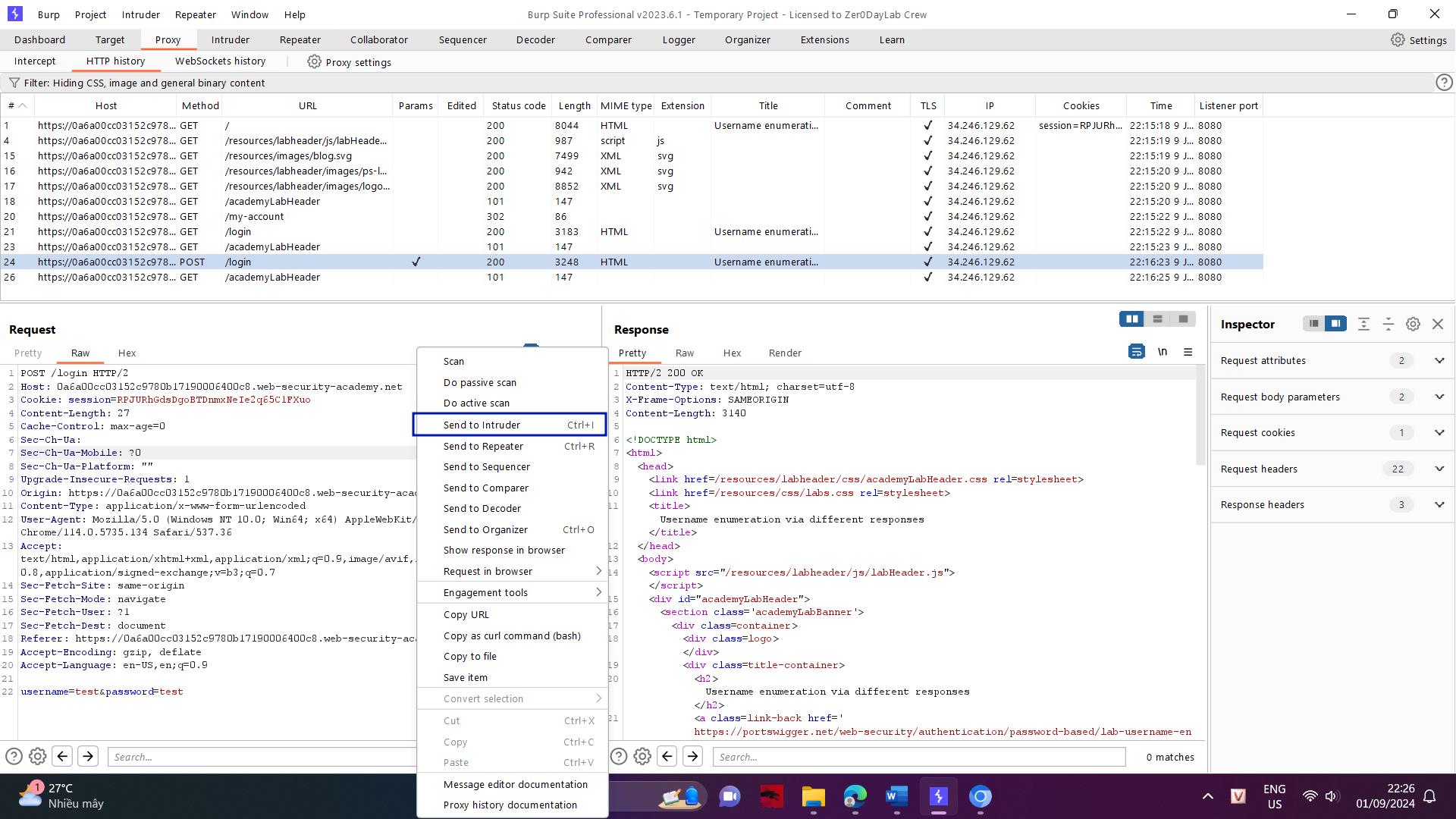


Bước đầu tiên, ta sẽ thử đăng nhập vào bằng một credential ngẫu nhiên để test thử, ở đây em nhập test/test.

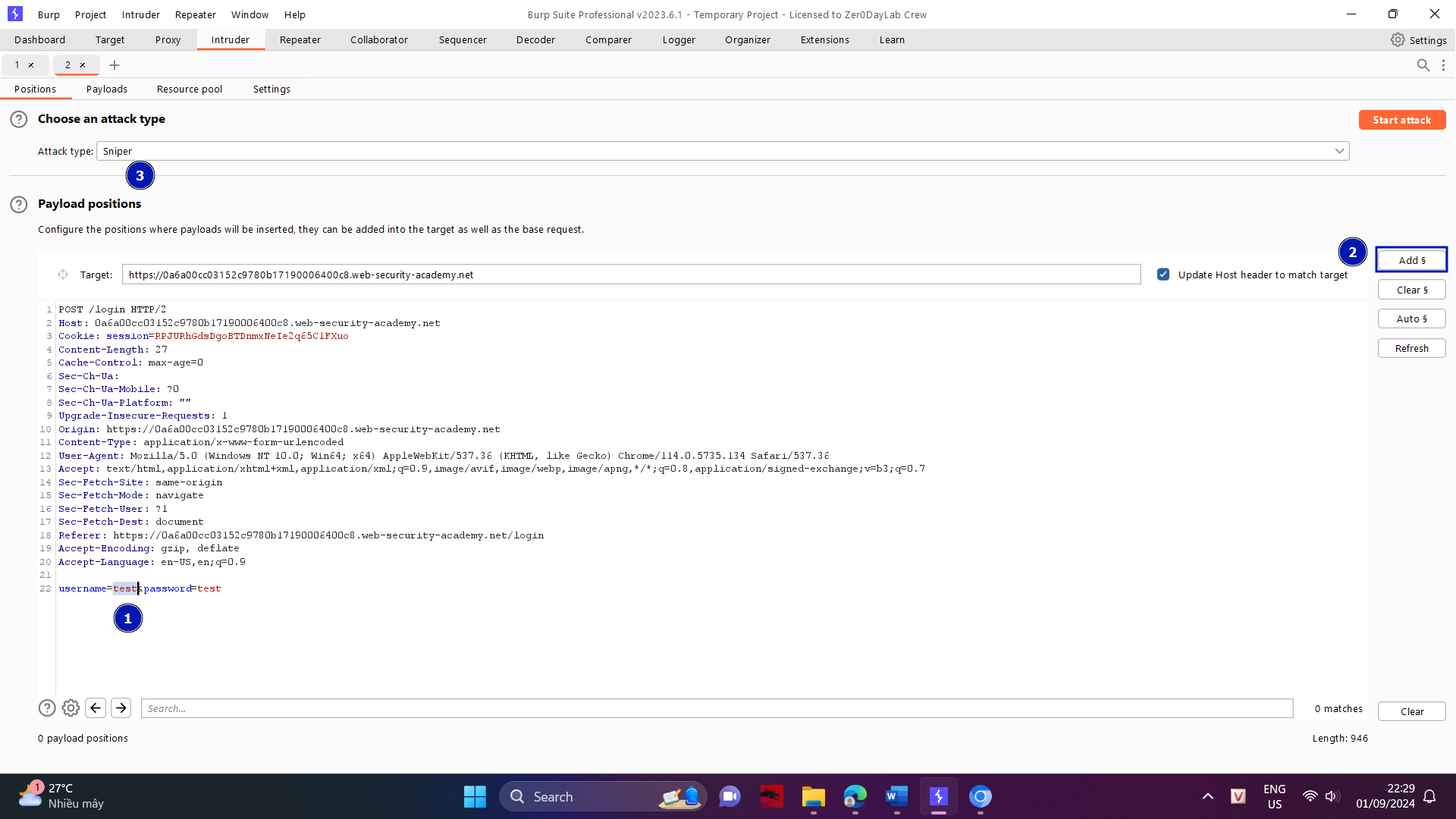
Chuyển qua phần proxy của burpssuite để xem chi tiết request post được gửi đi khi đăng nhập.



