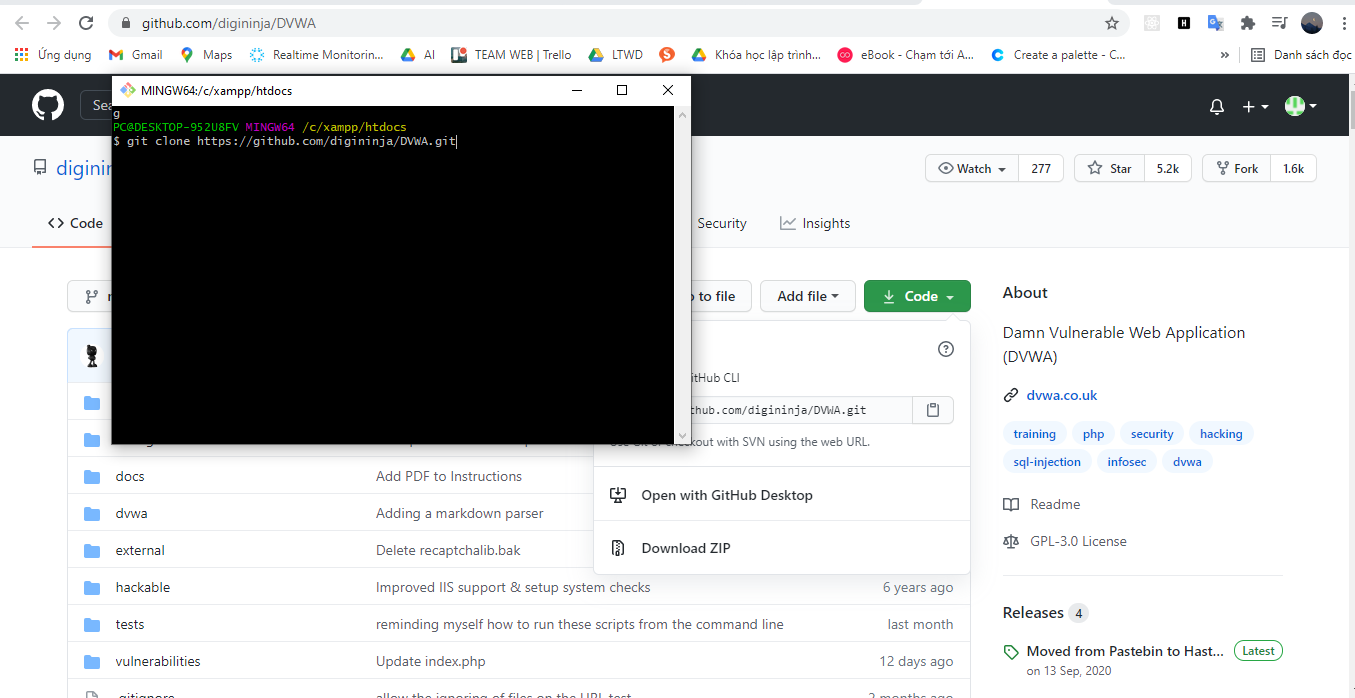
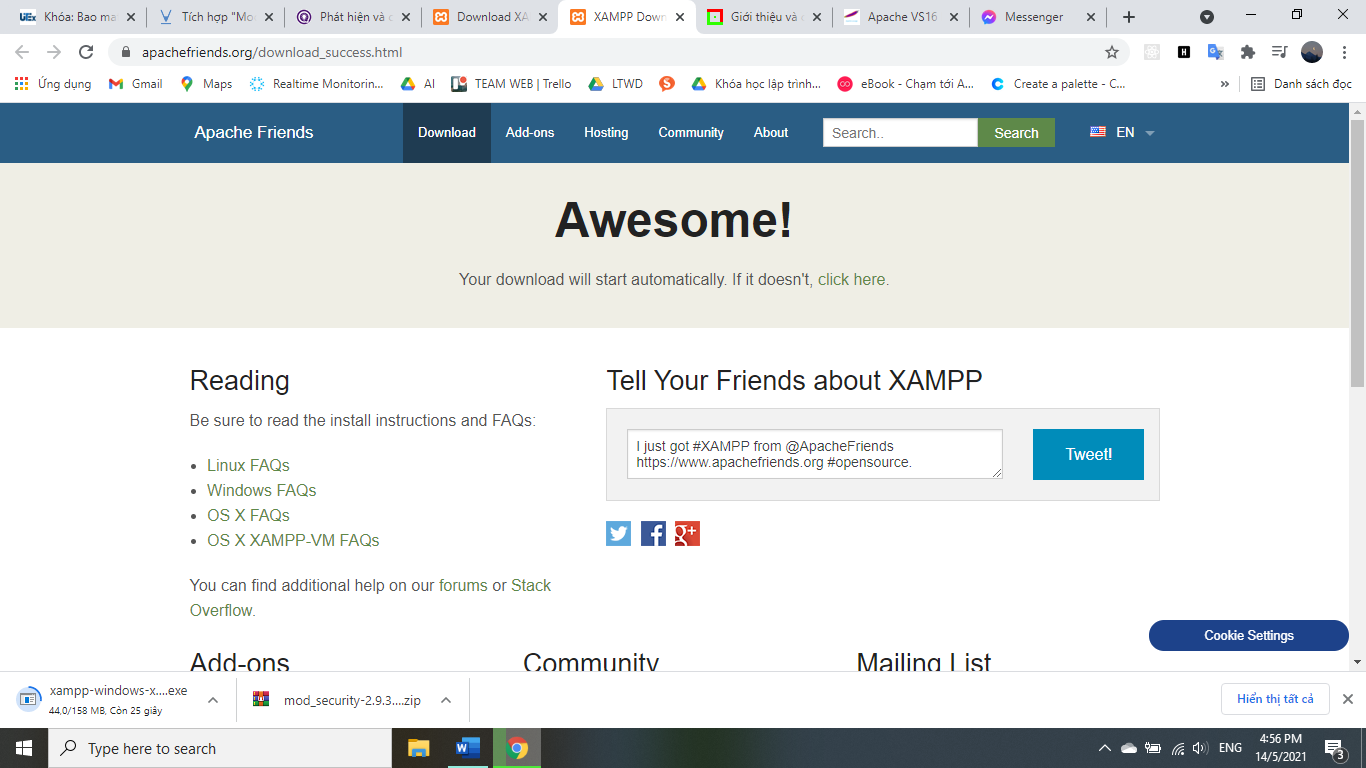
**BÀI TẬP MOD - SECURITY**

