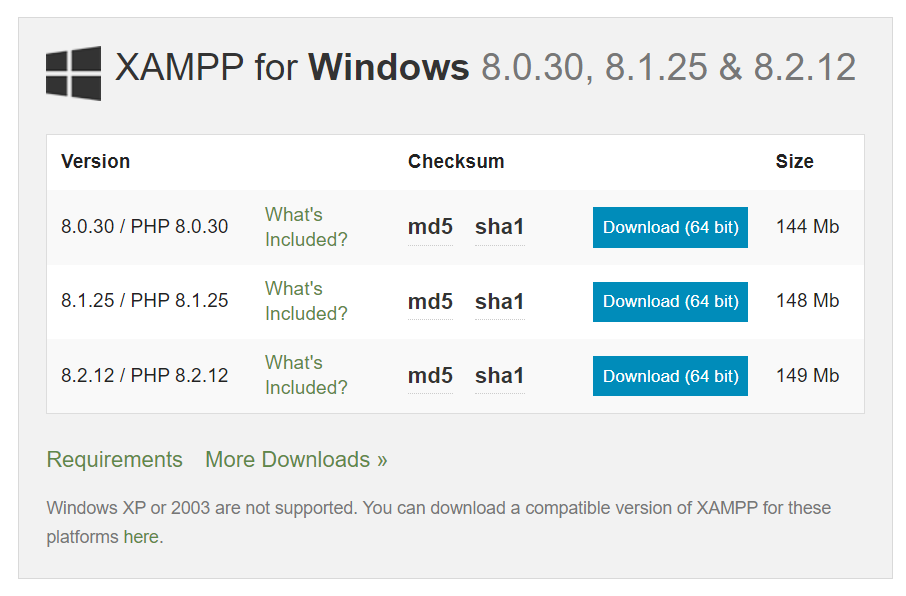
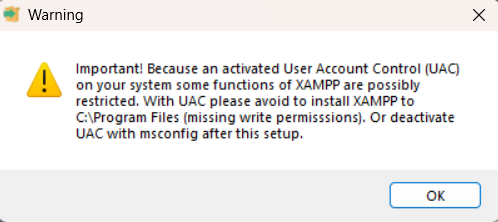
**HƯỚNG DẪN CÀI ĐẶT**

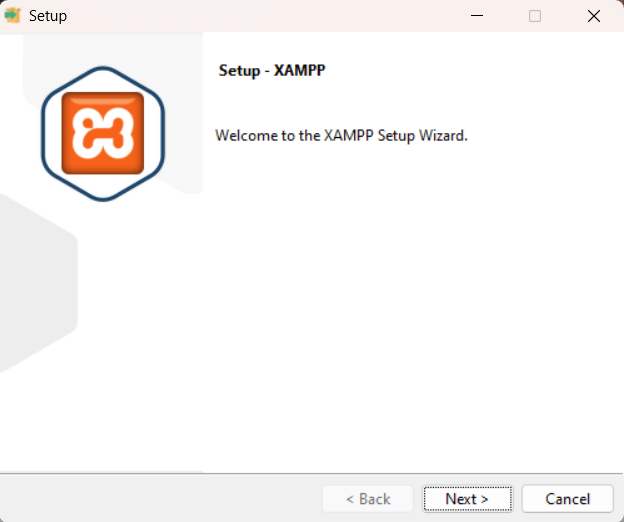
**B1:** *Cài đặt phần mềm XAMPP*

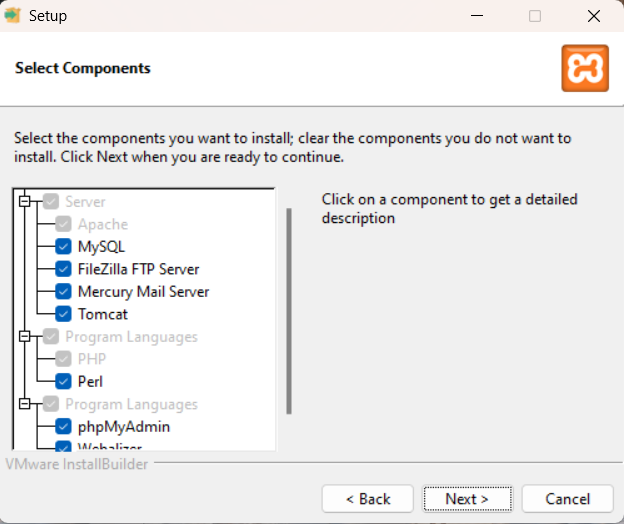
* Truy cập vào đường link và tải version phù hợp với máy tính: <https://www.apachefriends.org/download.html>