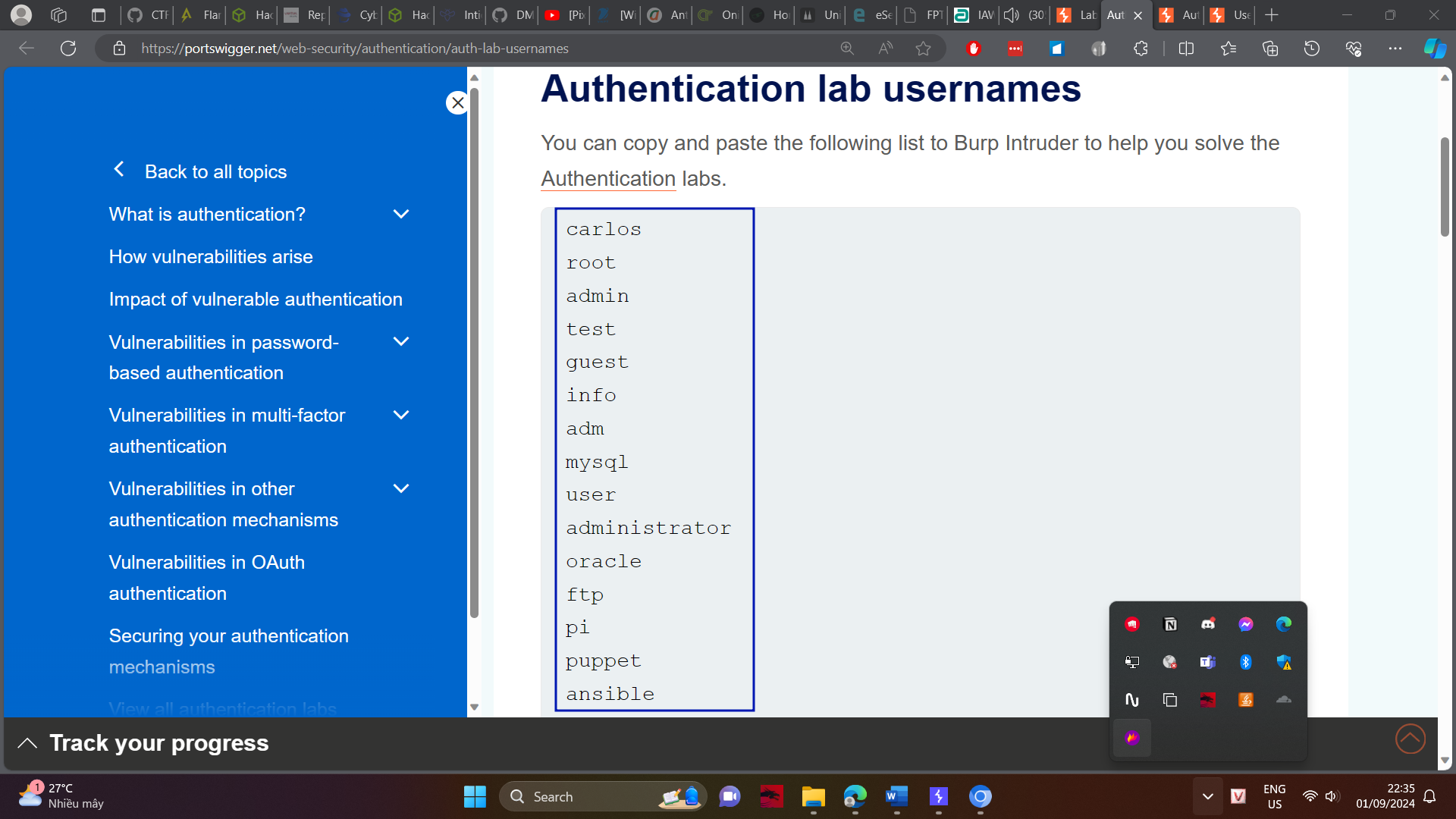
Sau đó ta chuyển request này sang intruder để tiến hành bruteforce.

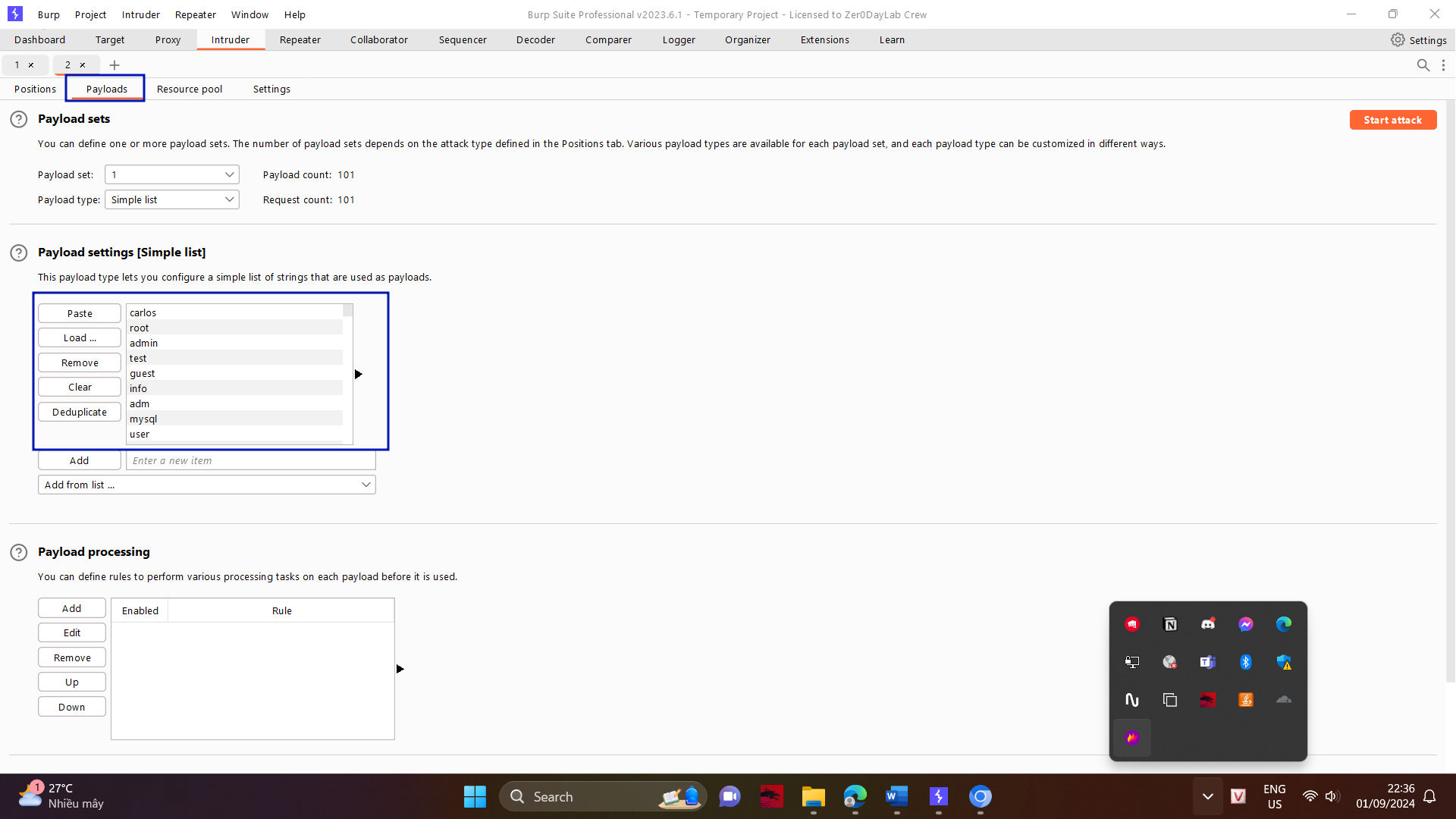


Ta bôi đen phần username để tiến hành bruteforce username, lưu ý để chế độ tấn công là sniper.

