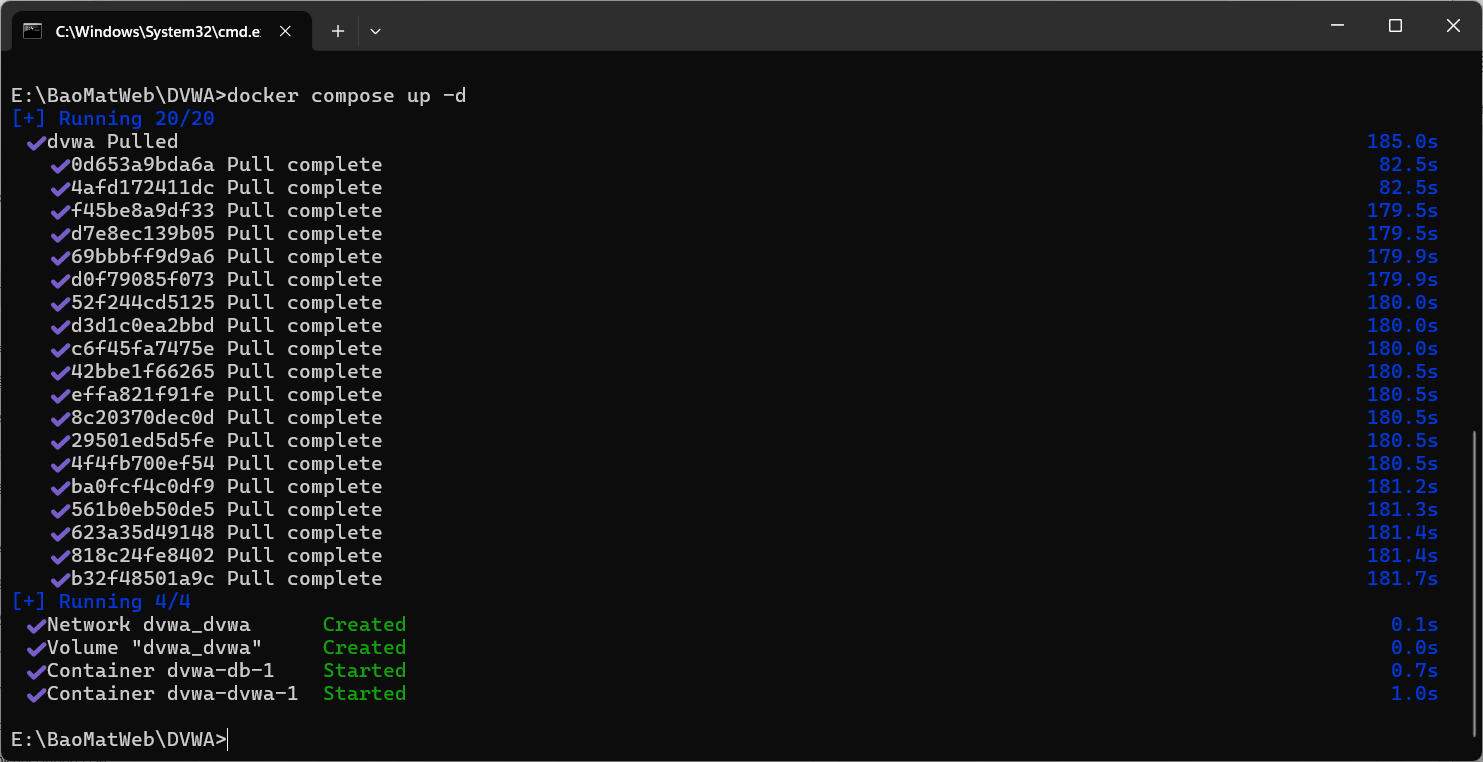
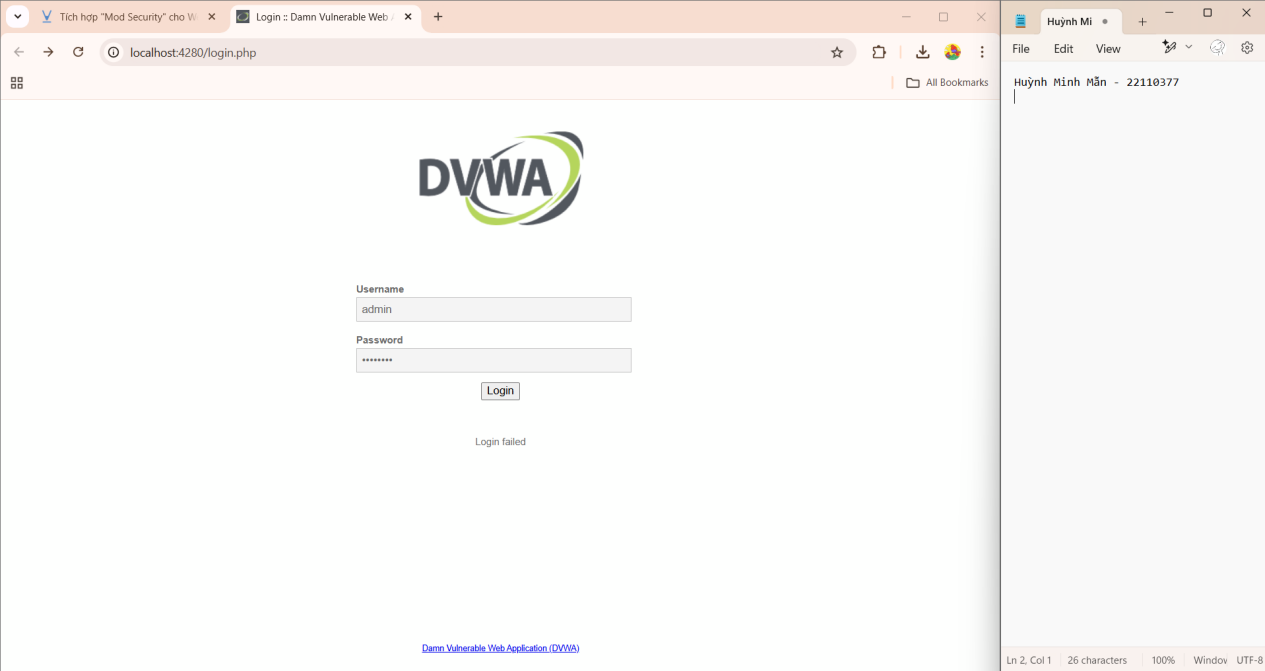
**Mod Security - Tích hợp "Mod Security" cho Web Application Server để chống lại SQL Injection, tấn công XSS**