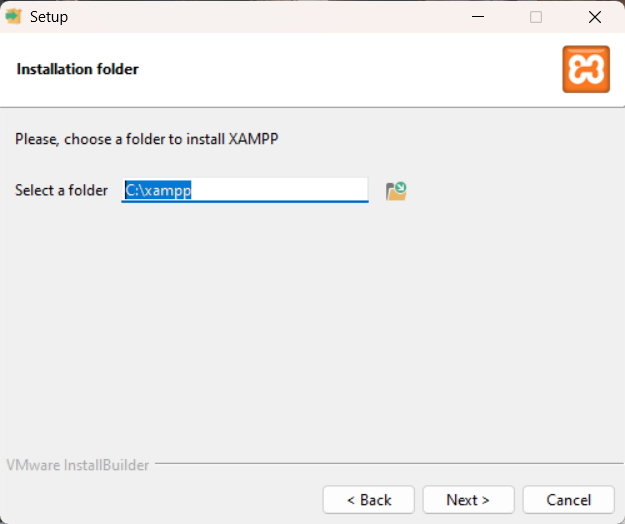
* Mở file đã tải về máy

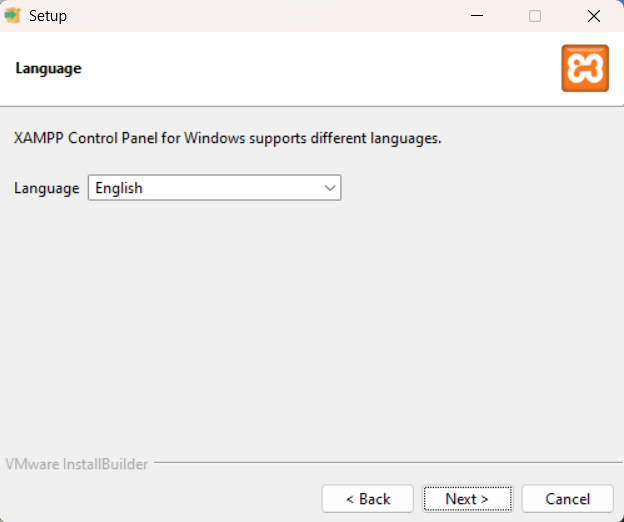


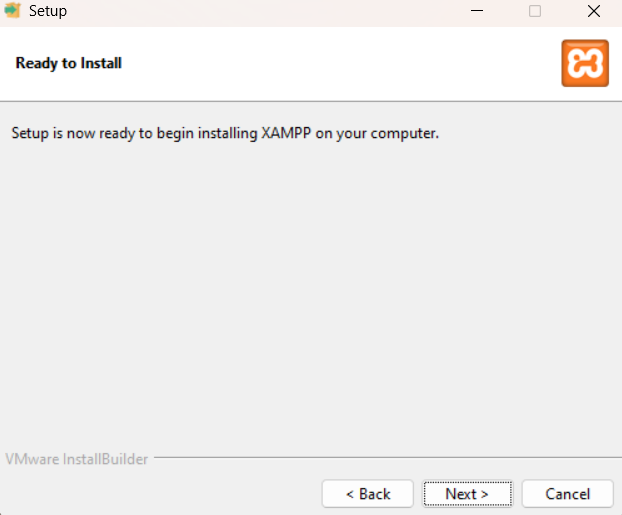




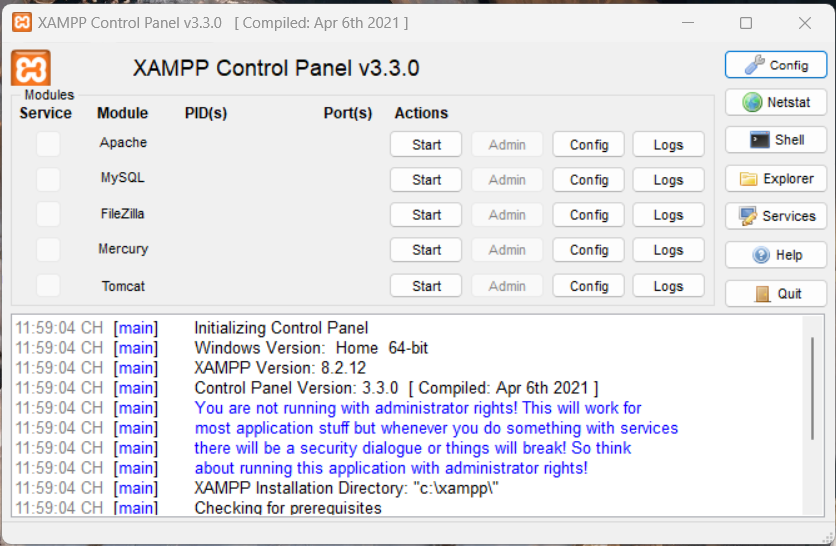
* Chọn đường dẫn để lưu folder -> Next



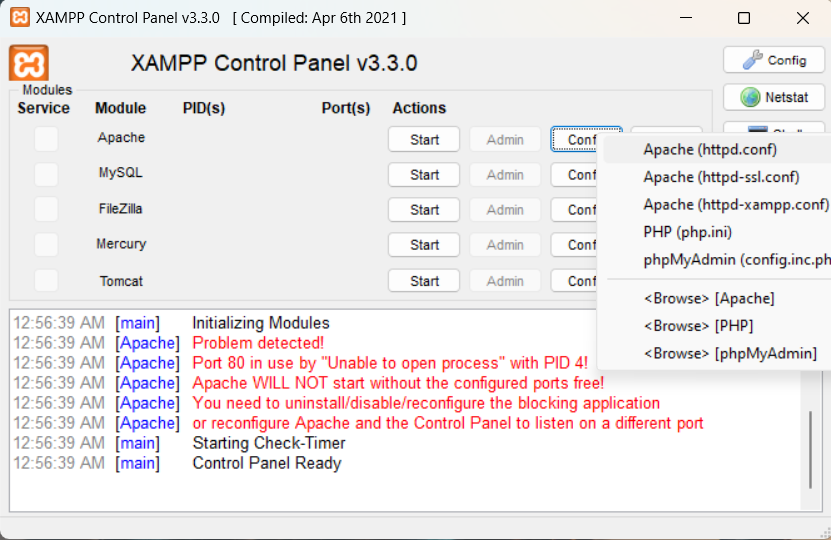




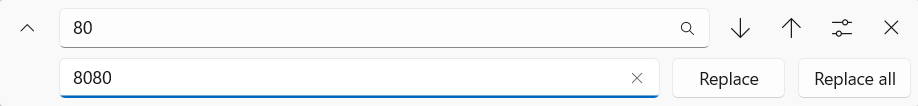
* Ta được bảng điều khiển:



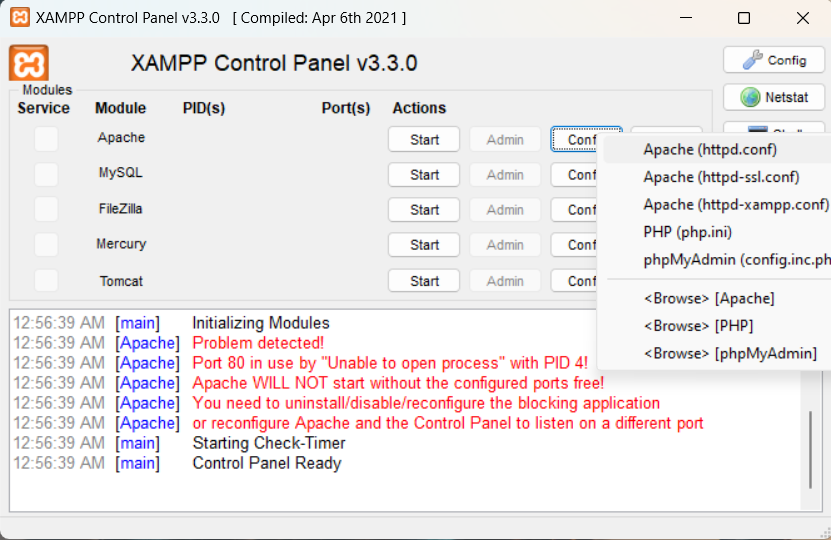
* Đổi port cho Apache:
* Chọn **Config** của Apache -> Chọn **Apache (httpd.conf)** và mở bằng Notepad



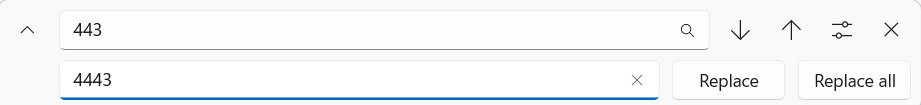
* Nhấn Ctrl + H
* Ở dòng **Find** nhập 80
* Ở dòng **Replace** nhập 8080 (Có thể là một con số khác ngoài 80)
* Nhấm nút **Replace all** và **Save**