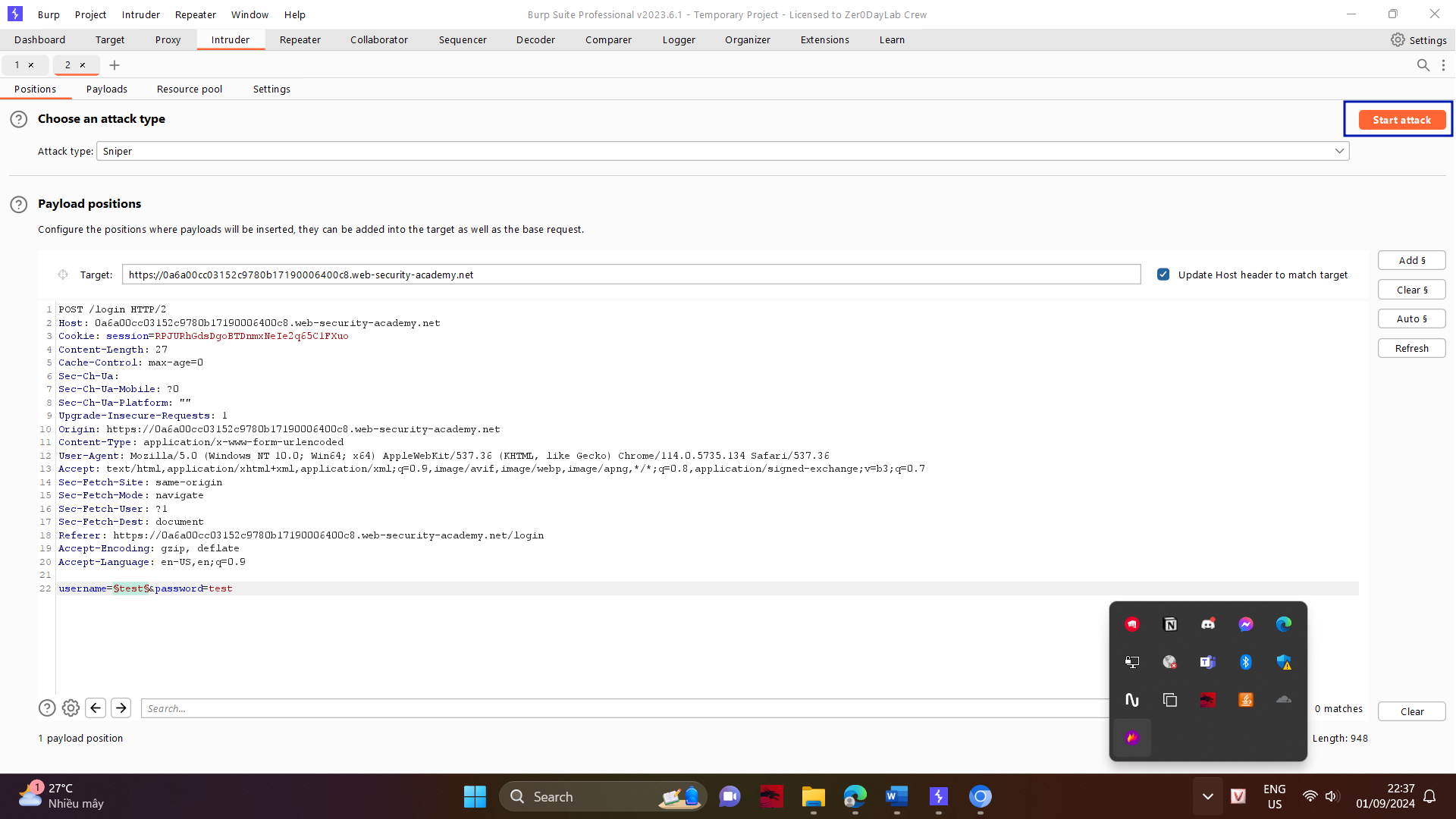


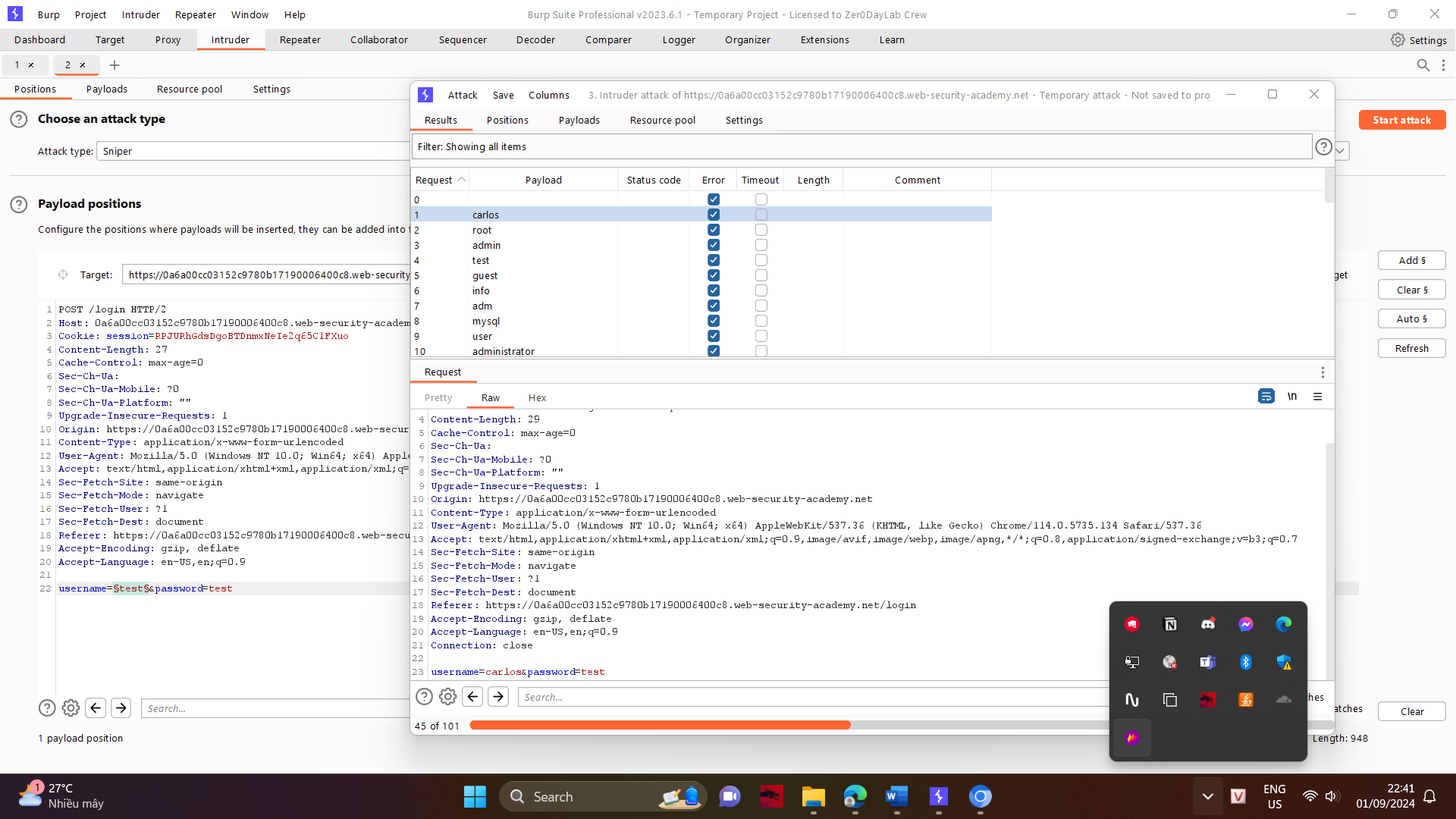
Chọn sang mục payloads và điền wordlist do đề cho sẵn vào.





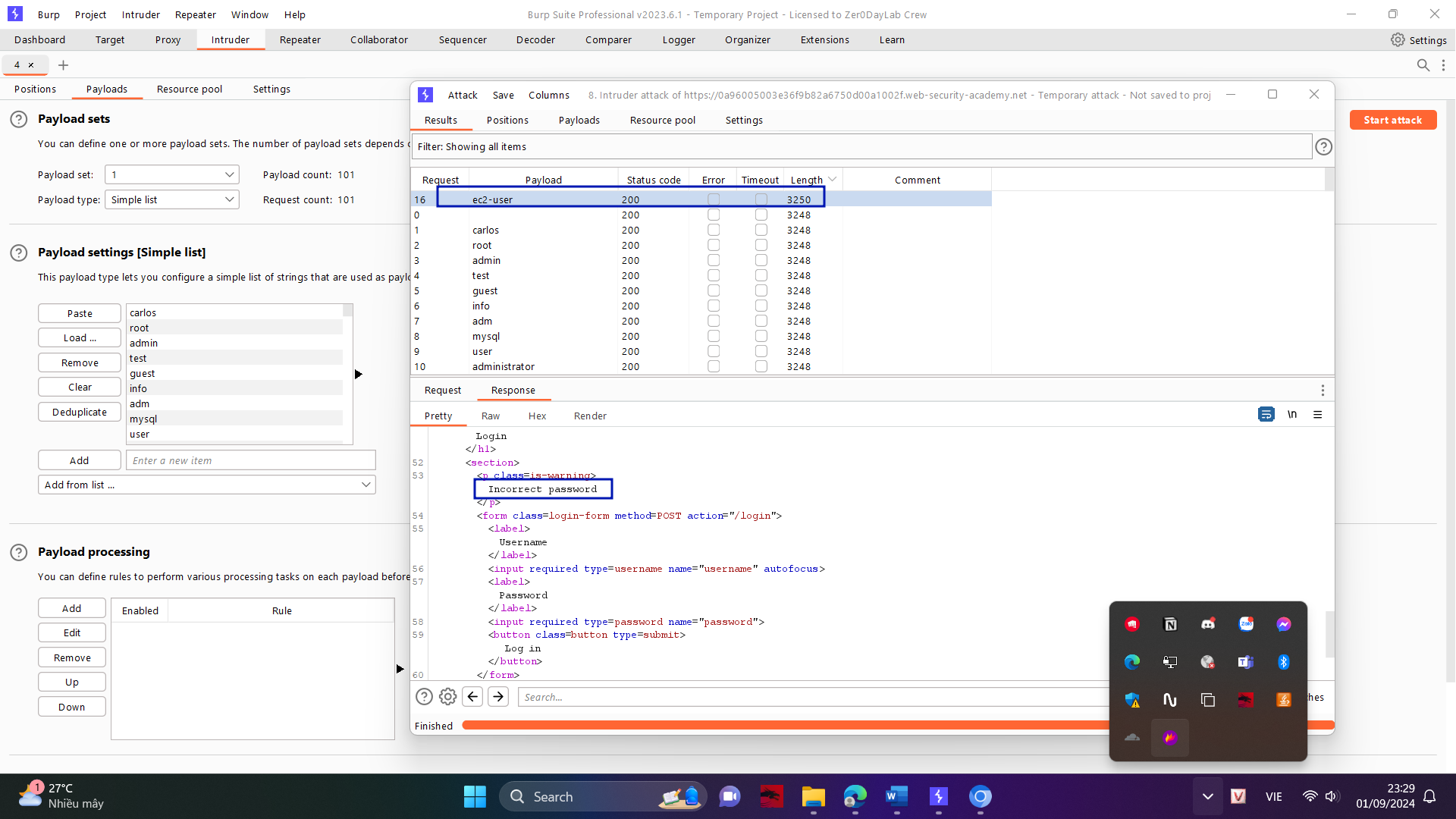
Rồi ta bắt đầu tấn công bằng cách nhấn nút start attack