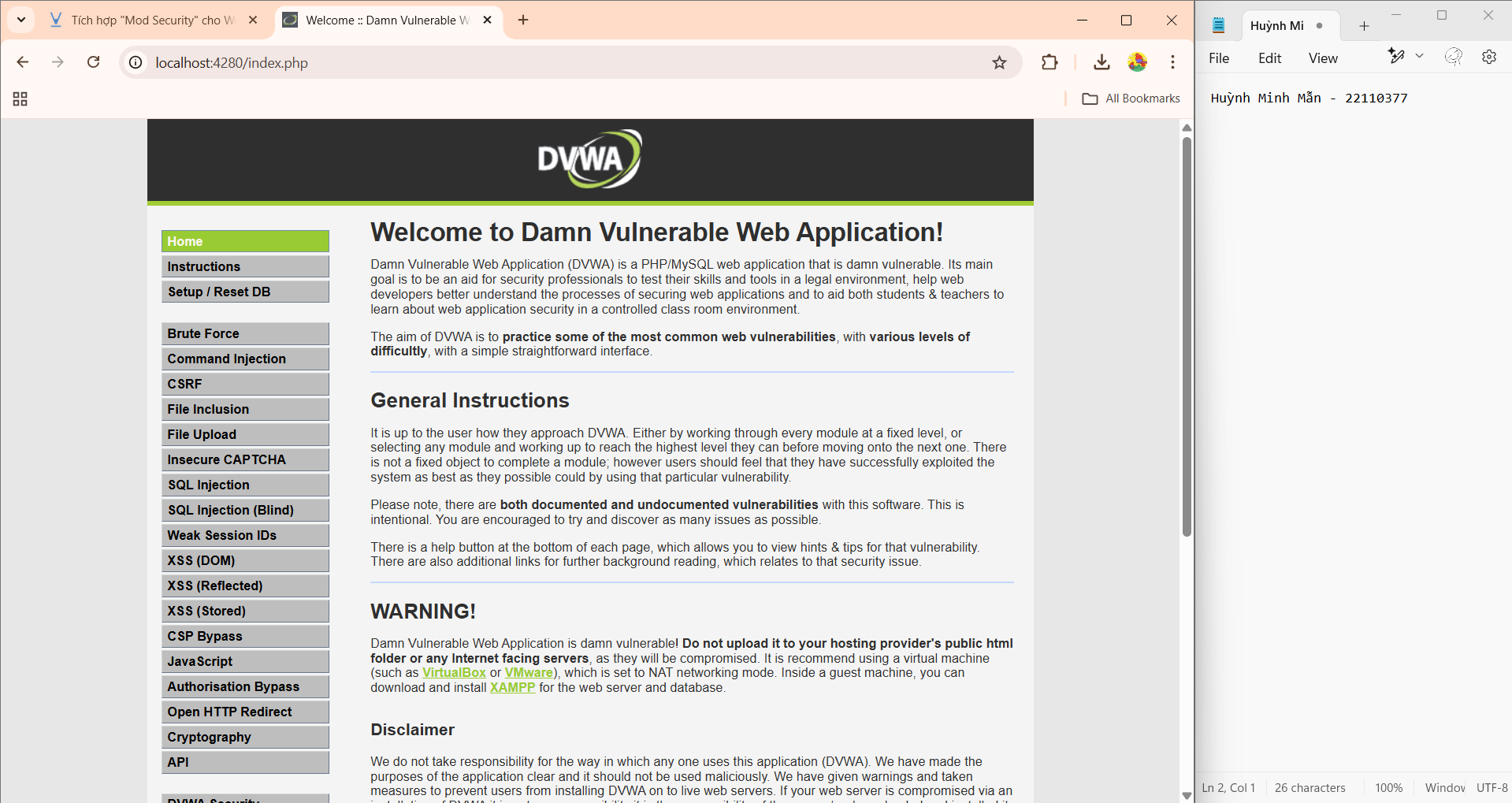
1. **SQL Injection và tấn công XSS khi chưa tích hợp Mod Security**

Vào Link github: <https://github.com/ethicalhack3r/DVWA> clone về, sau đó trỏ vào thư mục DVWA, mở cmd lên và nhập docker compose up -d