# **Bài 1: Tích hợp "Mod Security" cho Web Application Server để chống lại SQL Injection và tấn công XSS**

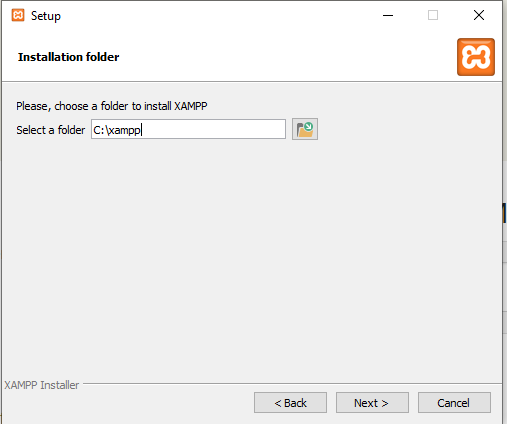
Link https://viblo.asia/p/tich-hop-mod-security-cho-web-application-server-de-chong-lai-sql-injection-va-tan-cong-xss-bJzKmx6X59N

Download DVWA



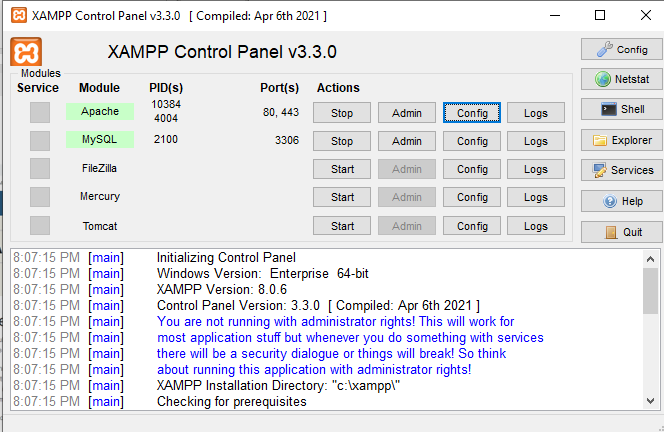
Download xampp

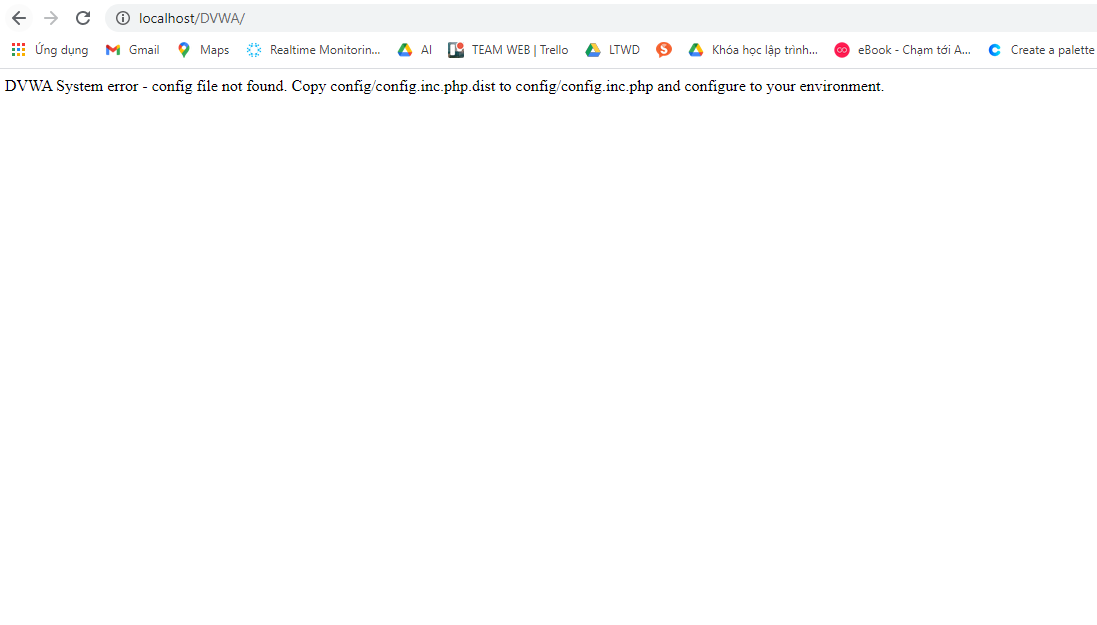
Setup xampp



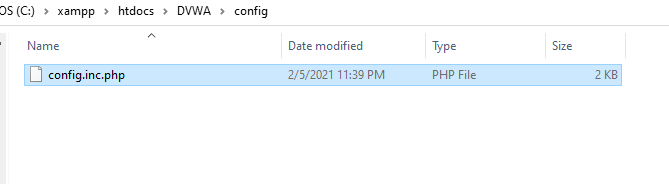
Run xampp