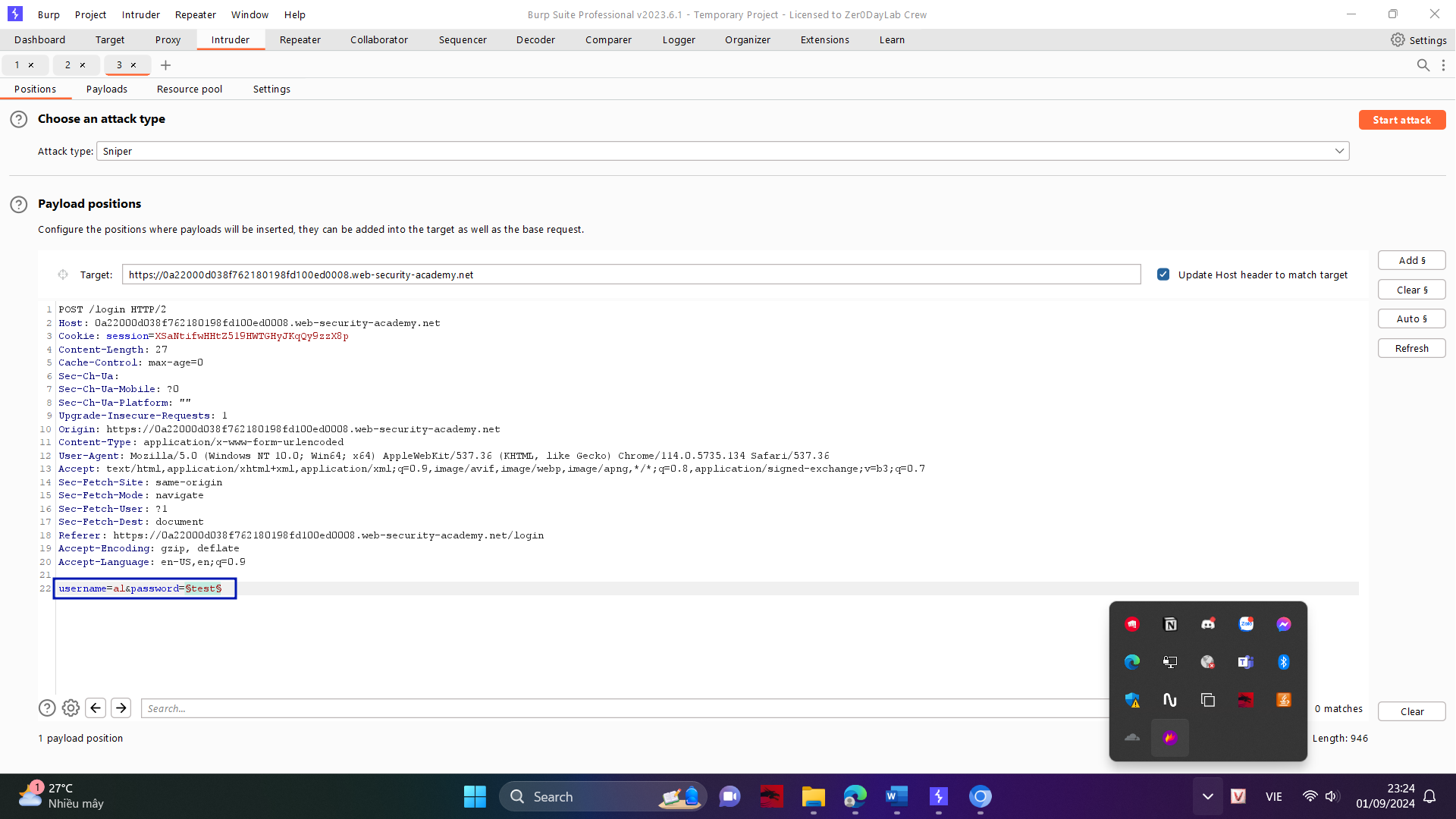


Đây là giao diện màn hình cửa sổ lúc ta đang tấn công username enumerate.

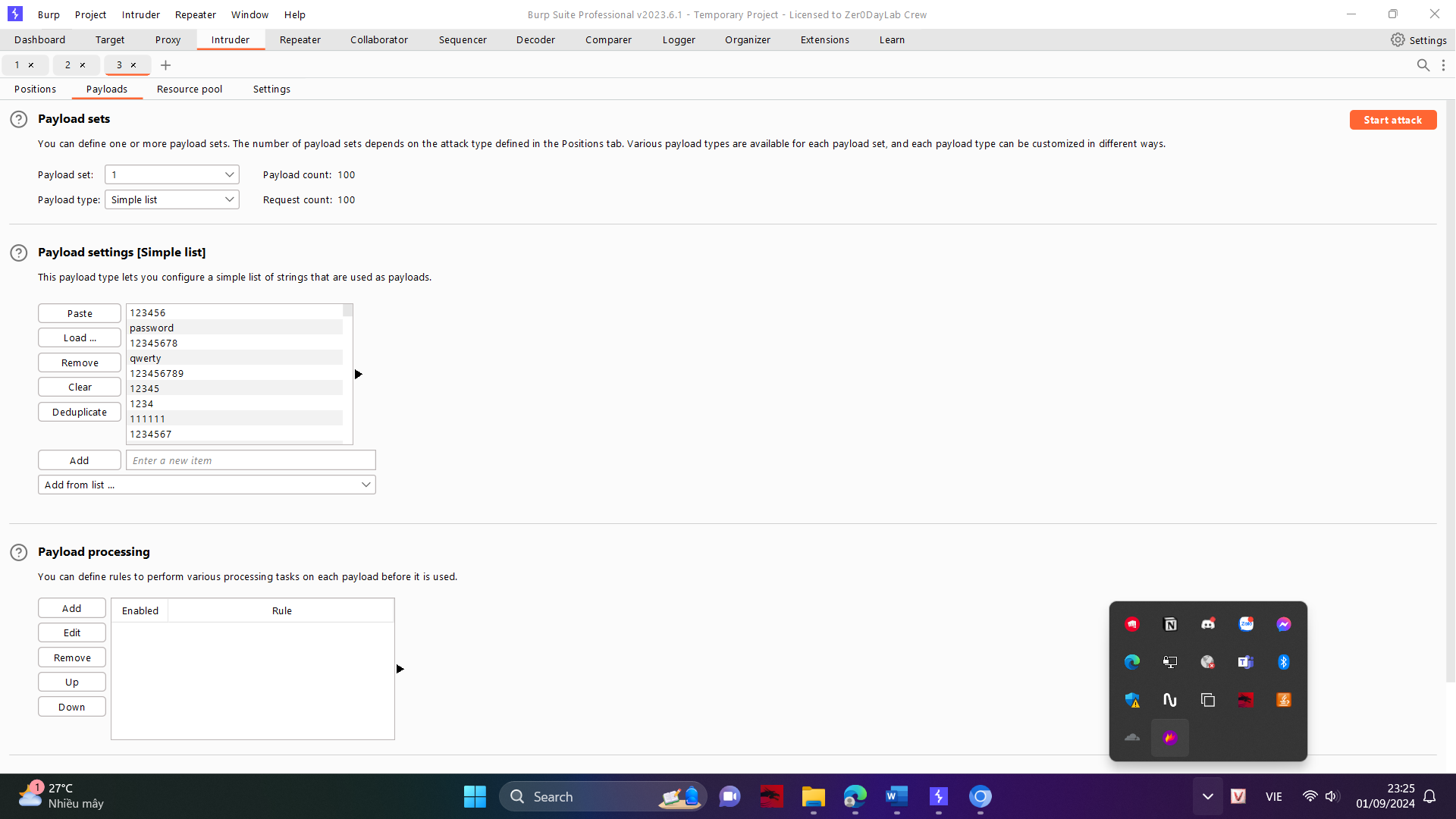
Cuối cùng sau khoảng thời gian chờ đợi. Ta nhận được kết quả 1 request có response độ dài khác những cái còn lại. Chuyển sang xem response thì được thông báo là Invalid password trong khi những response khác thì báo invalid username => Đây là username đúng.



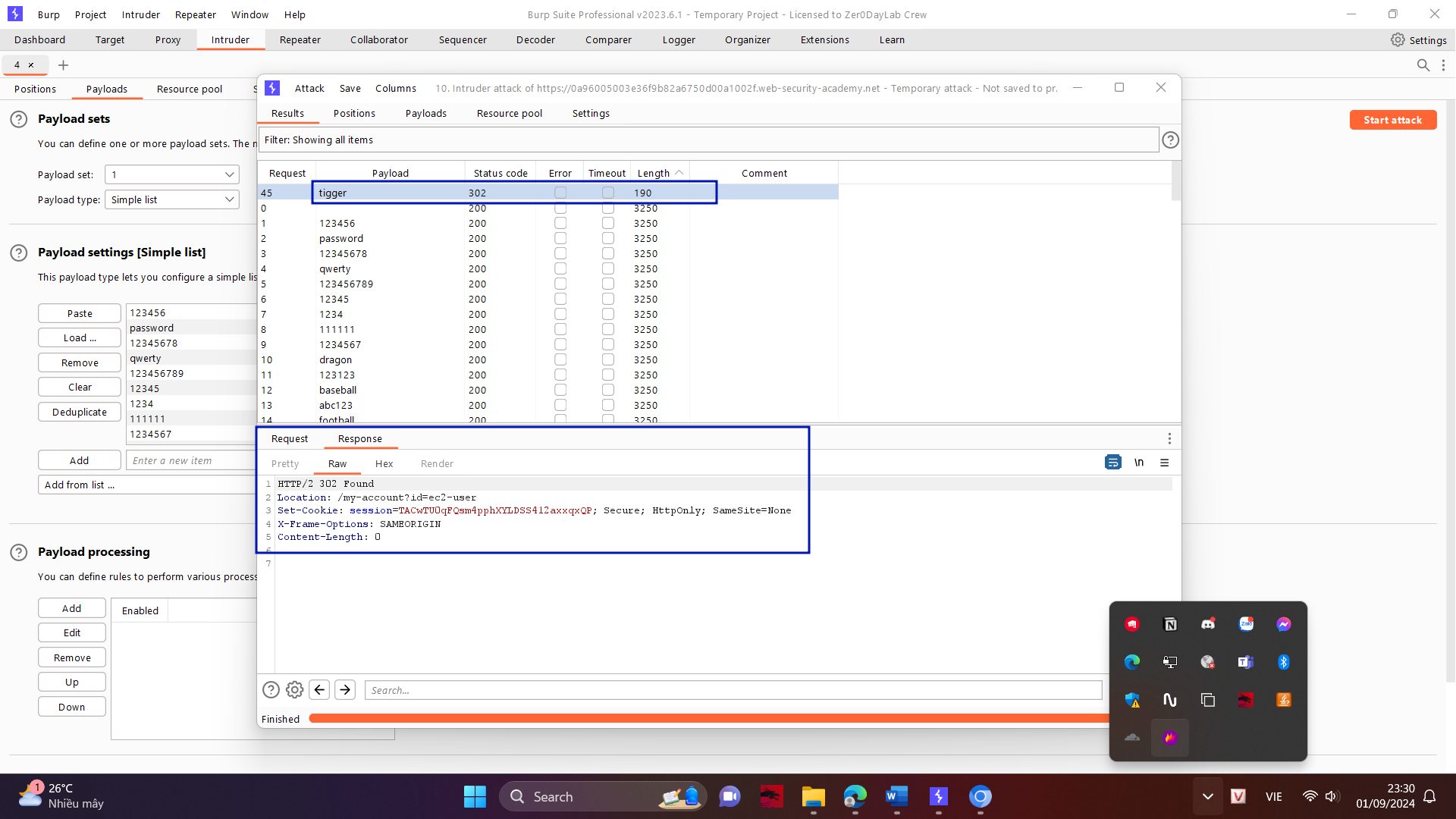
Tới bước này ta đã tìm ra được username đúng nên việc làm tiếp theo là tìm ra password đúng. Ta sửa lại như sau.