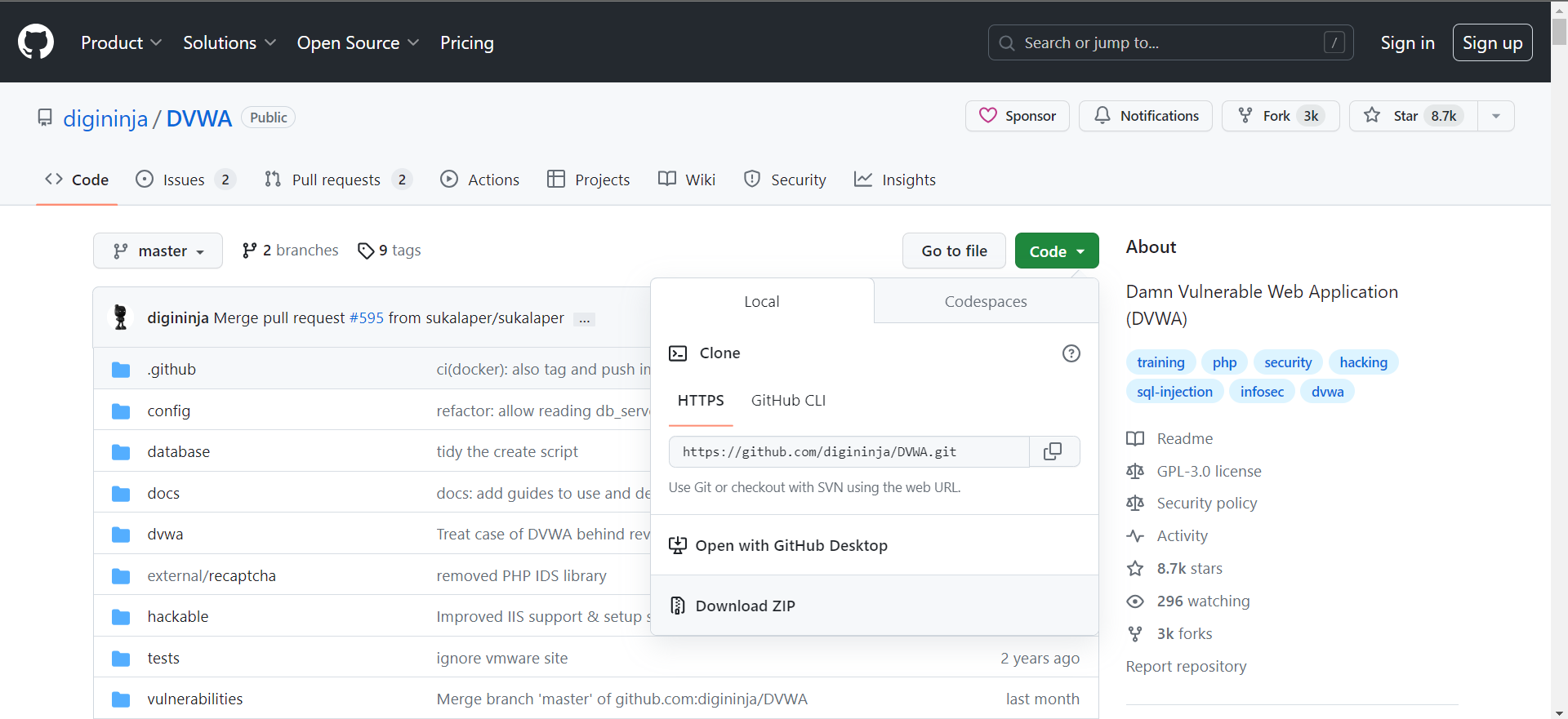
* Chọn **Config** của Apache -> Chọn **Apache (httpd-ssl.conf)** và mở bằng Notepad



* Nhấn Ctrl + H
* Ở dòng **Find** nhập 443
* Ở dòng **Replace** nhập 4443 (Có thể là một con số khác ngoài 443)
* Nhấm nút **Replace all** và **Save**



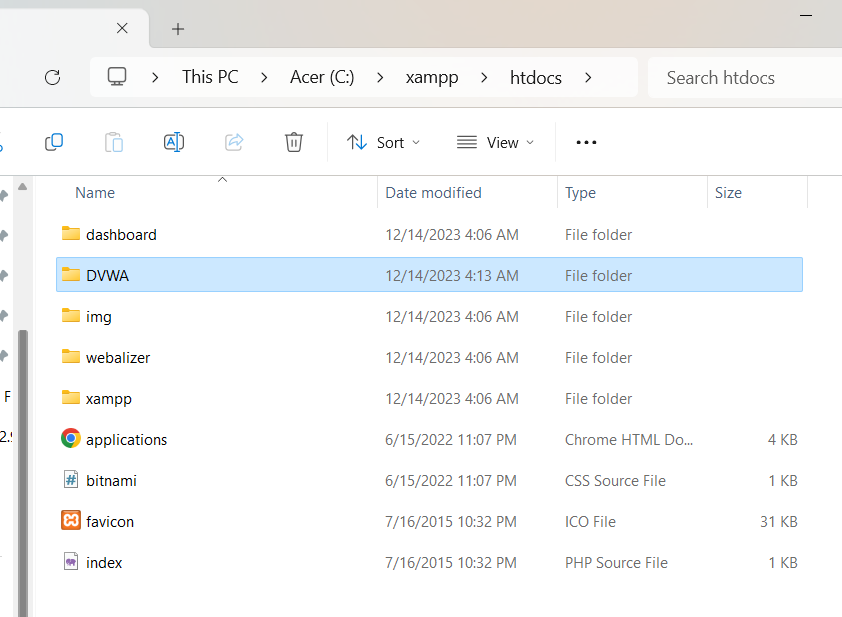
**B2:** *Tải DVWA:* <https://github.com/digininja/DVWA>