 Sau đó lên web gõ vào thanh url: <http://localhost:4280> để mở ra giao diện DVWA

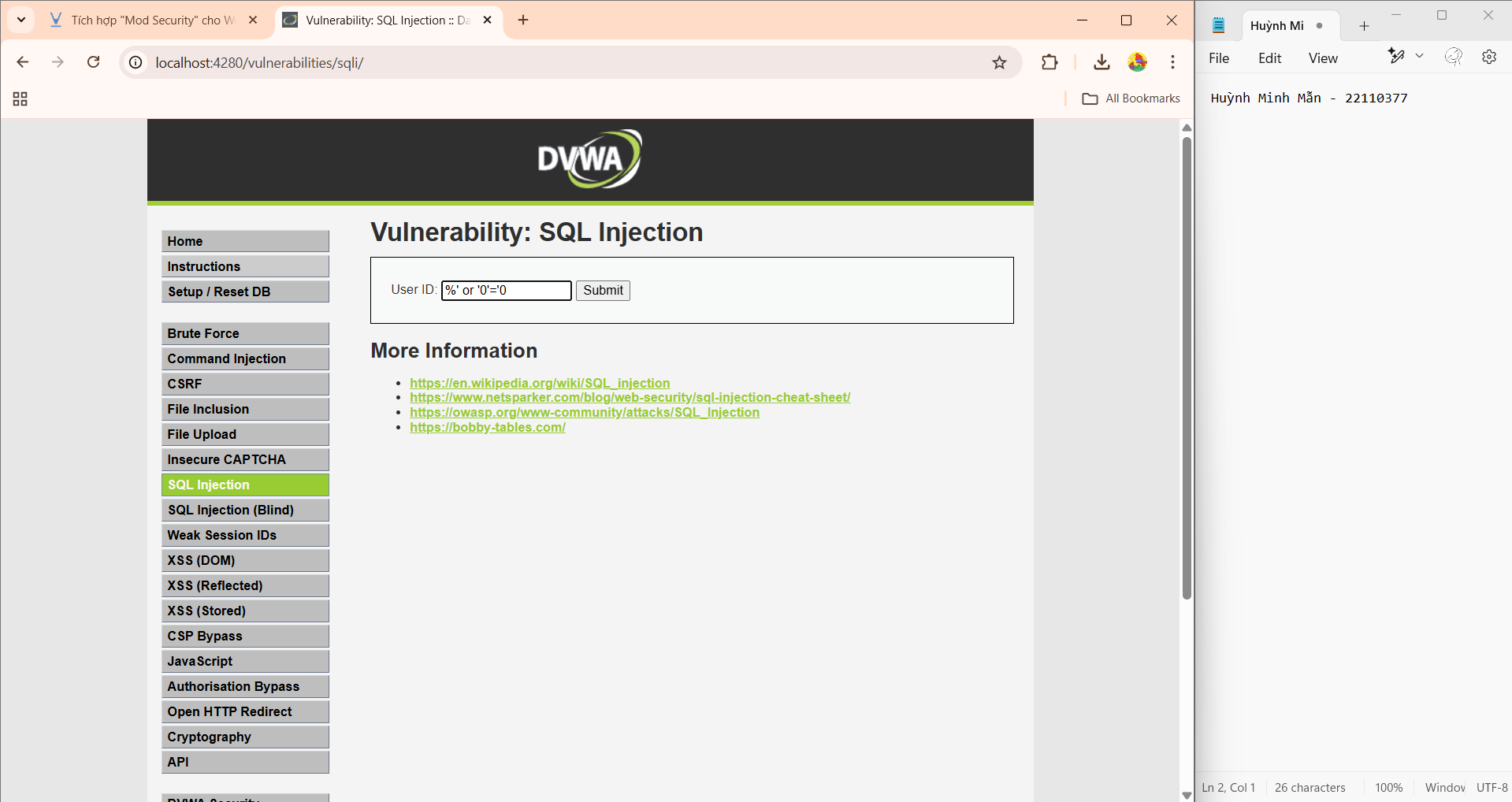


Nhập username/password là admin/password để tiến hành đăng nhập, một giao diện sẽ mở ra như sau:

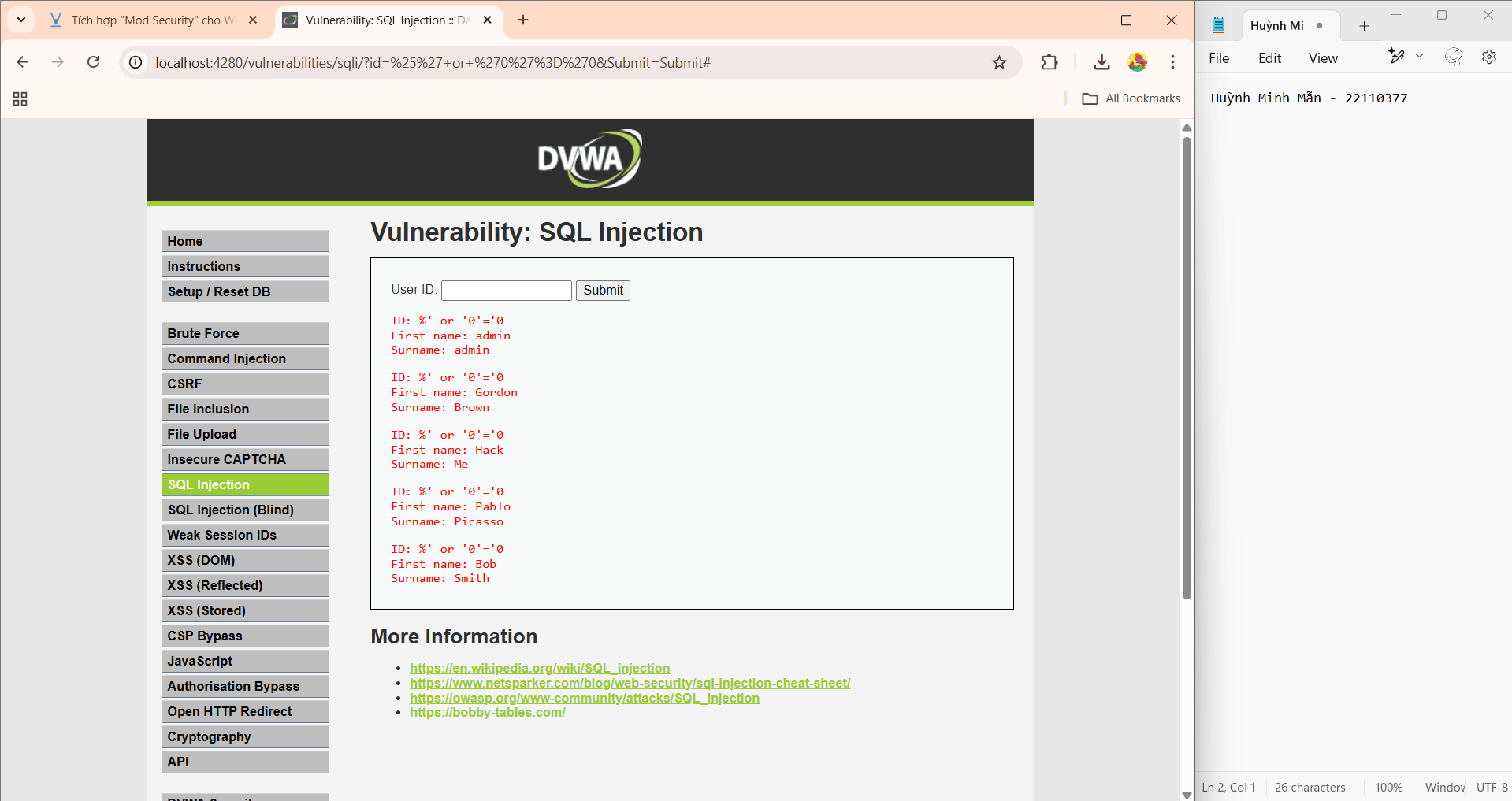


1. **Thử nghiệm SQL Injection**

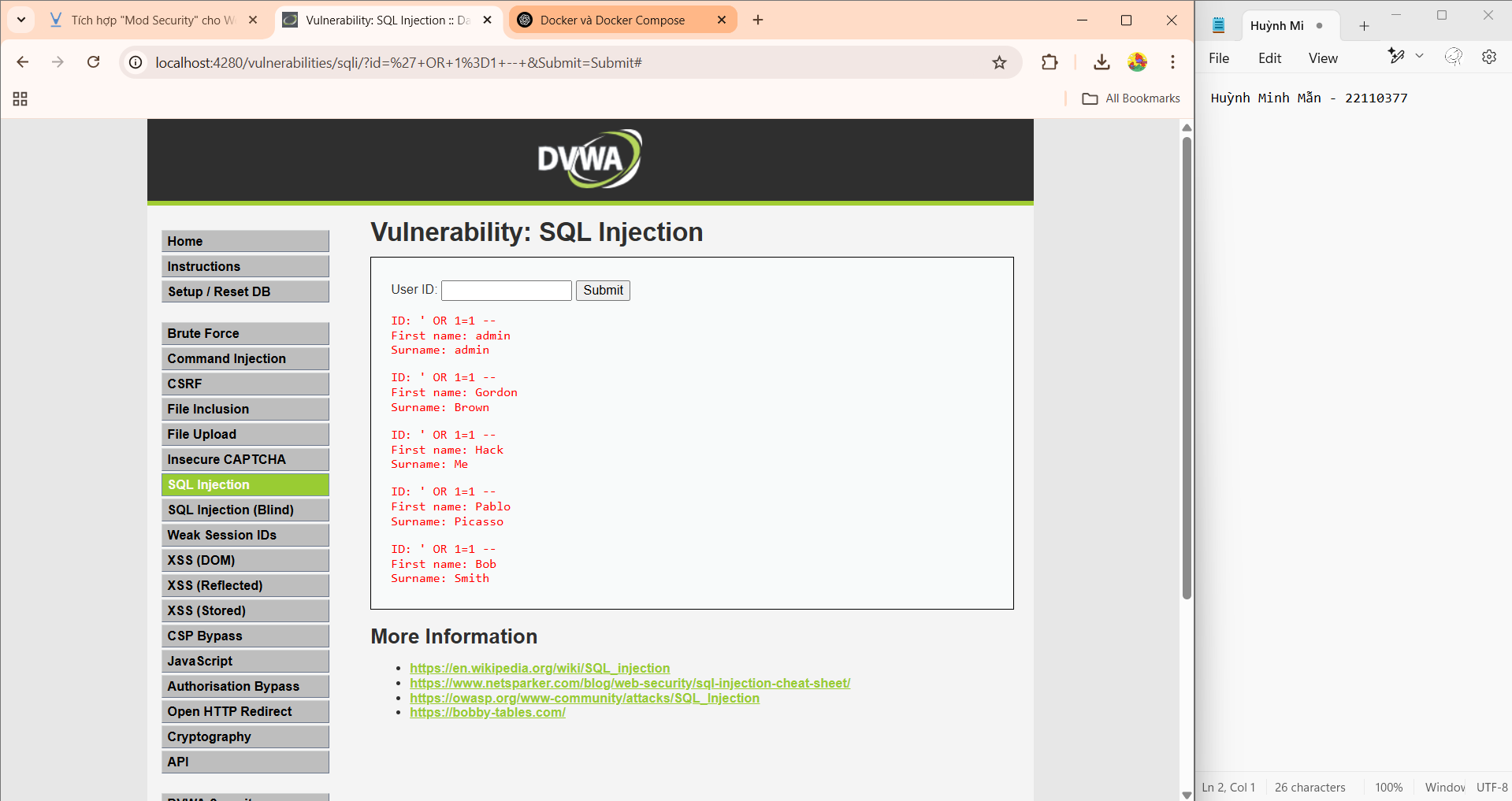
Vào SQL Injection, đến thanh nhập User ID và nhập vào %' or '0'='0, ấn button submit.



Kết quả sẽ nhận được thông tin của tất cả các users có trong cơ sở dữ liệu. Bởi vì câu truy vấn lúc này được hiểu là : SELECT \* FROM users WHERE user\_id = '%' or '0'='0'

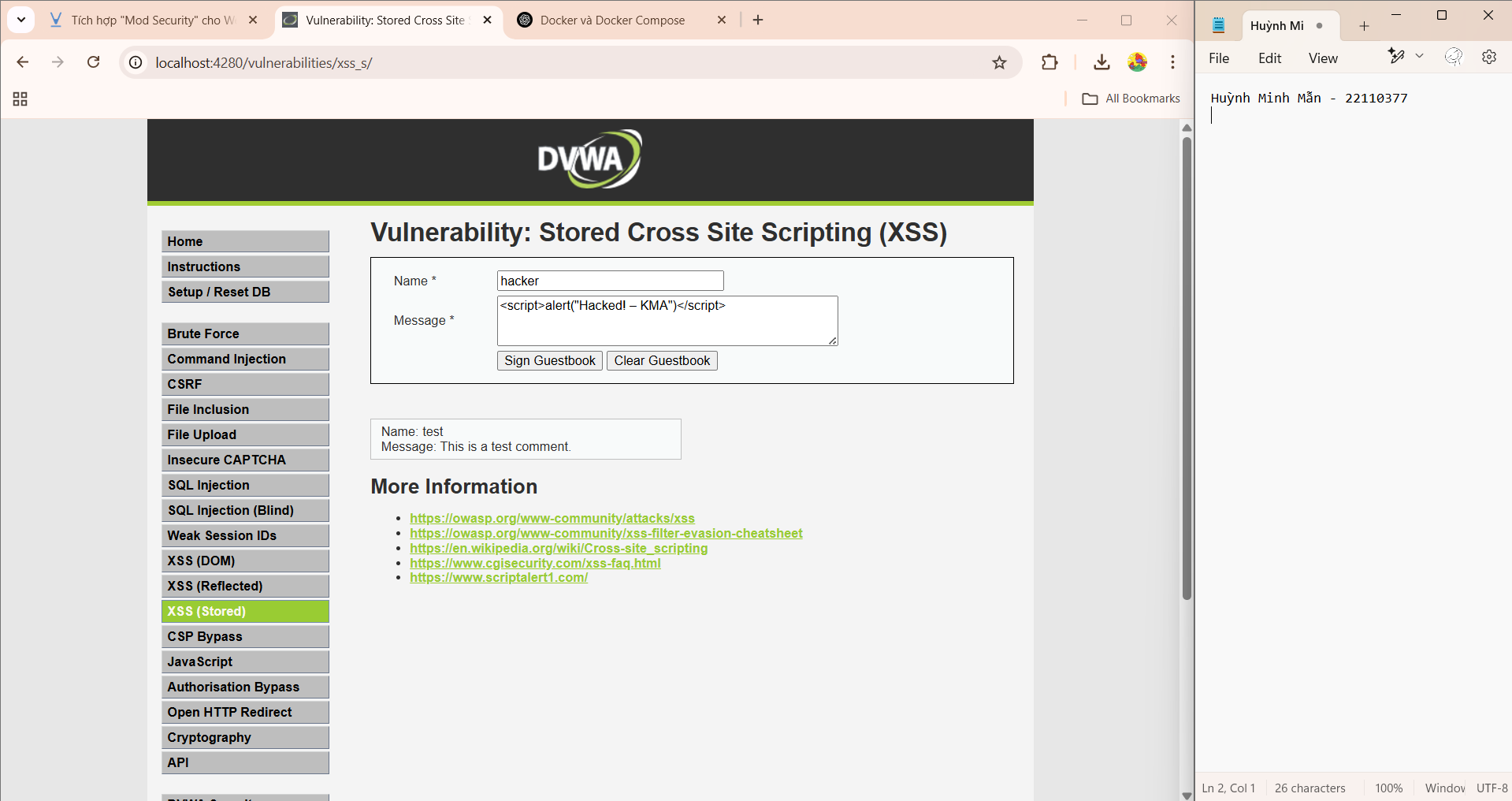


Hoặc 1 vài lệnh khác như ' OR 1=1 -- và ấn button submit.