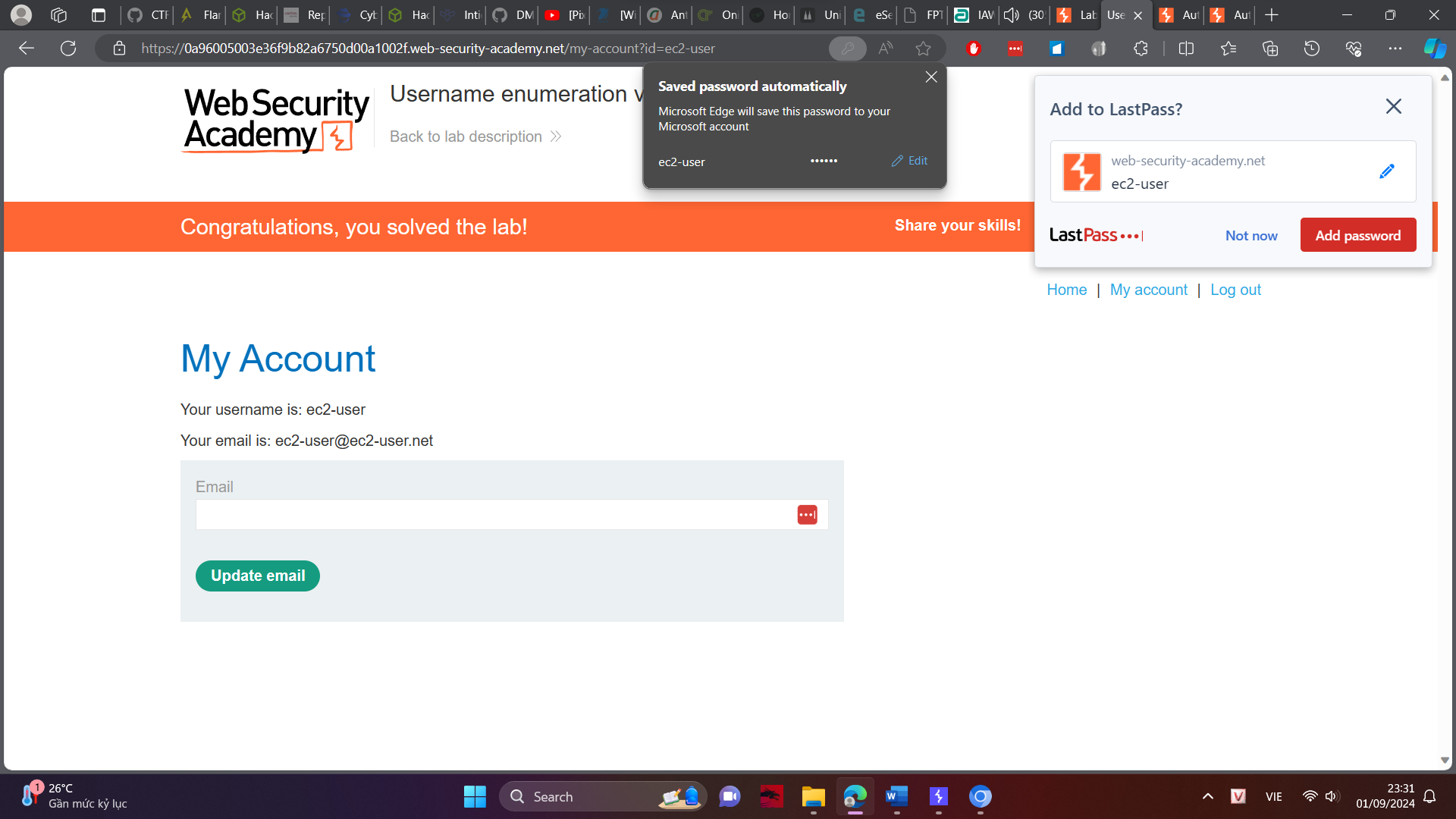
Đồng thời cập nhật danh sách wordlist lại mới.



Vậy password đúng của chúng ta là tigger



Tiến hành đăng nhập thử vào hệ thống.

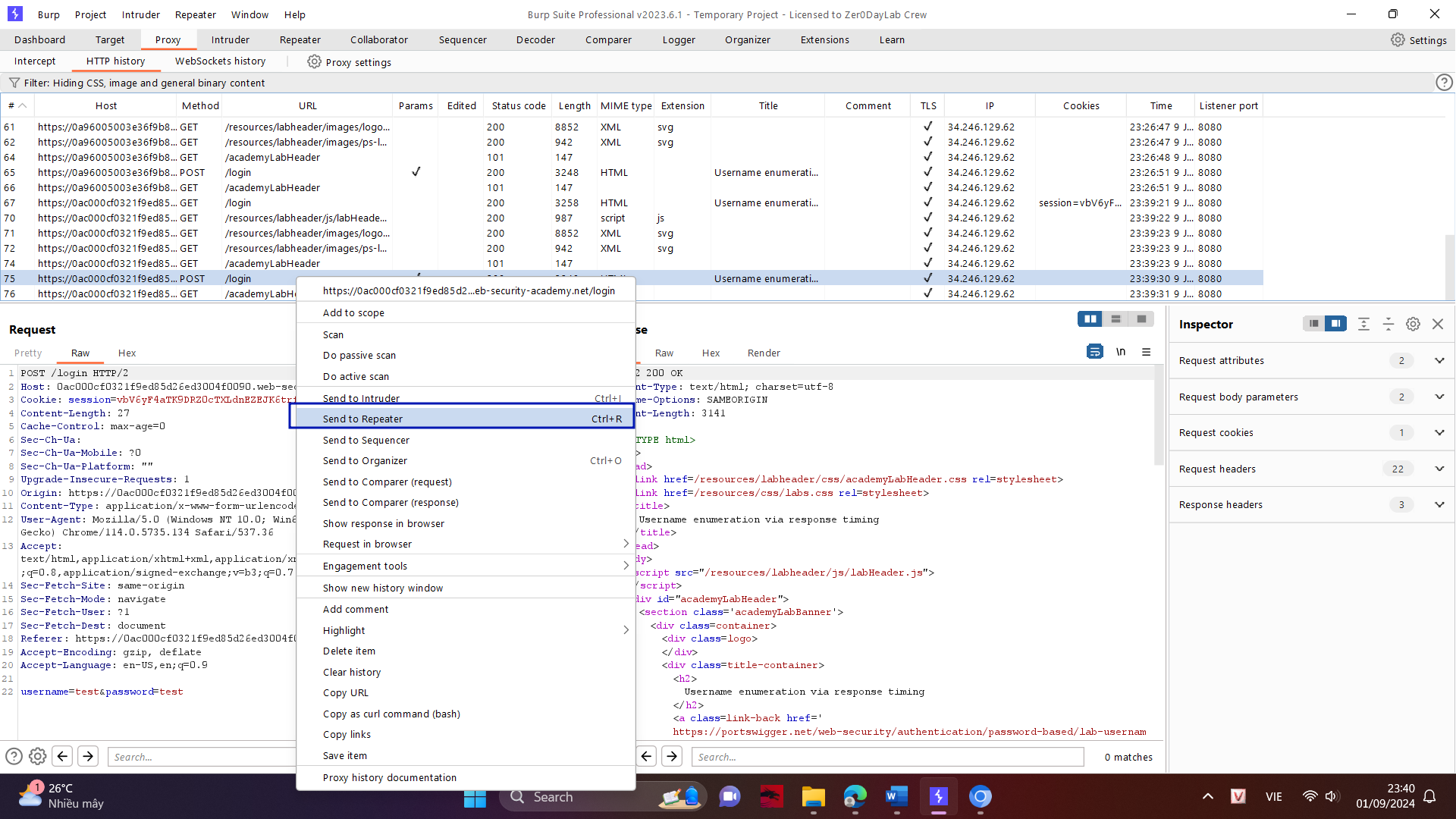


Vậy là ta đã xong bài lab đầu tiên rồi.