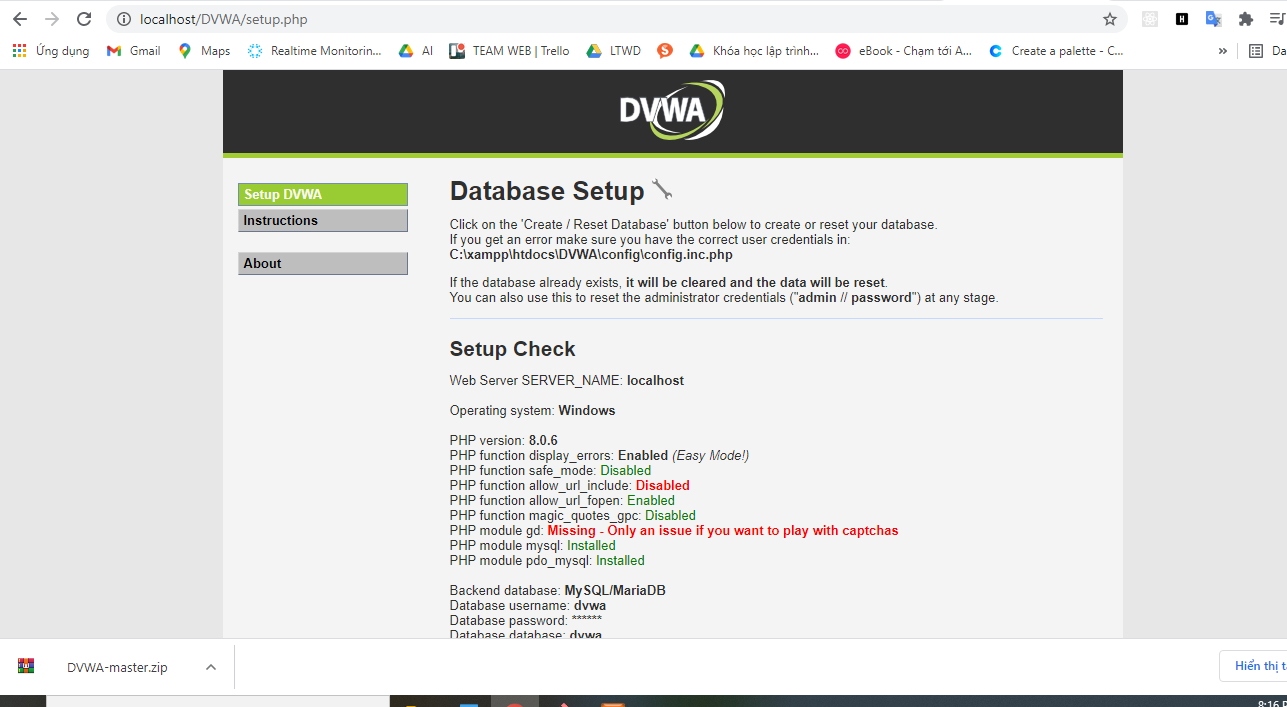


Fix config cho DVWA

Sửa lại tên file

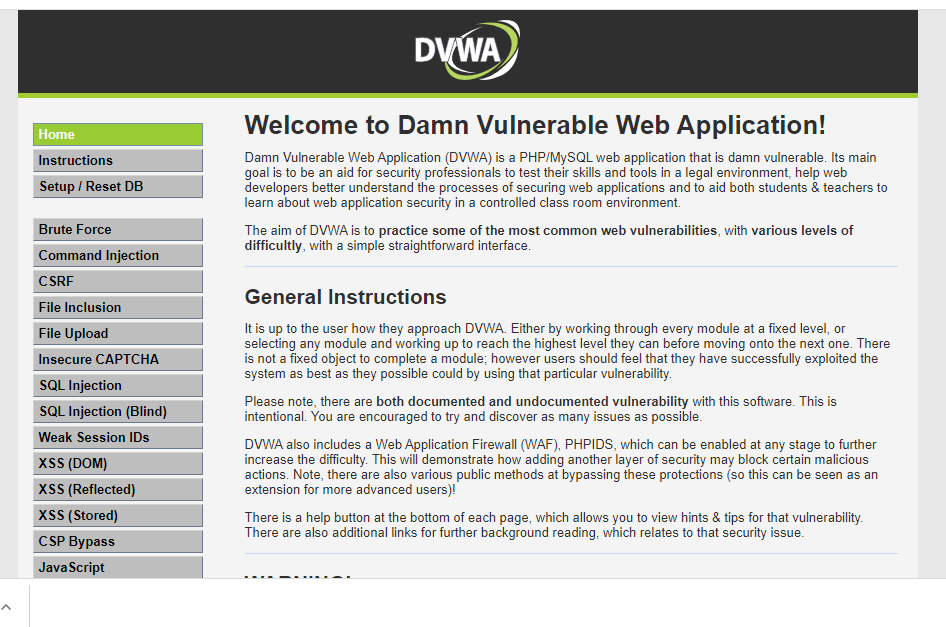


Run DVWA

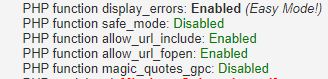


Sửa password sang ‘’ và dbUser là Root

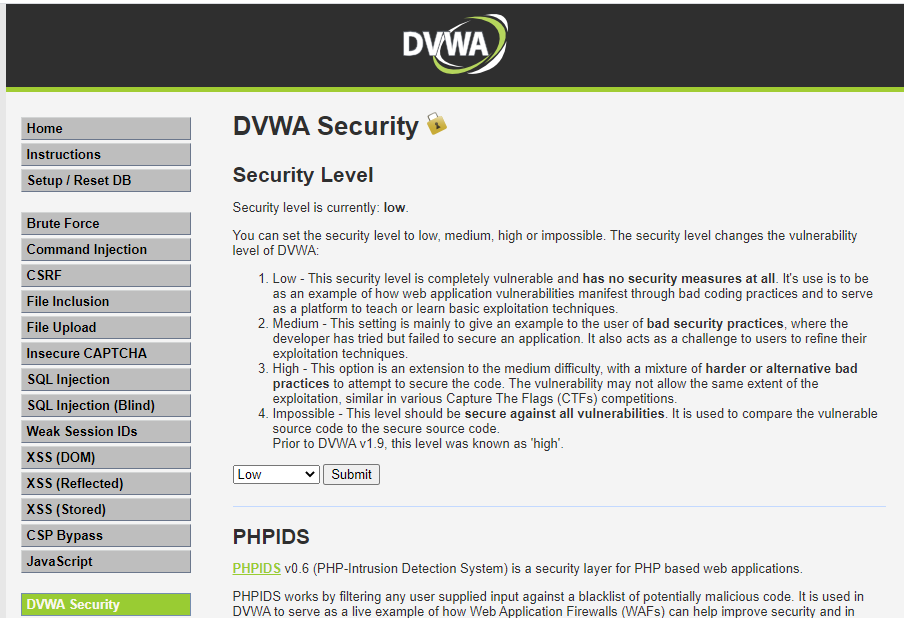