****

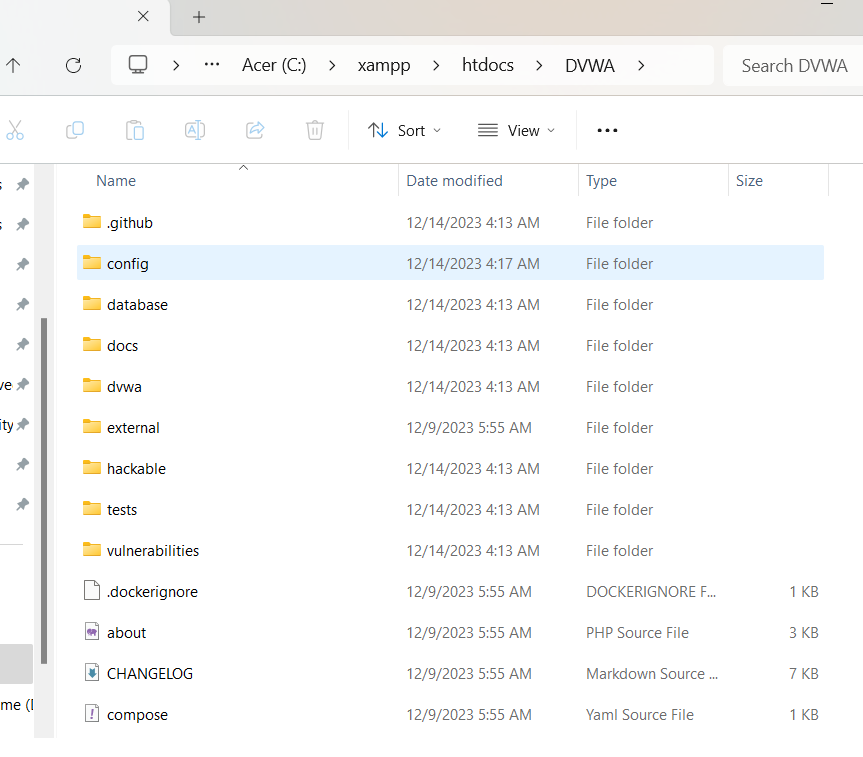
**1**

**2**

* Giải nén file và tạo thư mục DVWA trong: C:\xampp\htdocs

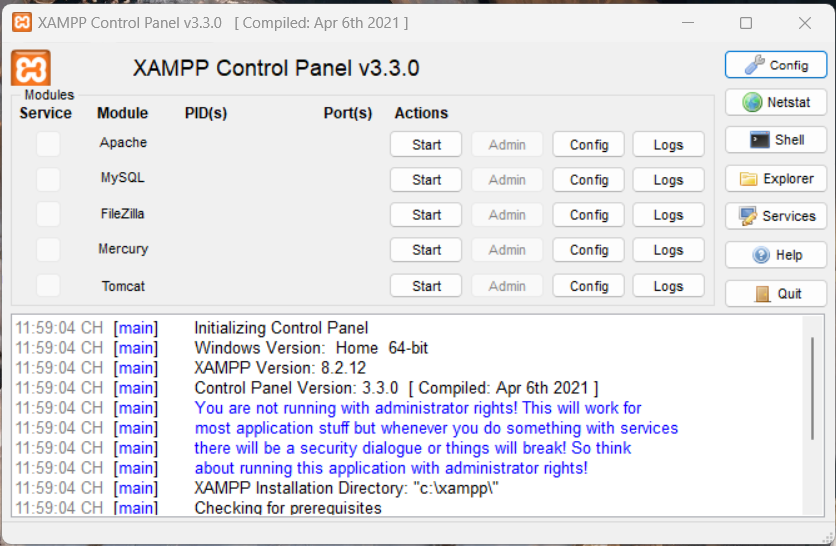


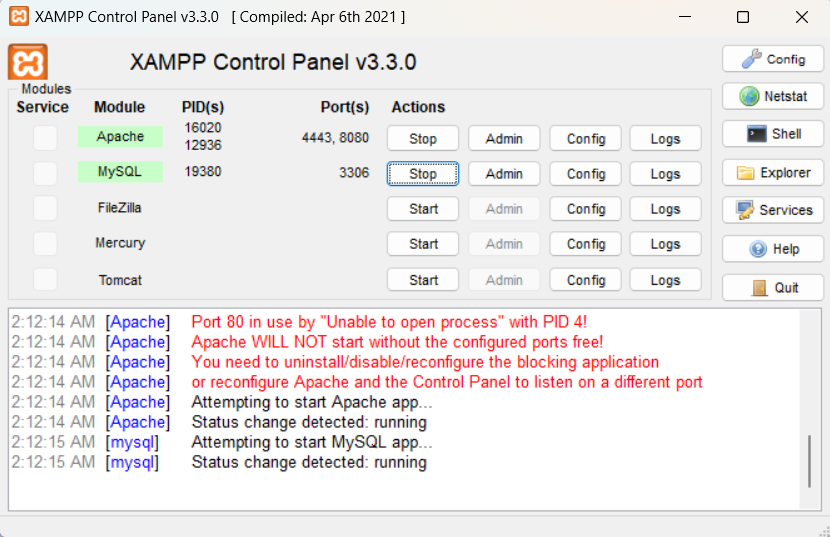
* Copy tất cả các file vào thư mục: C:\xampp\htdocs\DVWA



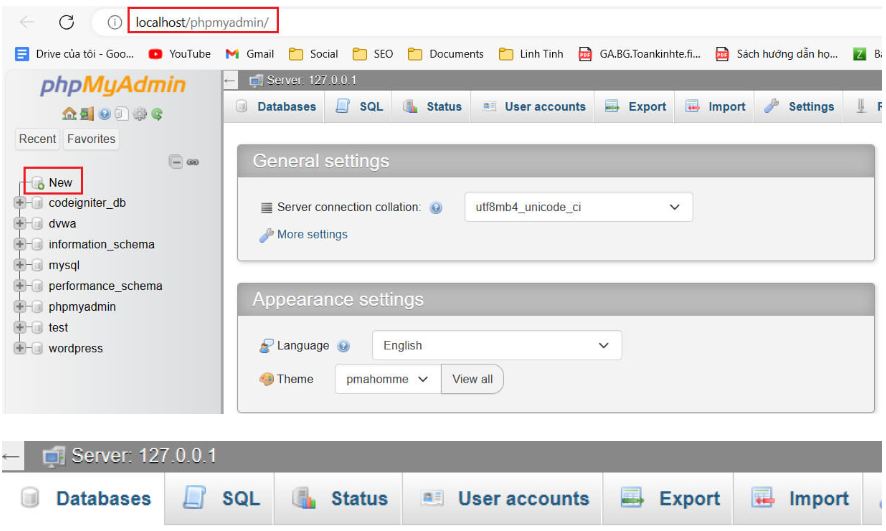
**B3:** *Khởi động XAMPP Control Panel*

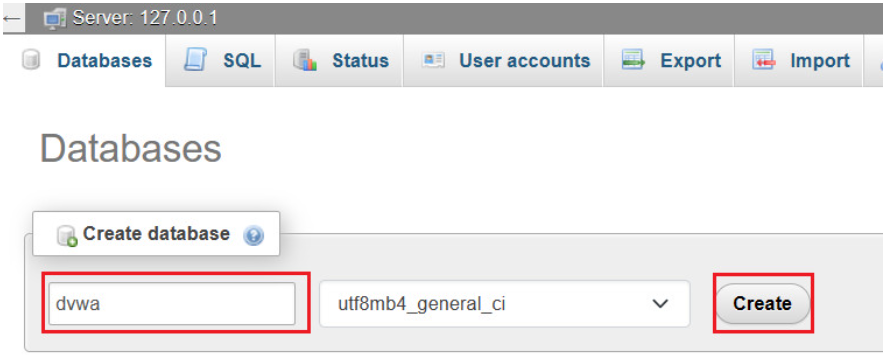
* Start **Apache** và **MySQL**



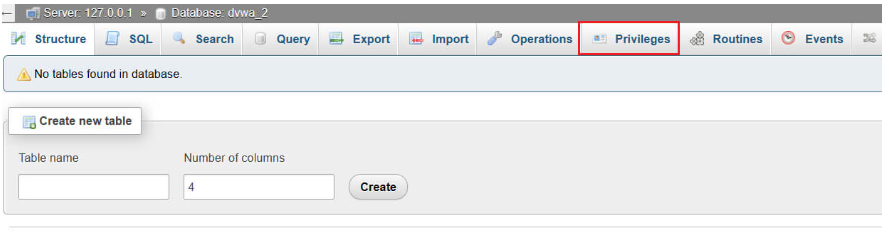


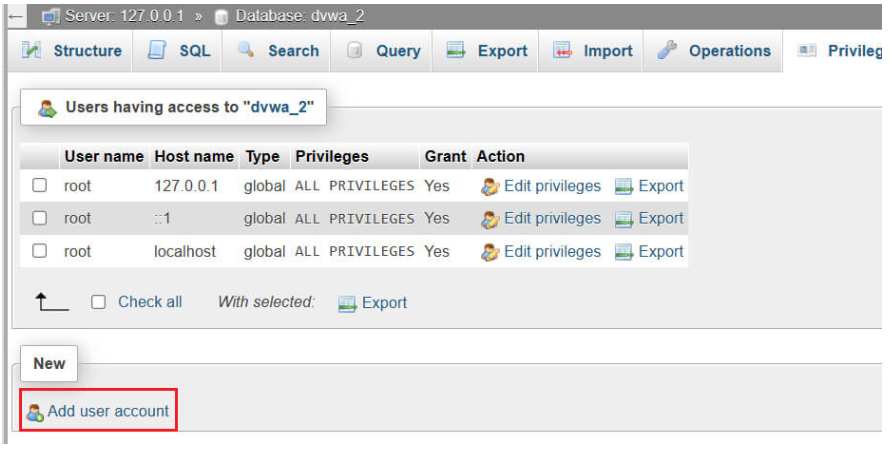
* Mở trình duyệt web và gõ: <http://localhost:8080/phpmyadmin/>
* Tạo **database**