## **Information disclosure in version control history: <**[**HERE**](https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-response-timing)**>**

Ta tiếp tục với một phiên bản nâng cấp hơn cảu loại lỗ hổng này.

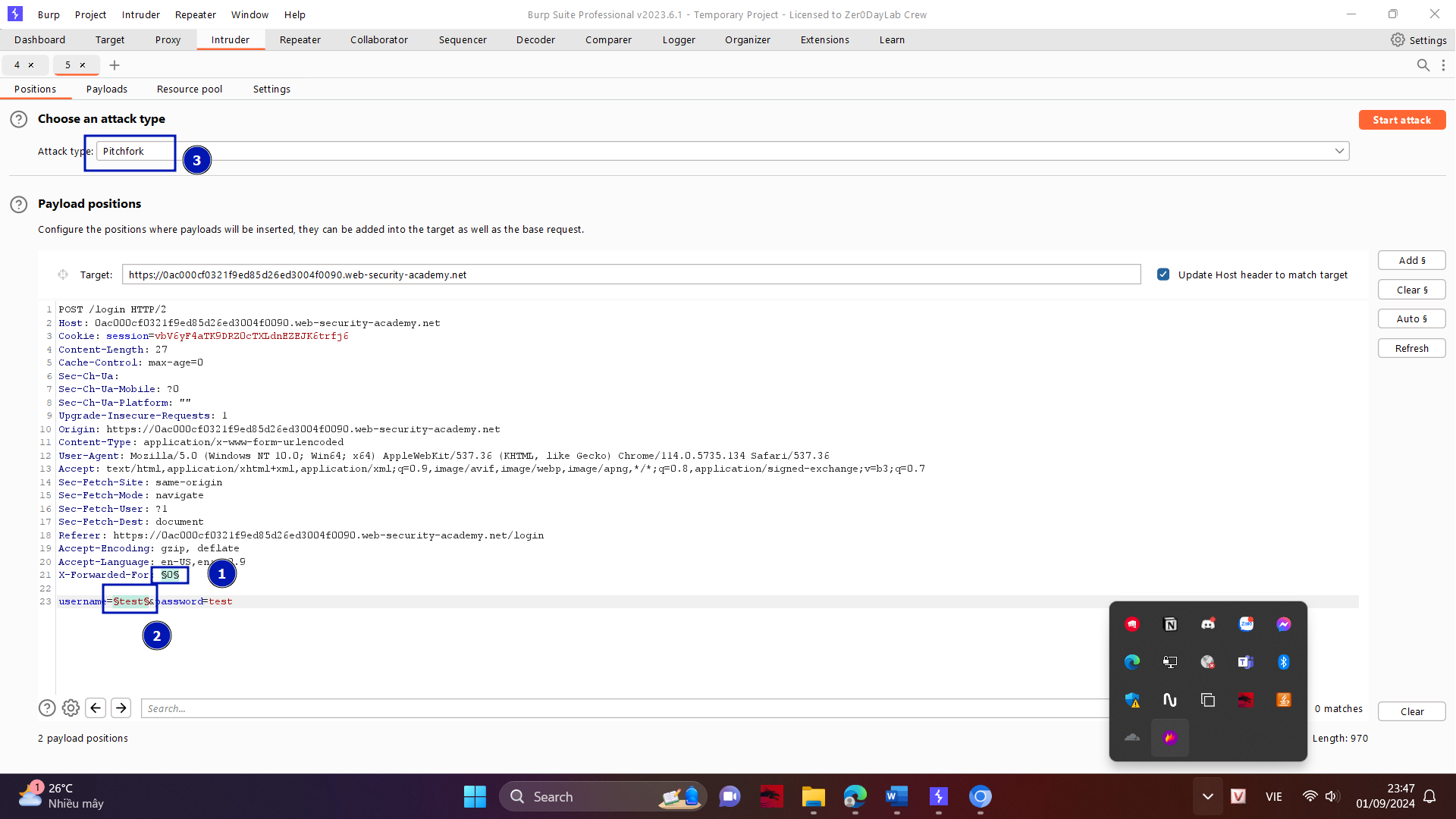
Lần này ta chuyển qua repeater trước.



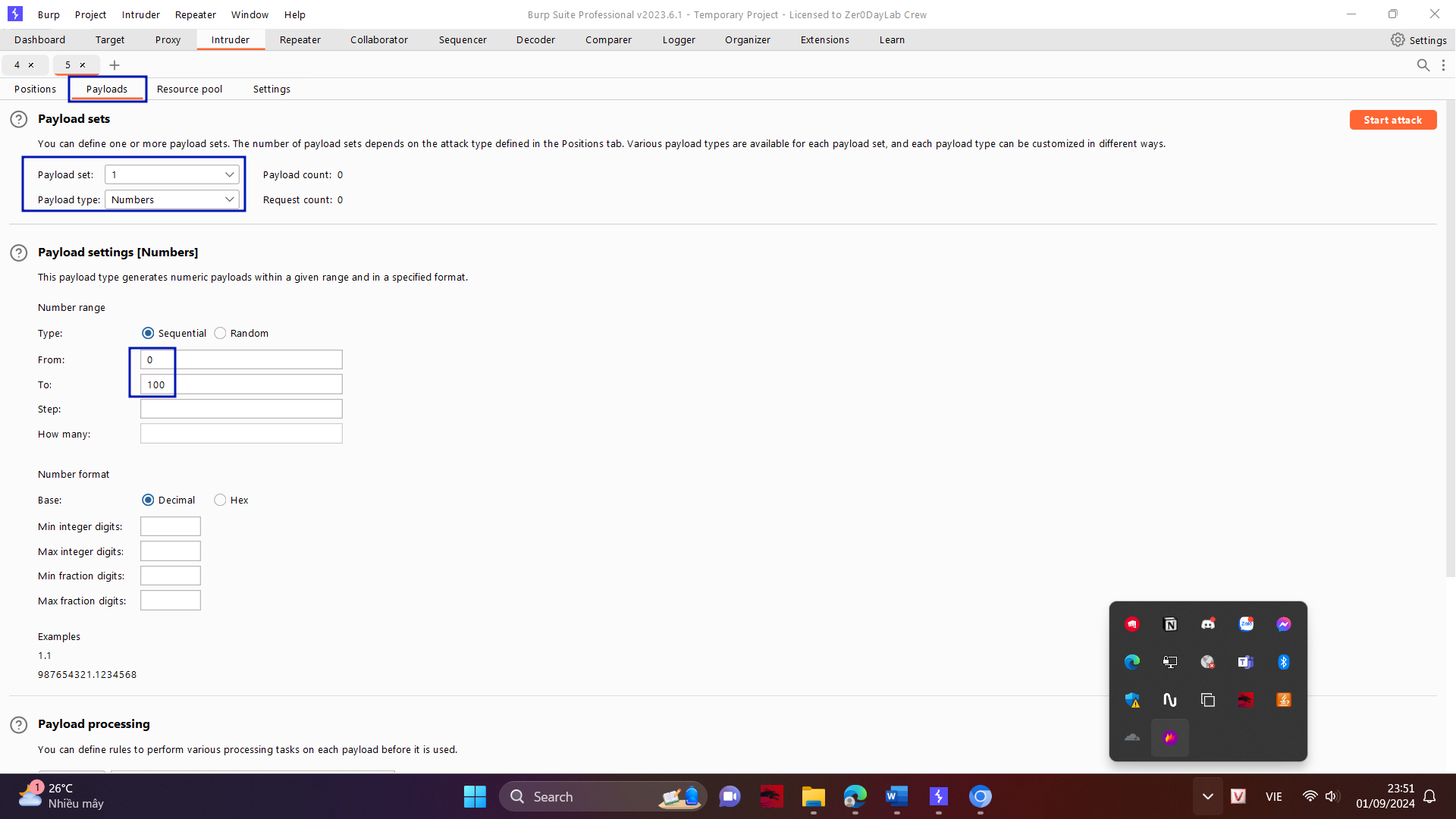
Tiếp tục thử nghiệm với tên người dùng và mật khẩu. Chú ý đặc biệt đến thời gian phản hồi. Lưu ý rằng khi tên người dùng không hợp lệ, thời gian phản hồi gần như giống nhau. Tuy nhiên, khi bạn nhập một tên người dùng hợp lệ (của bạn), thời gian phản hồi tăng lên tùy thuộc vào độ dài của mật khẩu bạn đã nhập.

Xác định rằng tiêu đề X-Forwarded-For được hỗ trợ, cho phép bạn làm giả địa chỉ IP và vượt qua bảo vệ chống tấn công brute-force dựa trên địa chỉ IP.

Ta đổi sang chế độ intruder để tiến hành brute force.