Fix config  allow\_url\_include: Disabled

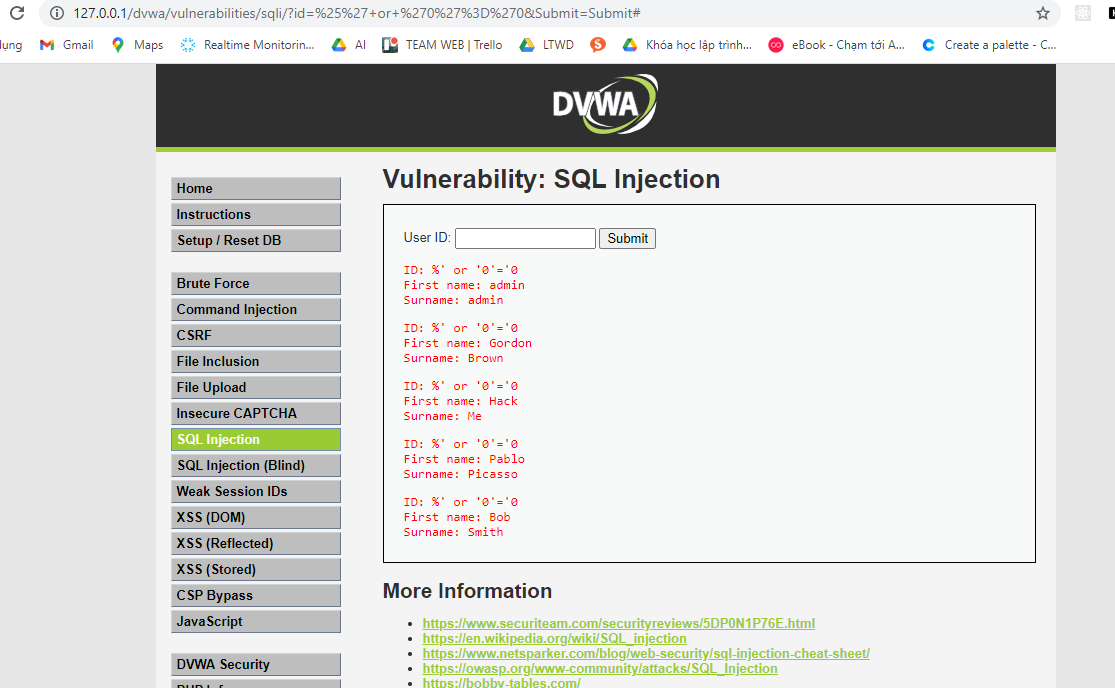


Đổi sang Security Level: low



1.1 Thử nghiệm SQL Injection

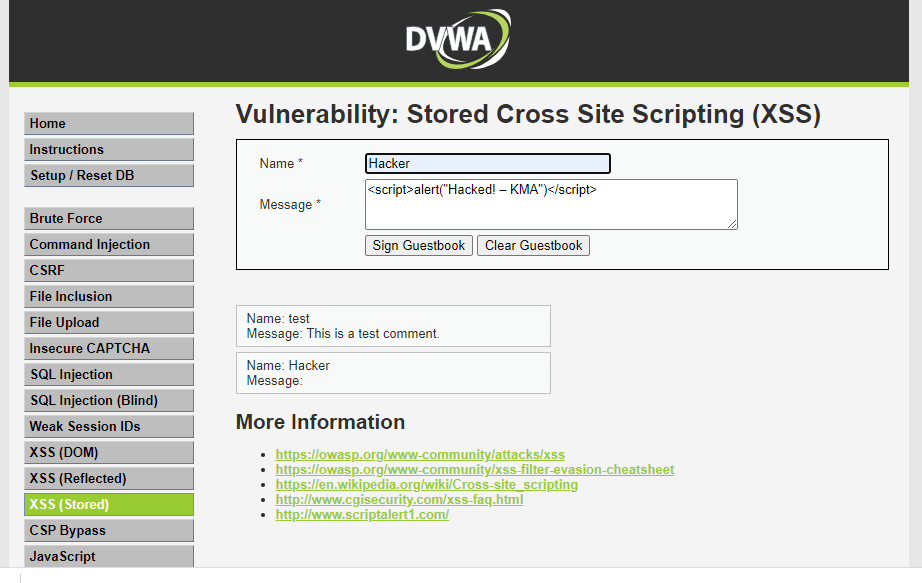
Vào SQL Injection nhập vào %' or '0'='0 và submit