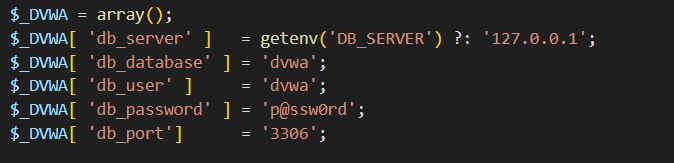


* Chọn **Privileges** > **Add user account**

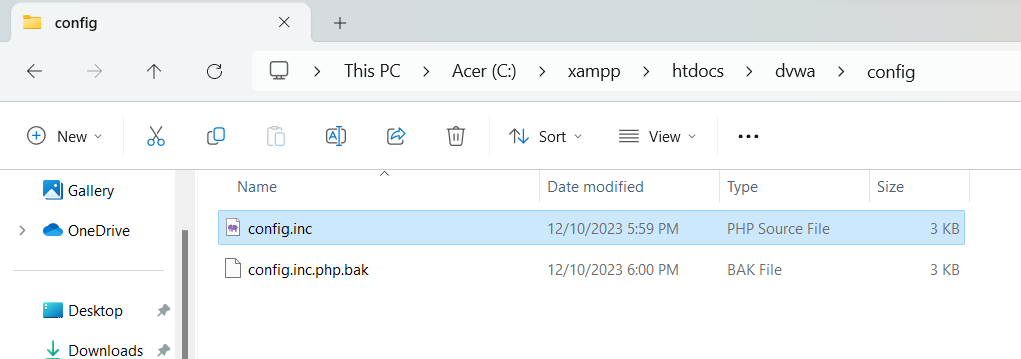




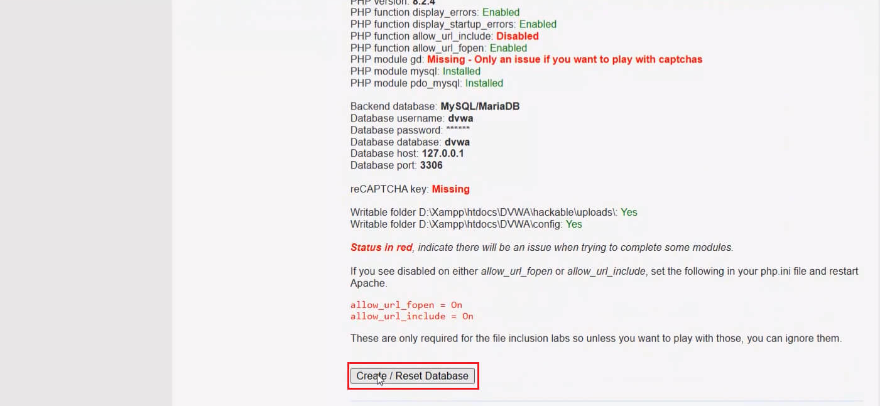
* Thiết lập **username**, **password** và **re-type** giống trong file **config.inc.php.dist** và chọn **Go** để hoàn tất add user



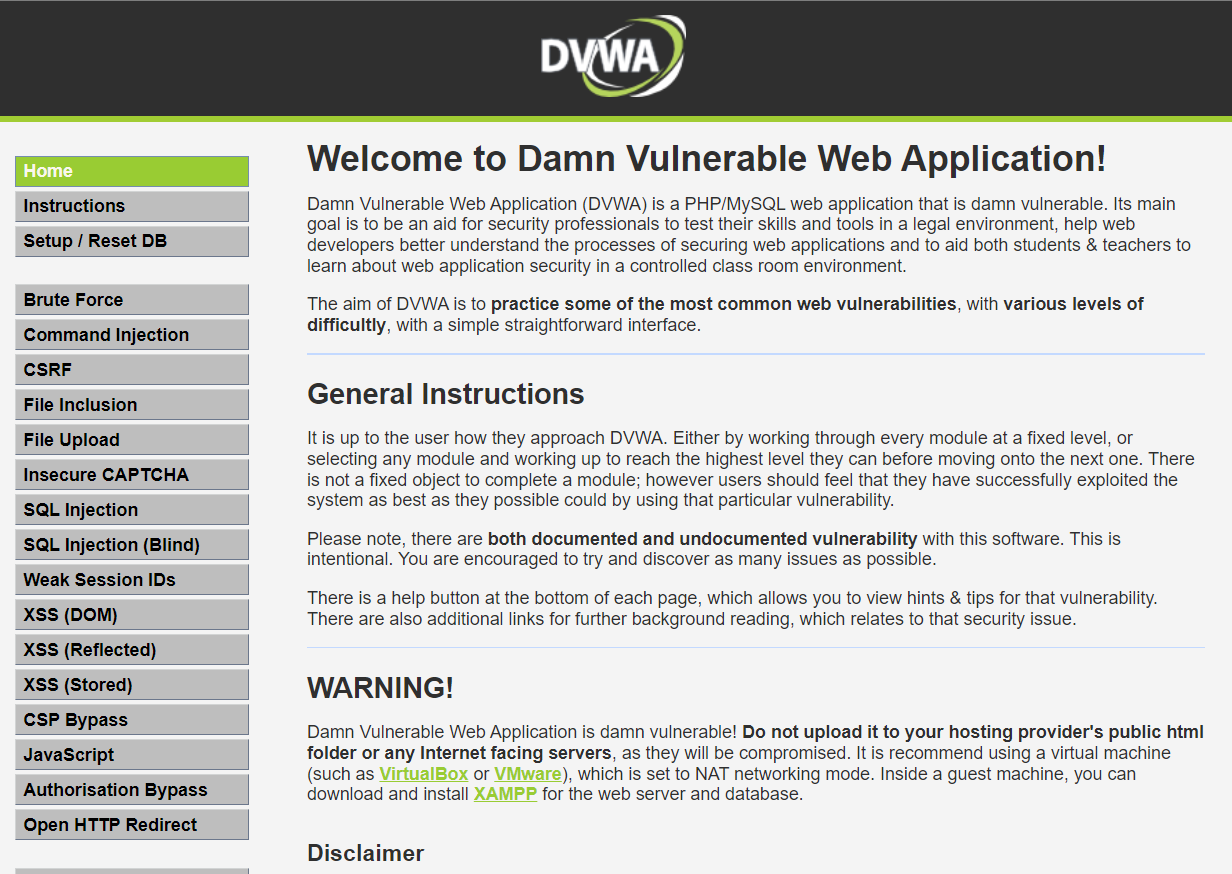
* Vào thư mục: C:\xampp\htdocs\DVWA\config
* Đổi tên file **config.inc.php.dist** thành **config.inc.php**



* Mở trình duyệt web và gõ: <http://localhost:8080/dvwa/setup.php> và chọn **Create/Reset Database**

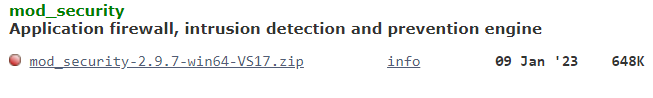


* Đăng nhập bằng tài khoản **username/password**: **admin/password** thì giao diện trang web sẽ như sau:

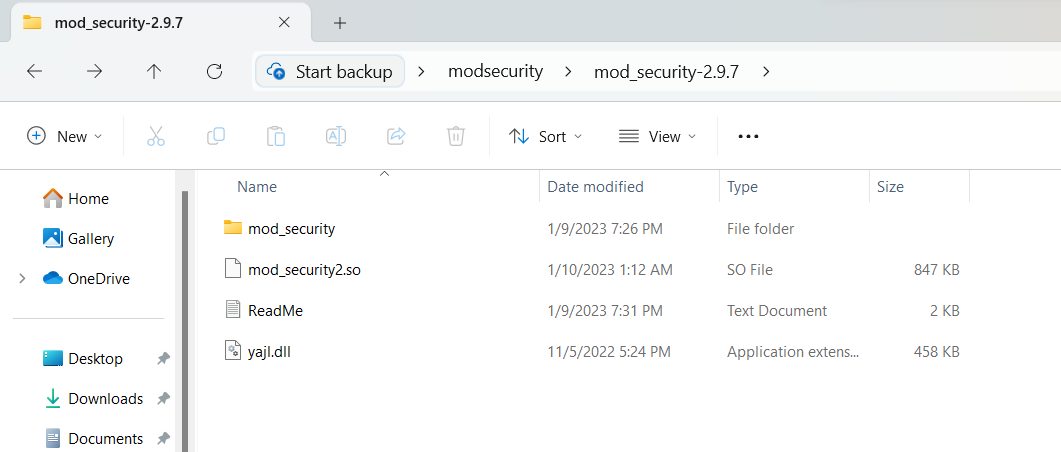


**B4:** *Triển khai Mod Security để chặn các cuộc tấn công*

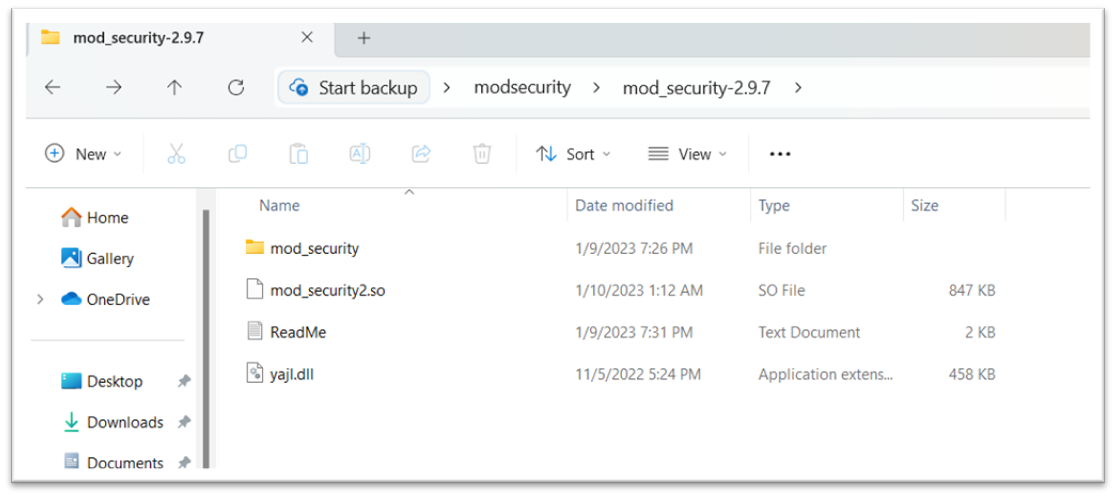
* Truy cập vào <https://www.apachelounge.com/download/> và tải về mod\_security tương ứng



* Sau khi download ta giải nén và làm theo các bước sau:
* Copy **mod\_security2.so** vào thư mục C:\xampp\apache\modules



* Copy **yail.dll** vào thư mục C:\xampp\apache\bin



* Mở file **httpd.conf** tại C:\xampp\apache\conf và thêm các dòng sau:

LoadModule security2\_module modules/mod\_security2.so

LoadModule unique\_id\_module modules/mod\_unique\_id.so

SecRuleEngine DetectionOnly

<IfModule security2\_module>

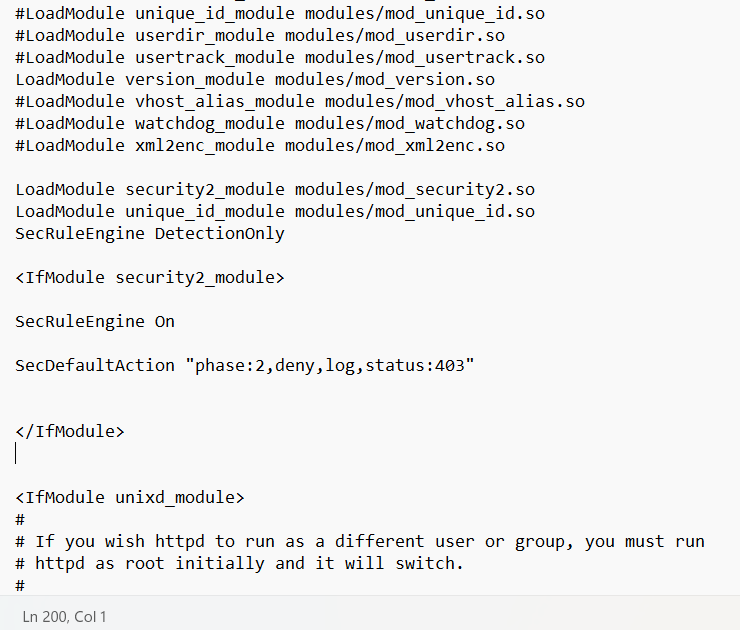
#Bật chế độ lọc của ModSecurity

SecRuleEngine On

#Thiết lập action mặc định

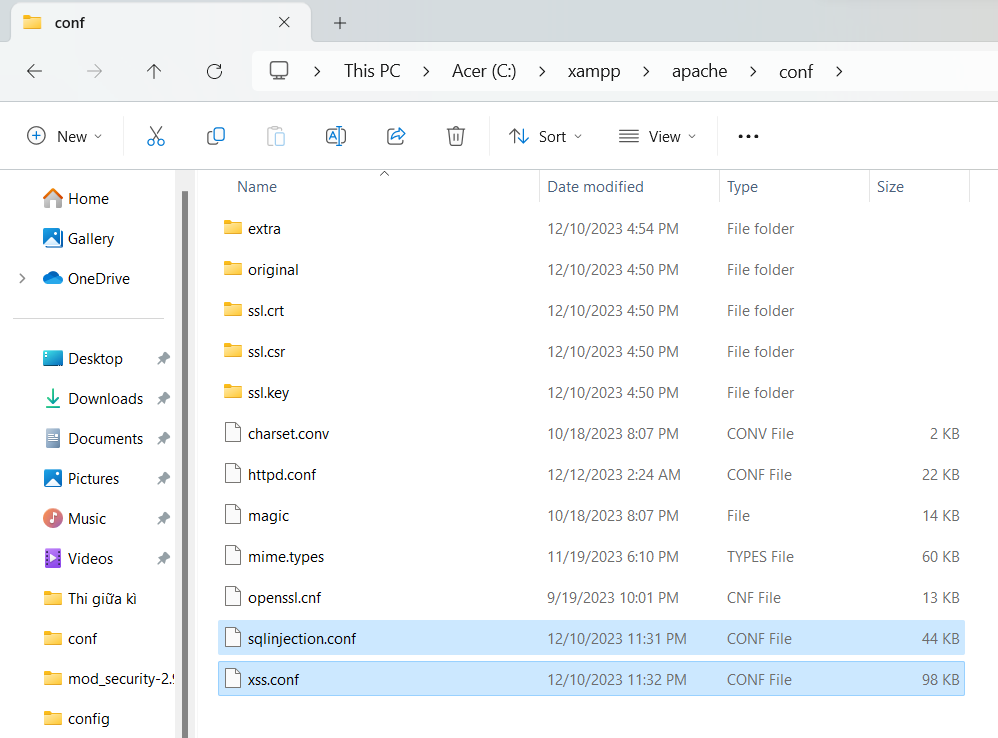
SecDefaultAction "phase:2,deny,log,status:403"

</IfModule>



**B5:** *Tạo file conf để thiết lập rules*

* Tiến hành tạo 2 file ***sqlinjection.conf*** và ***xss.conf*** trong thư mục C:\xampp\apache\conf



* ***Rules SQL Injection***:

<https://raw.githubusercontent.com/SEC642/modsec/master/rules/base_rules/modsecurity_crs_41_sql_injection_attacks.conf>

Copy toàn bộ vào file ***sqlinjection.conf*** đã tạo.