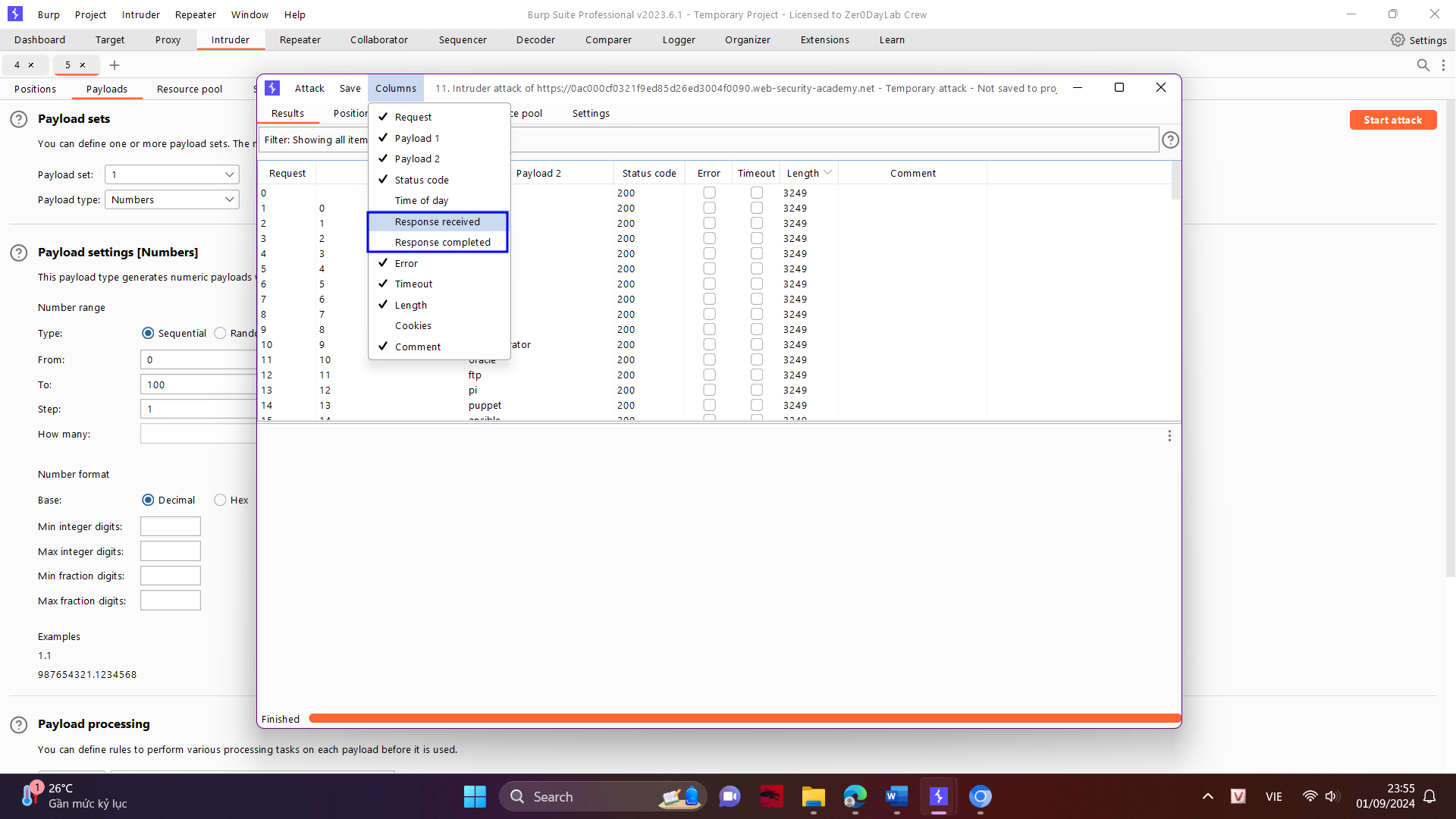


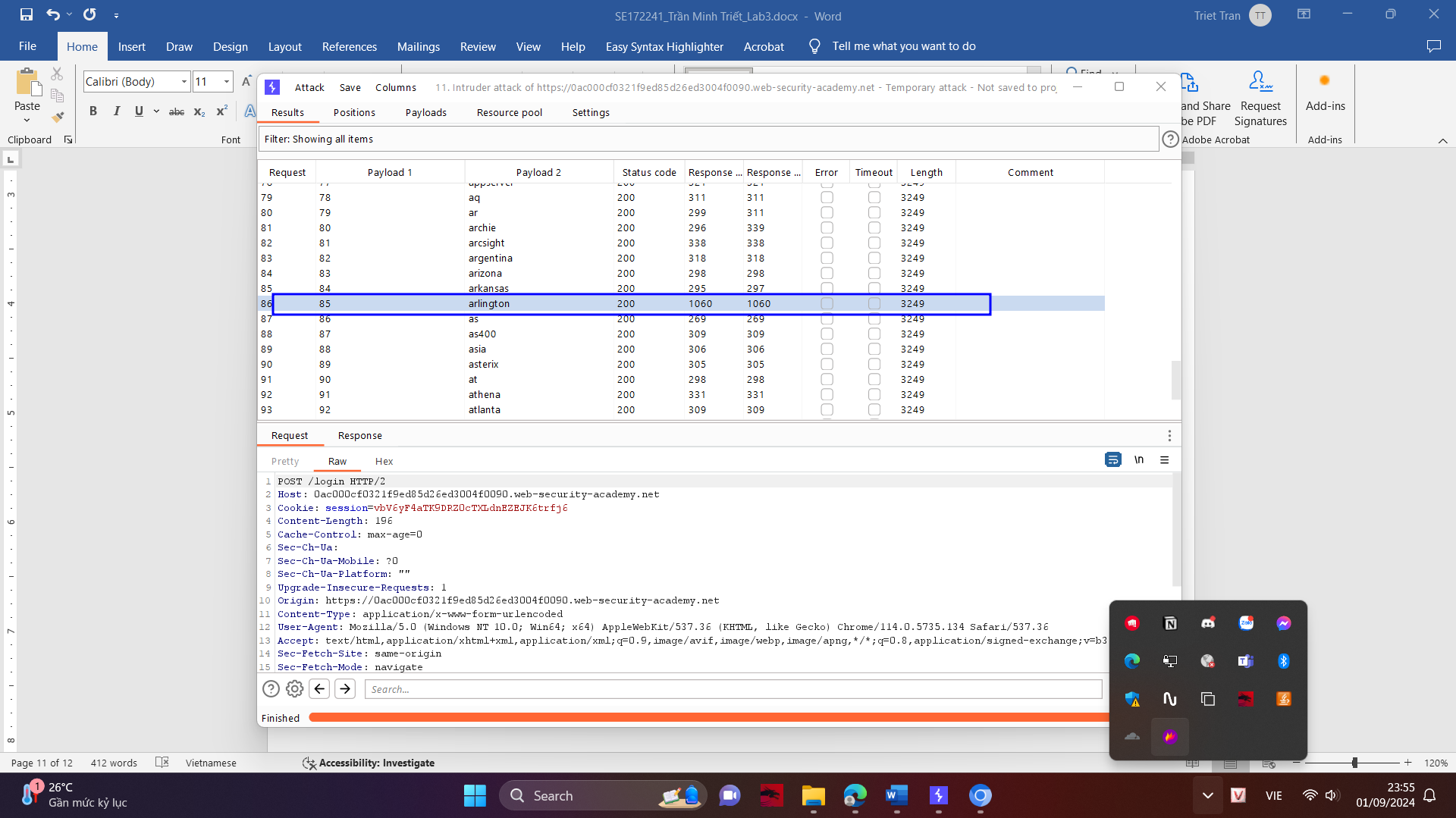
Chuyển sang phần payload để config





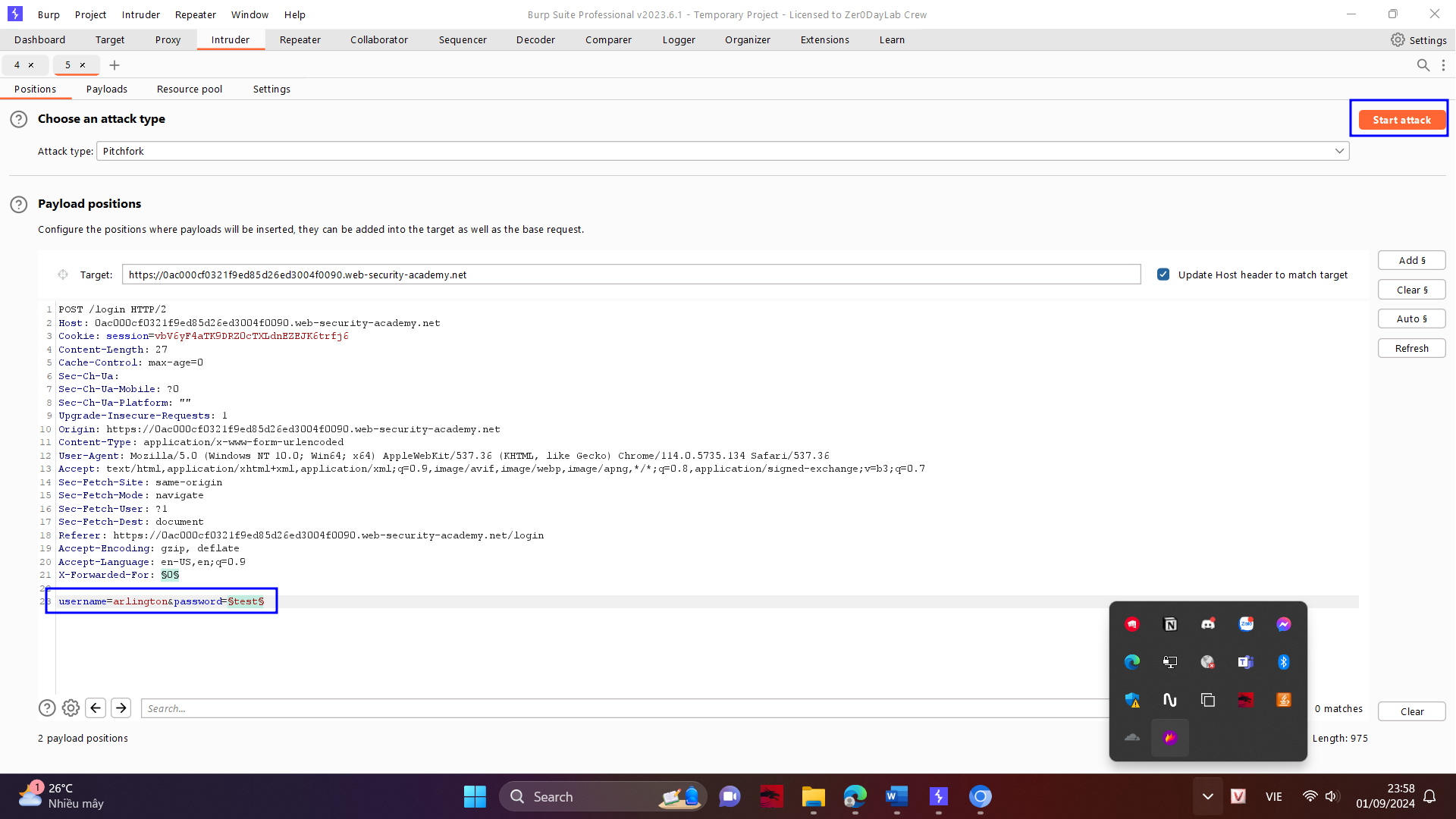
Chỉnh password thật là dài, kế tiếp bắt đầu tấn công.