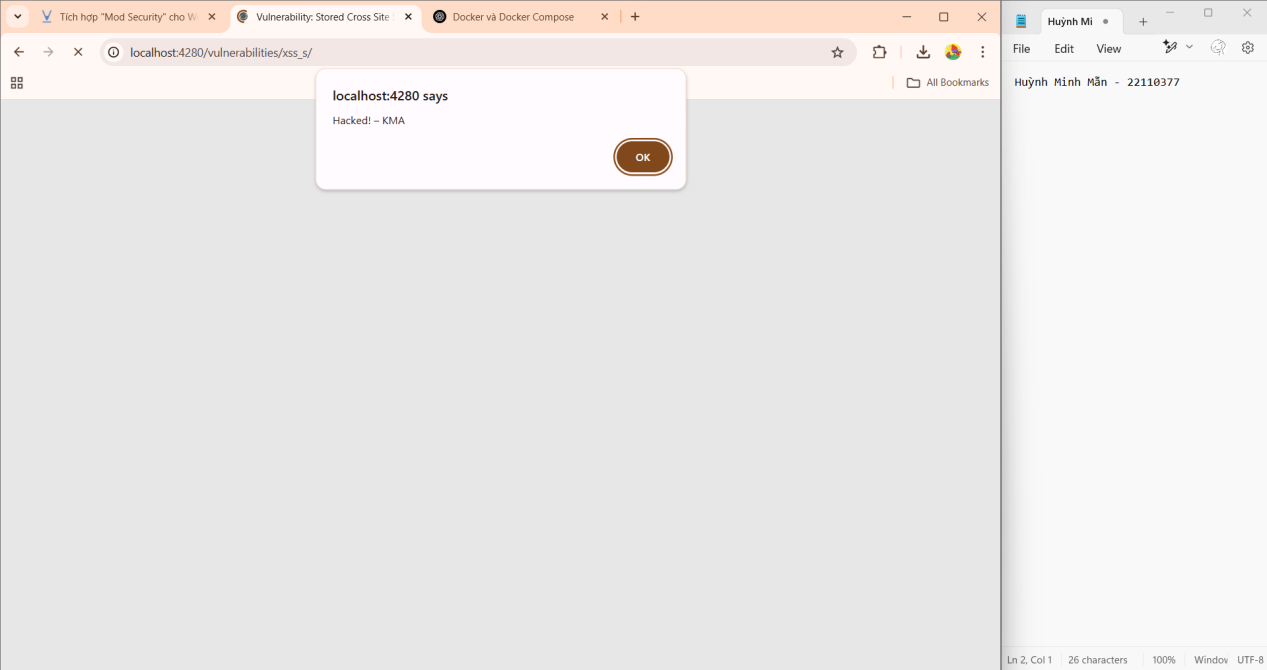


1. **Thử nghiệm XSS**

Vào XSS(stored), nhập name là hacker, Message nhập đoạn script sau: <script>alert("Hacked! – KMA")</script> và nhấn Sign Guestbook.



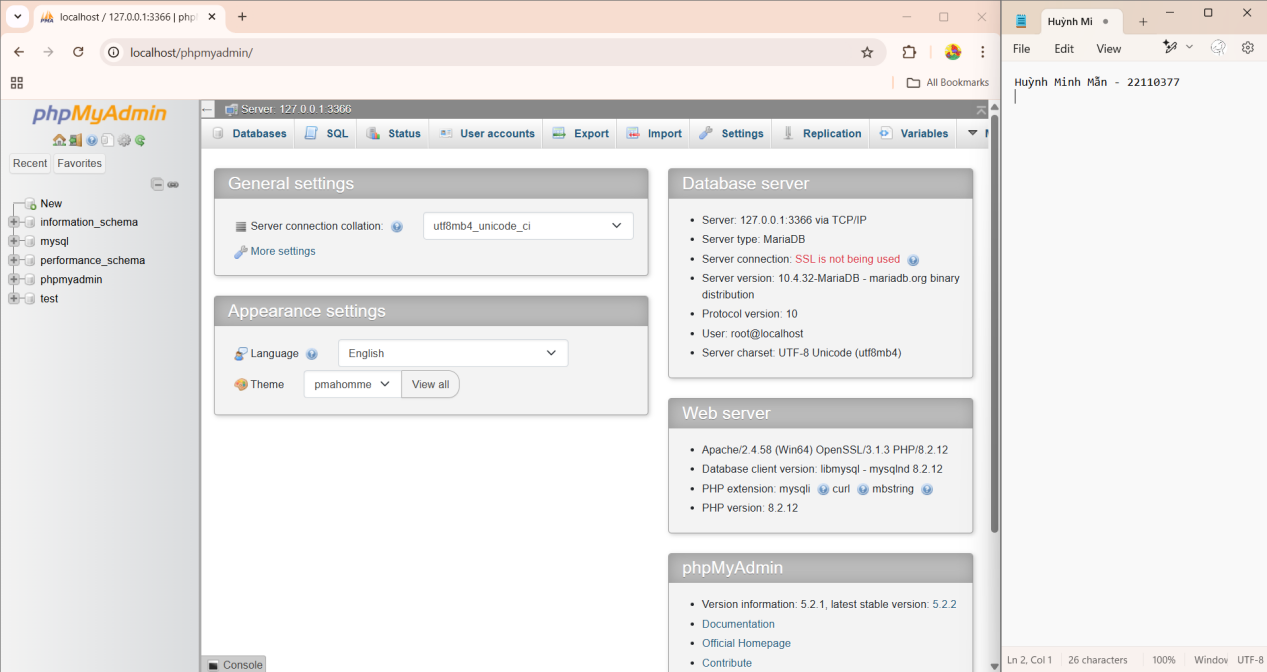
Sau khi submit đoạn script trên thì mỗi lần truy cập vào, trang web sẽ hiện một thông báo cho người dùng như sau



Có thể thấy được lỗi SQL Injection và XSS rất dễ dàng bị khai thác trong trang web DVWA này nên ta sẽ dùng phương pháp tích hợp tường lửa và cụ thể là Mod Security.