* ***Rules XSS***:

<https://raw.githubusercontent.com/SEC642/modsec/master/rules/base_rules/modsecurity_crs_41_xss_attacks.conf>

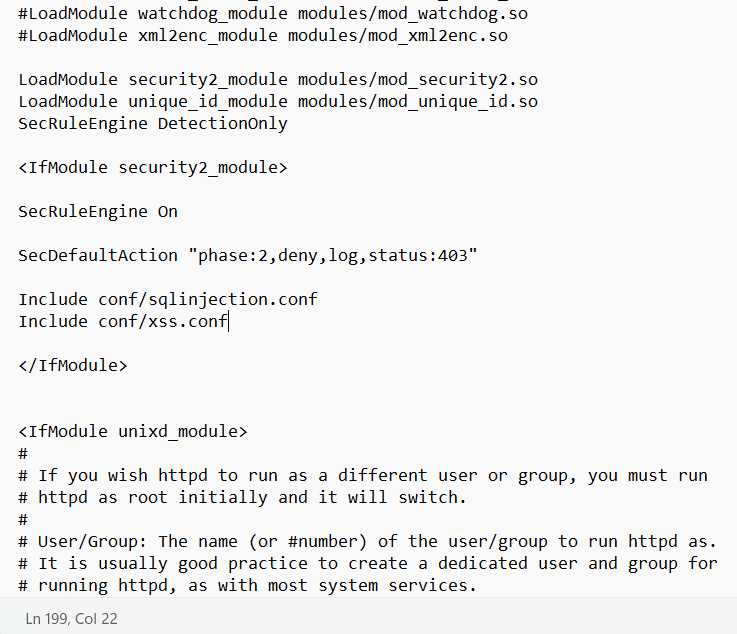
Copy toàn bộ vào file ***xss.conf*** đã tạo.

* Mở lại file **httpd.conf** và thêm các dòng sau:

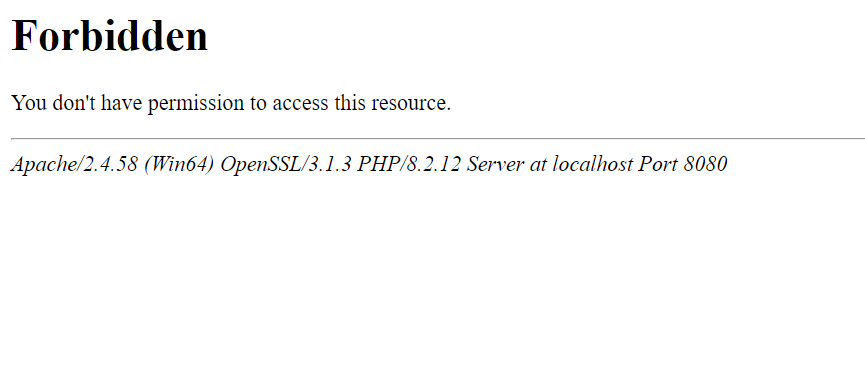
#Include <đường dẫn đến file rule>

Include conf/sqlinjection.conf

Include conf/xss.conf



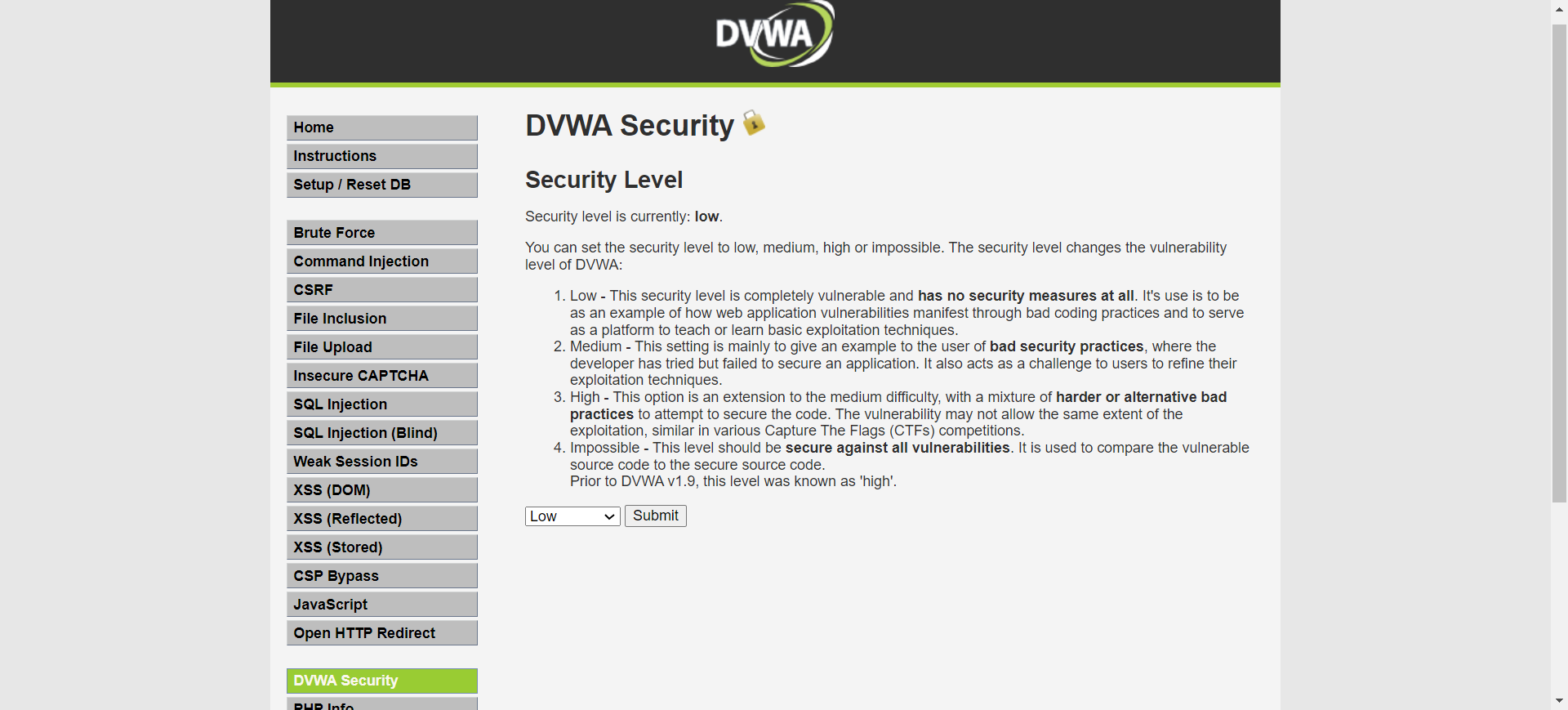
Tiến hành restart lại XAMPP Control Panel. Thử nghiệm lại tấn công SQL Injection và XSS như demo. Kết quả như hình:



**HOÀN THÀNH !!!**

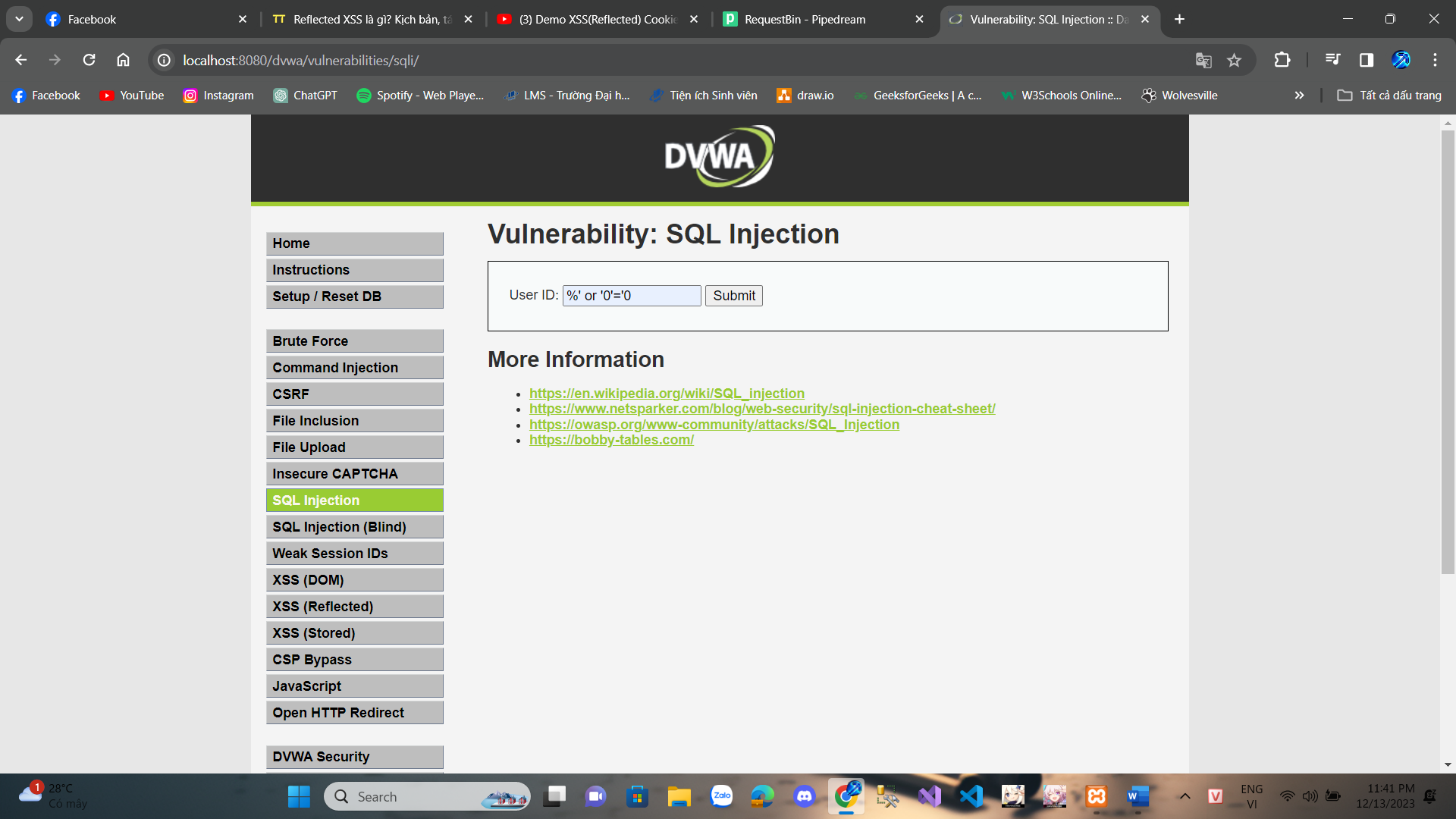
***HƯỚNG DẪN TẤN CÔNG (Lưu ý chỉ cài đặt tới B3)***

* Chỉnh mức độ Security của web DVWA về mức low:

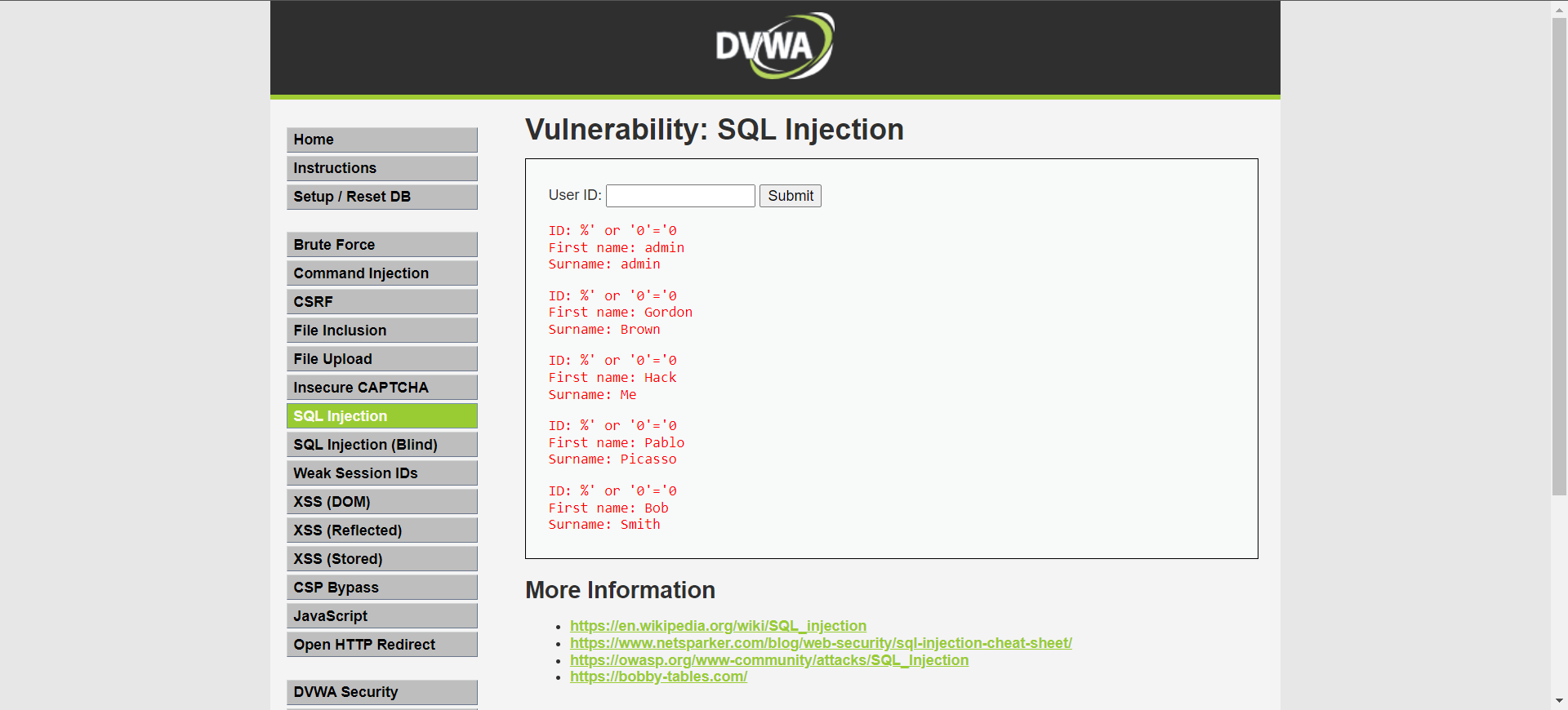
******

1. ***Tấn công SQL Injection:***

Nhập %' or '0'='0 và **submit**:



* Kết quả sẽ nhận được thông tin của tất cả các users có trong cơ sở dữ liệu.
* Câu truy vấn lúc này máy chủ sẽ được hiểu là: ***SELECT \* FROM users WHERE user\_id='%' or '0'='0'***
* Có thể thử tiếp ở các mức Security khác nhau của DVWA



1. ***Tấn công XSS:***
2. ***XSS (DOM):***

* Vào XSS(DOM) vào đường link và enter đoạn code sau:

</select><img src=x onerror=alert("Hi!Attacker")>

hoặc

</option></select><img src=x onerror=alert("Hello")>

1. ***XSS(Reflected):***

* Vào XSS(Reflected) và submit đoạn script sau:

<script>alert("Hello\_Attacker")</script>

hoặc

<img src=x onerror=alert("Good\_Morning\_Sir")>

***HƯỚNG DẪN BẢO VỆ MÁY CHỦ KHỎI CUỘC TẤN CÔNG***

(Cài đặt tiếp **B4** và **B5** rồi thử lại các cuộc tấn công)