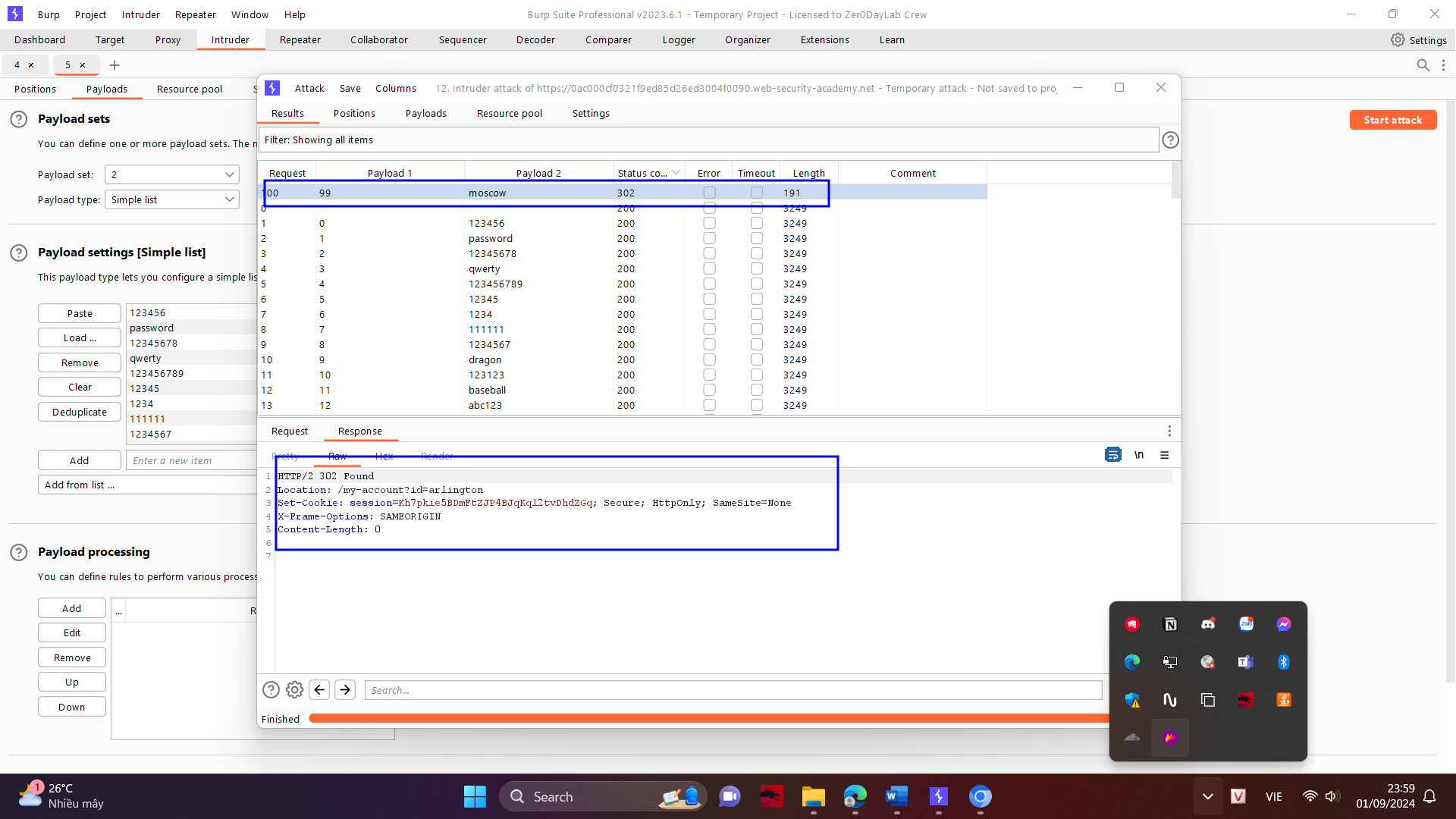




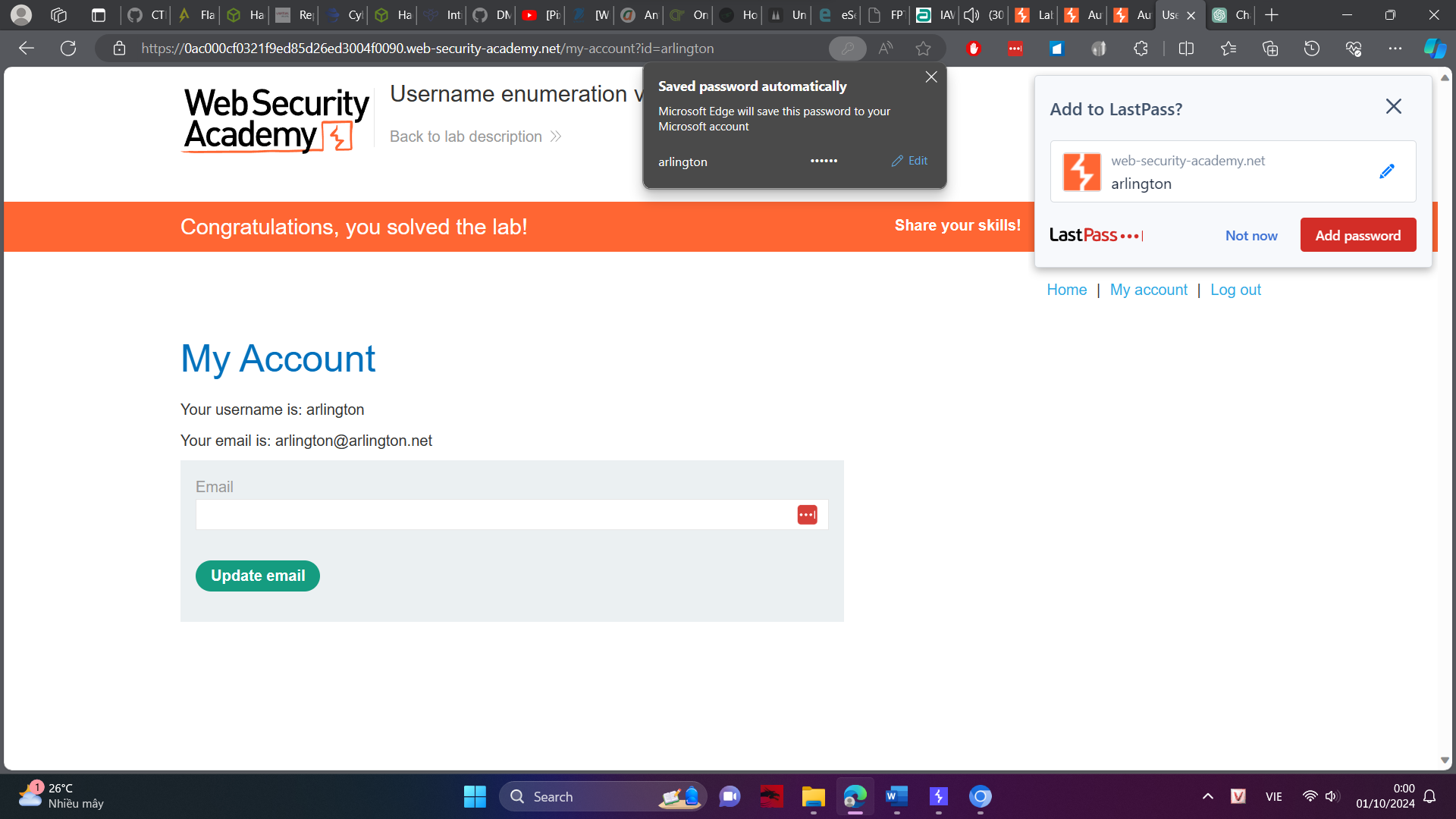
Trong số các kết quả thì arlington trả về thời gian lâu nhất nên nó là username ta cần tìm.

Bây giờ ta sẽ tiến hành bruteforce password như cũ.





Trong số các response thì có duy nhất password moscow là có response code 302 nên đây là password đúng.



Vậy là ta đã xong bài lab này rồi.

**---END---**