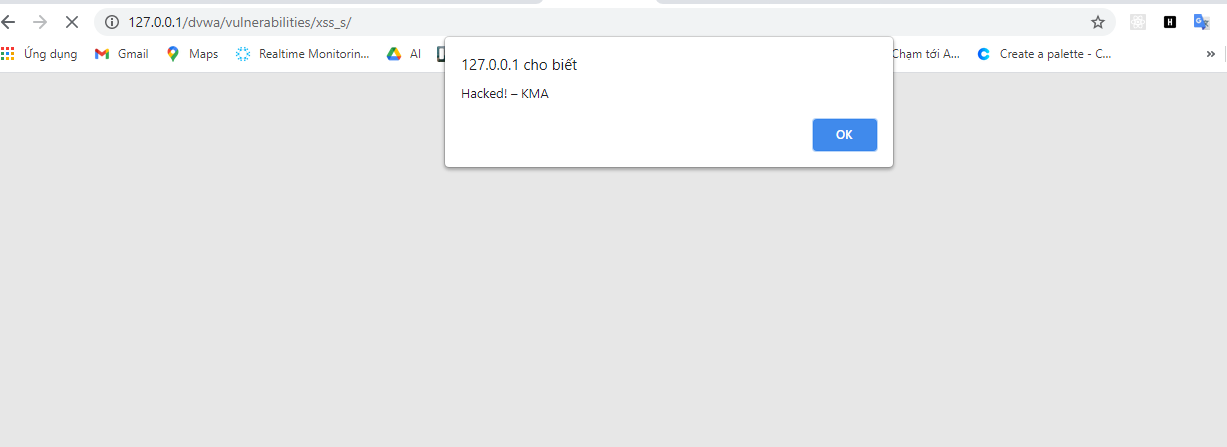


Kết quả sẽ nhận được thông tin của tất cả các users có trong cơ sở dữ liệu. Bởi vì câu truy vấn lúc này được hiểu là : SELECT \* FROM users WHERE user\_id = '%' or '0'='0'

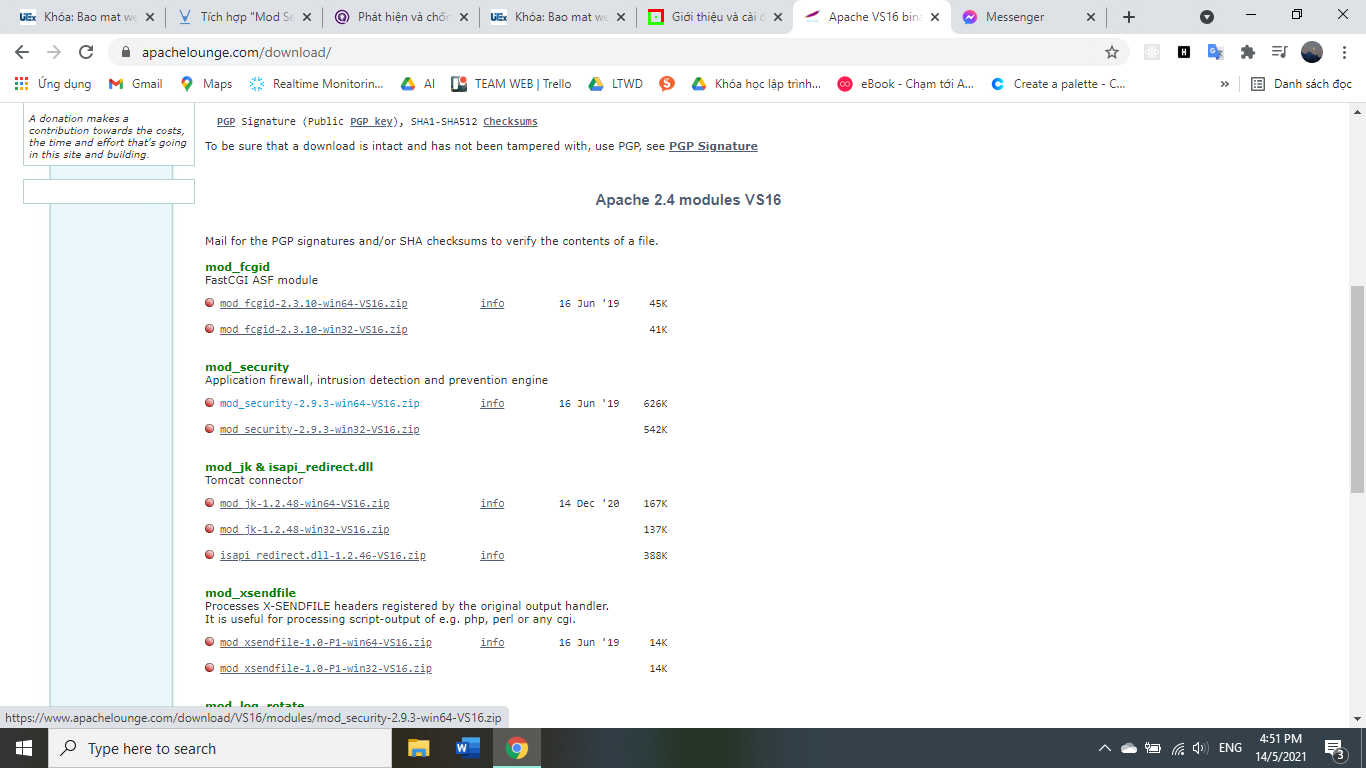
## 1.2 Thử nghiệm XSS

Vào XSS stored và submit đoạn script sau: <script>alert("Hacked! – KMA")</script>:



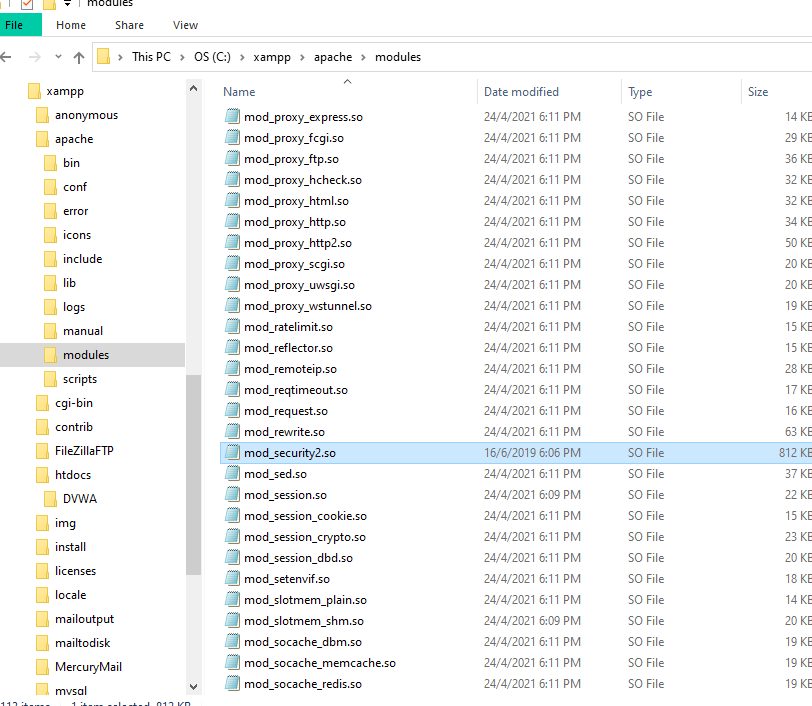


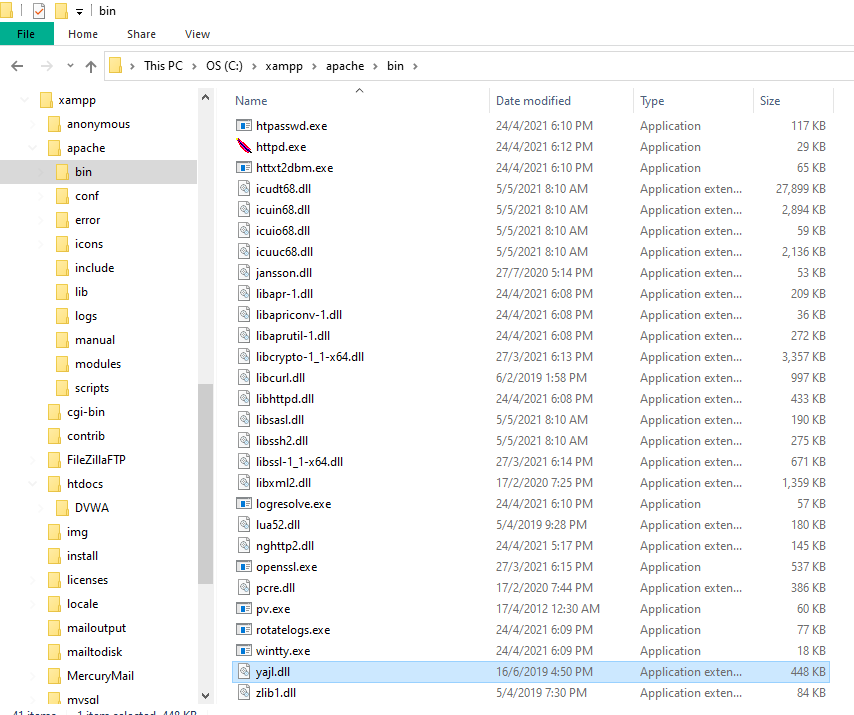
# 1.3 Cài đặt và cấu hình Mod Security

Download mod-security

Giải nén và tìm 2 file mod\_security2.so và yajl.dll trong thư mục vừa giải nén.