1. **Cài đặt và cấu hình Mod Security**

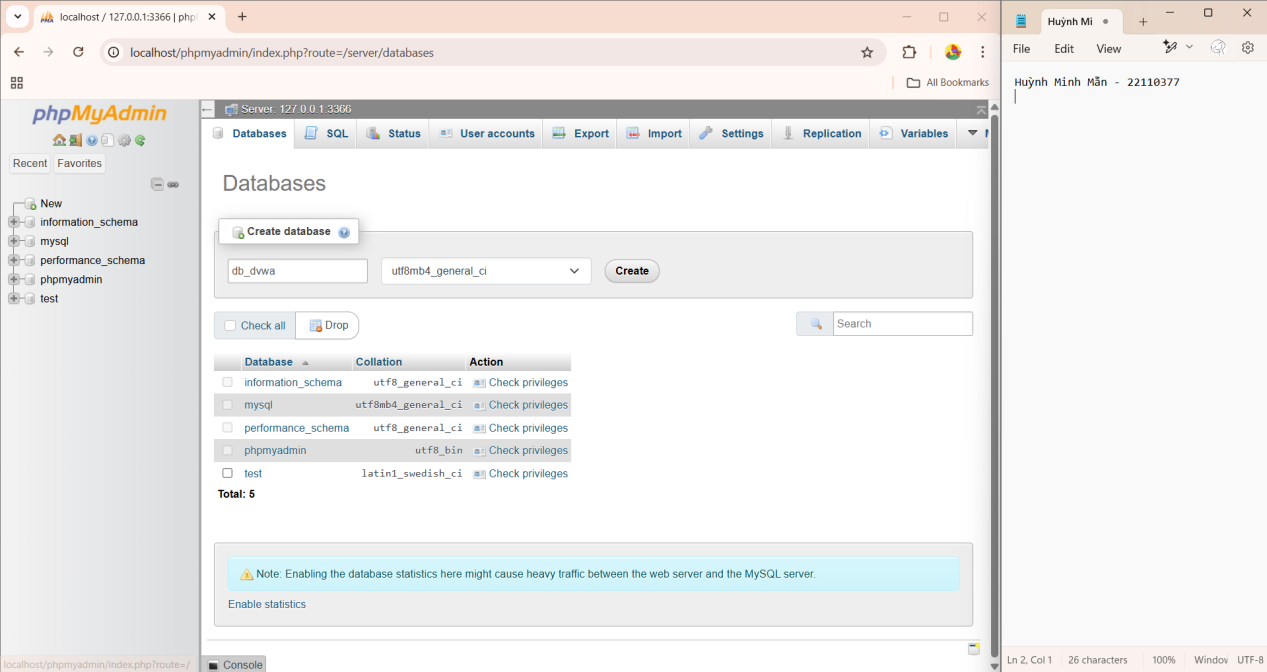
Để làm được bài này ta dùng công cụ XAMPP.



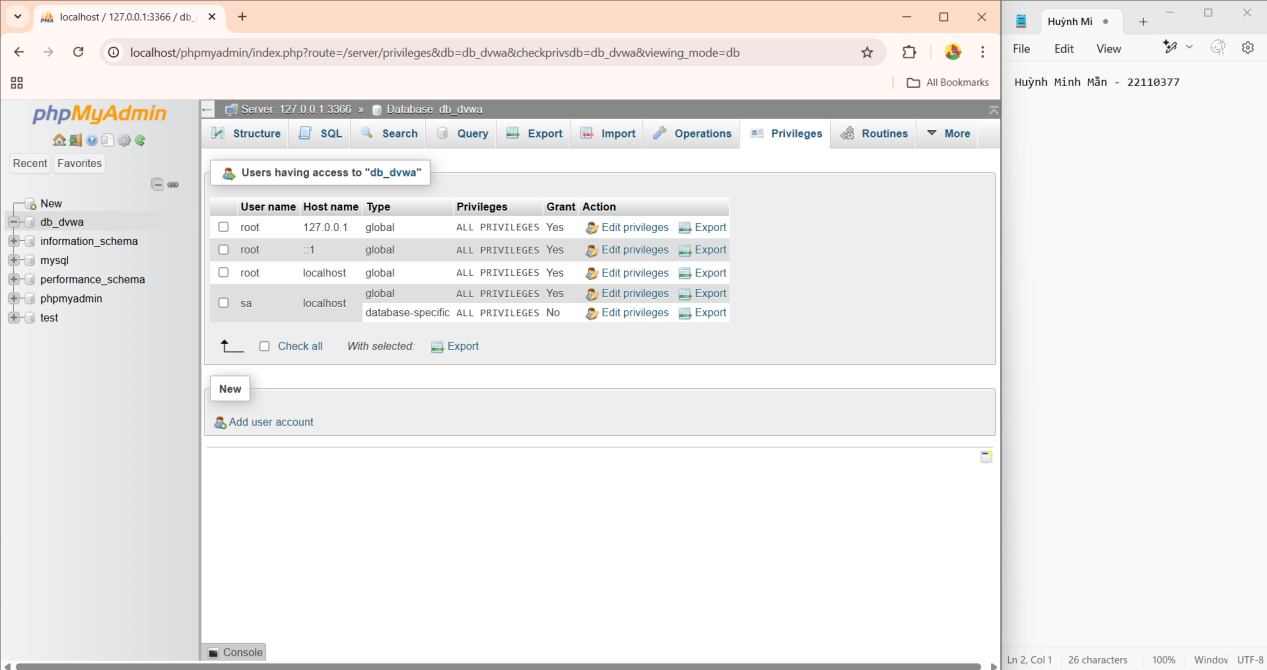
Đây là giao diện cơ bản của mySQL sau khi đã khởi động được.

Tiếp theo, ta tiến hành tạo mới database bằng cách:

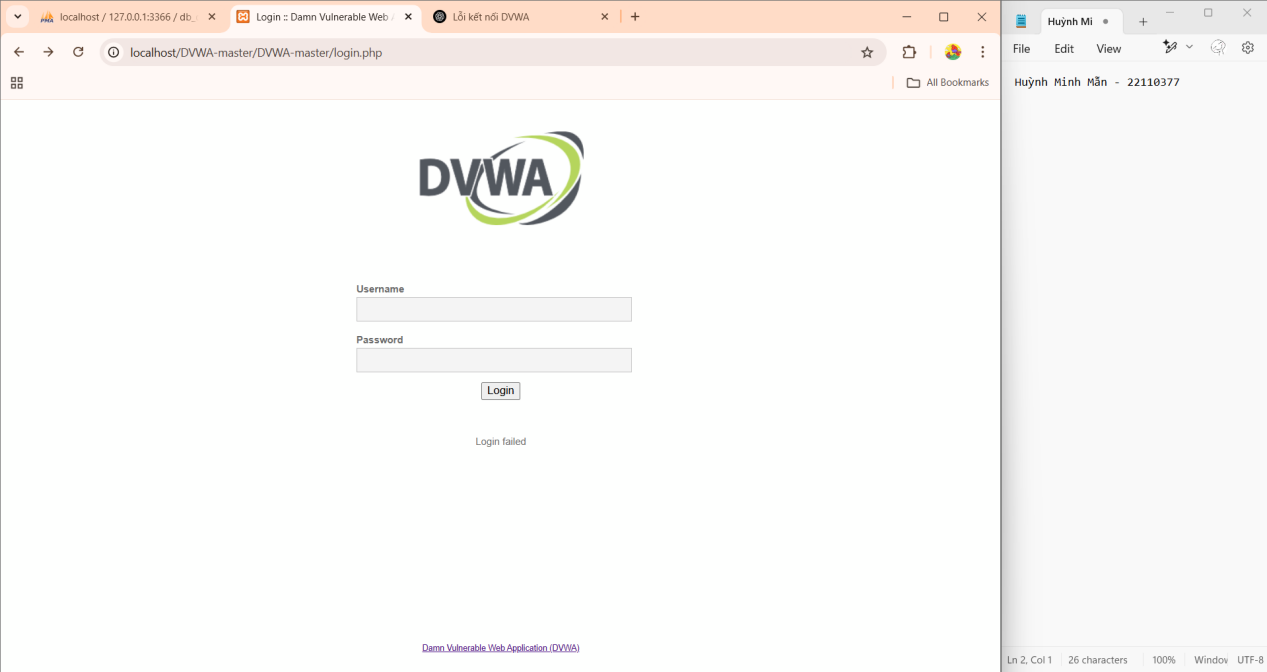
New -> nhập tên database -> Create

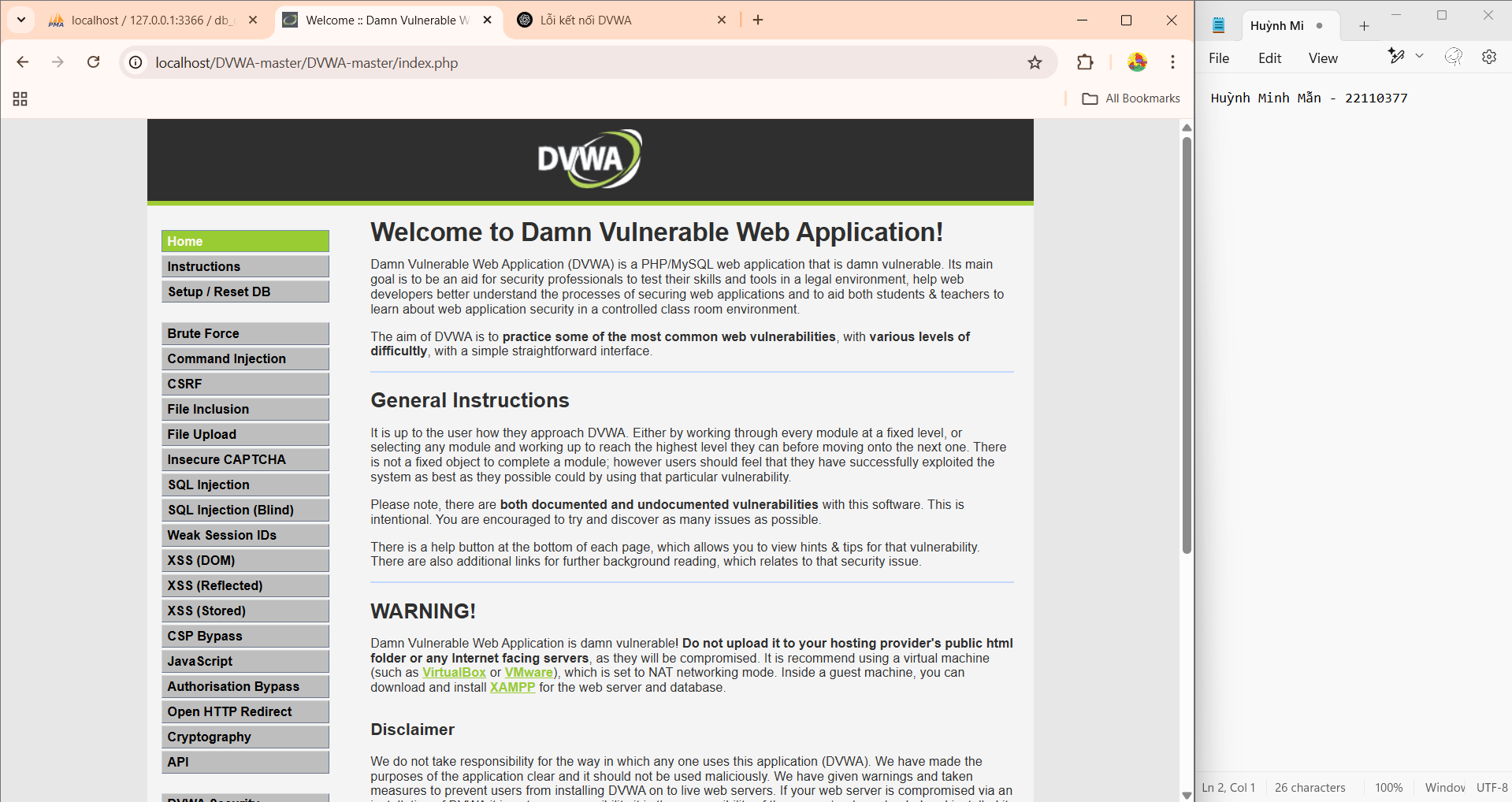


Tiếp theo, ta tạo user và gán quyền cho user đó có toàn quyền trên db\_dvwa vừa tạo.



Truy cập đường dẫn <http://localhost/DVWA-master/DVWA-master/login.php> để đăng nhập





Truy cập [https://www.apachelounge.com/download/](https://www.apachelounge.com/download/" \t "_blank) để tải mod\_security.

Sau đó ta sẽ copy 2 file mod\_security2.so vào ...\apache\modules và yajl.dll vào ...\apache\bin.

Sau đó, mở file httpd.conf của xampp, và thêm vào các dòng bên dưới:

*LoadModule security2\_module modules/mod\_security2.so*

*SecRuleEngine DetectionOnly*

*<IfModule security2\_module>*

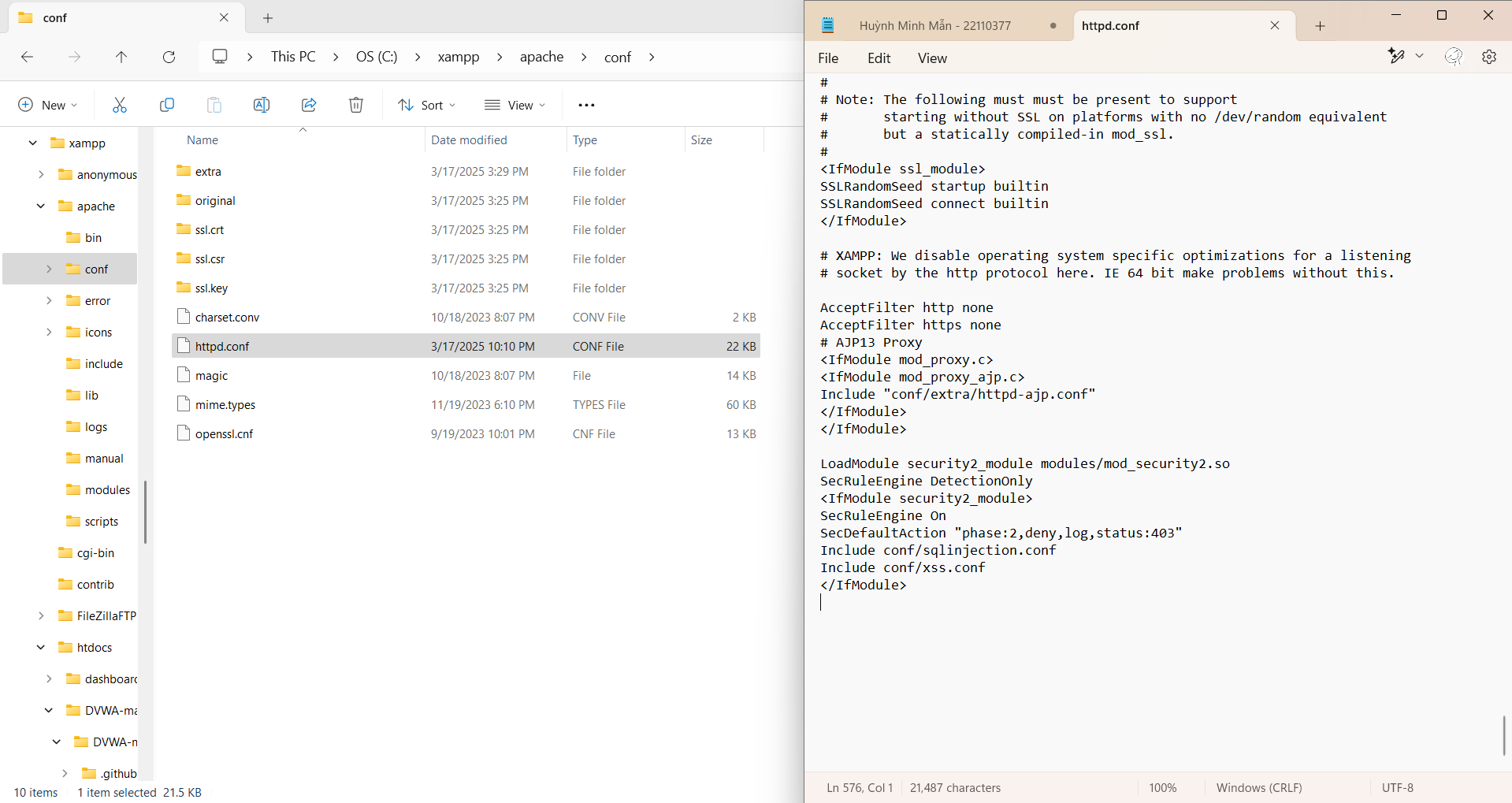
*SecRuleEngine On*

*SecDefaultAction "phase:2,deny,log,status:403"*

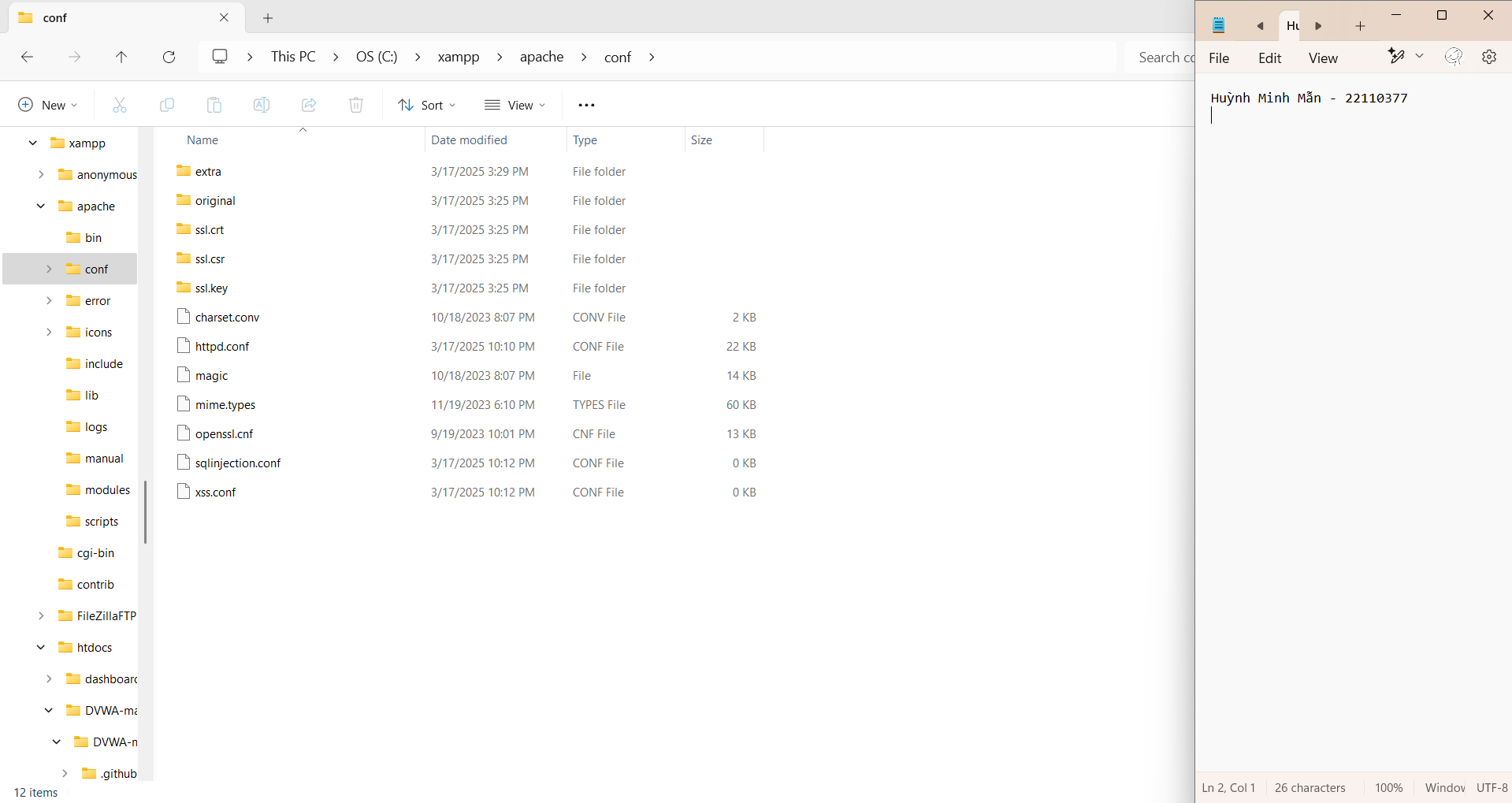
*Include conf/sqlinjection.conf*

*Include conf/xss.conf*

*</IfModule>*



Tiến hành tạo 2 file sqlinjection.conf và xss.conf trong thư mục apache\conf của Xampp.



Clone toàn bộ [rules SQL Injection](https://raw.githubusercontent.com/SEC642/modsec/master/rules/base_rules/modsecurity_crs_41_sql_injection_attacks.conf" \t "_blank) vào file sqlinjection.conf và [rules XSS Injection](https://github.com/SEC642/modsec/blob/master/rules/base_rules/modsecurity_crs_41_xss_attacks.conf" \t "_blank) vào file xss.conf.

Tiến hành restart lại Xampp Apache. Thử nghiệm lại tấn công SQL Injection và XSS.