* copy mod\_security2.so vào ...\apache\modules
* copy yajl.dll vao ...\apache\bin





Mở file httpd.conf của Xampp và thêm vào các dòng sau:

LoadModule security2\_module modules/mod\_security2.so

SecRuleEngine DetectionOnly

<IfModule security2\_module>

SecRuleEngine On

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

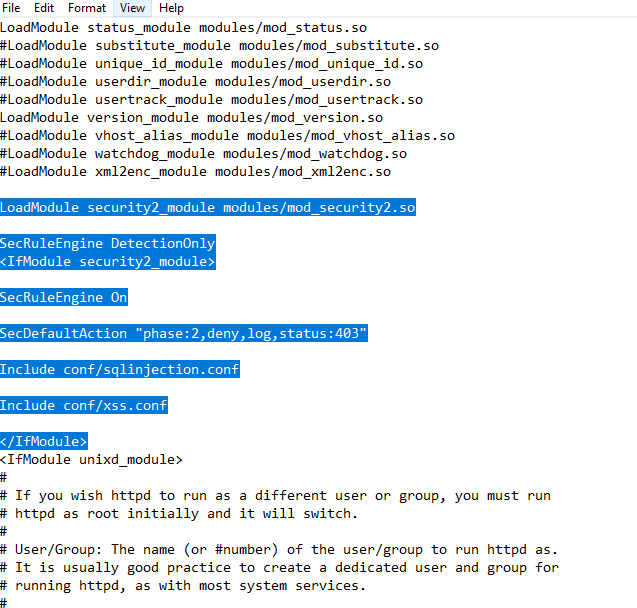
Include conf/sqlinjection.conf

Include conf/xss.conf

</IfModule>

*Đồng thời bỏ dấu # trước dòng:*

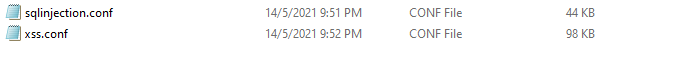
*LoadModule unique\_id\_module modules/mod\_unique\_id.so*



## 1.4 Tạo file conf để thiết lập rules

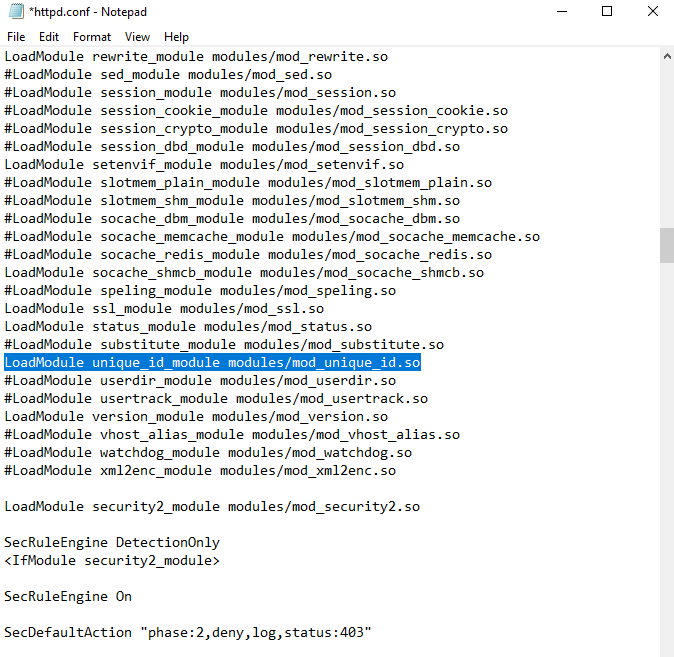
**Tiến hành tạo 2 file**sqlinjection.conf**và**xss.conf**trong thư mục**apache\conf**của Xampp.**

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



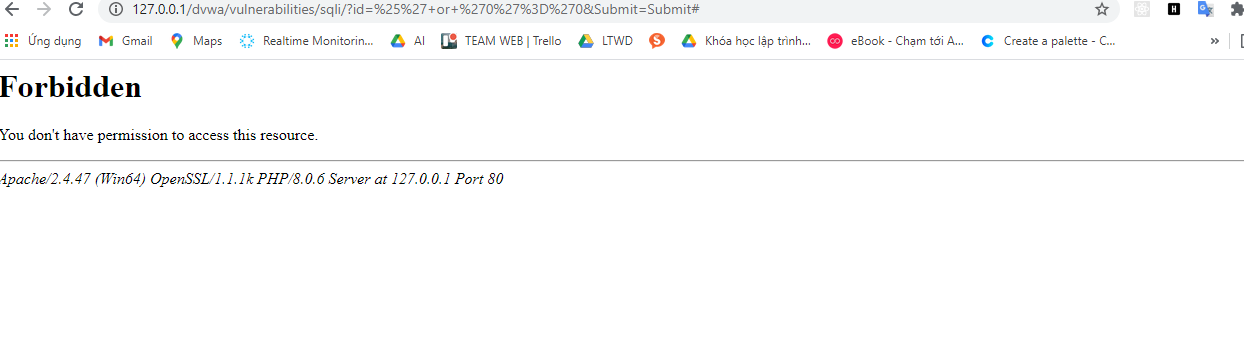
Sau đó bỏ dấu # ở dòng LoadModule unique\_id\_module modules/mod\_unique\_id.so

Trong file httpd.conf



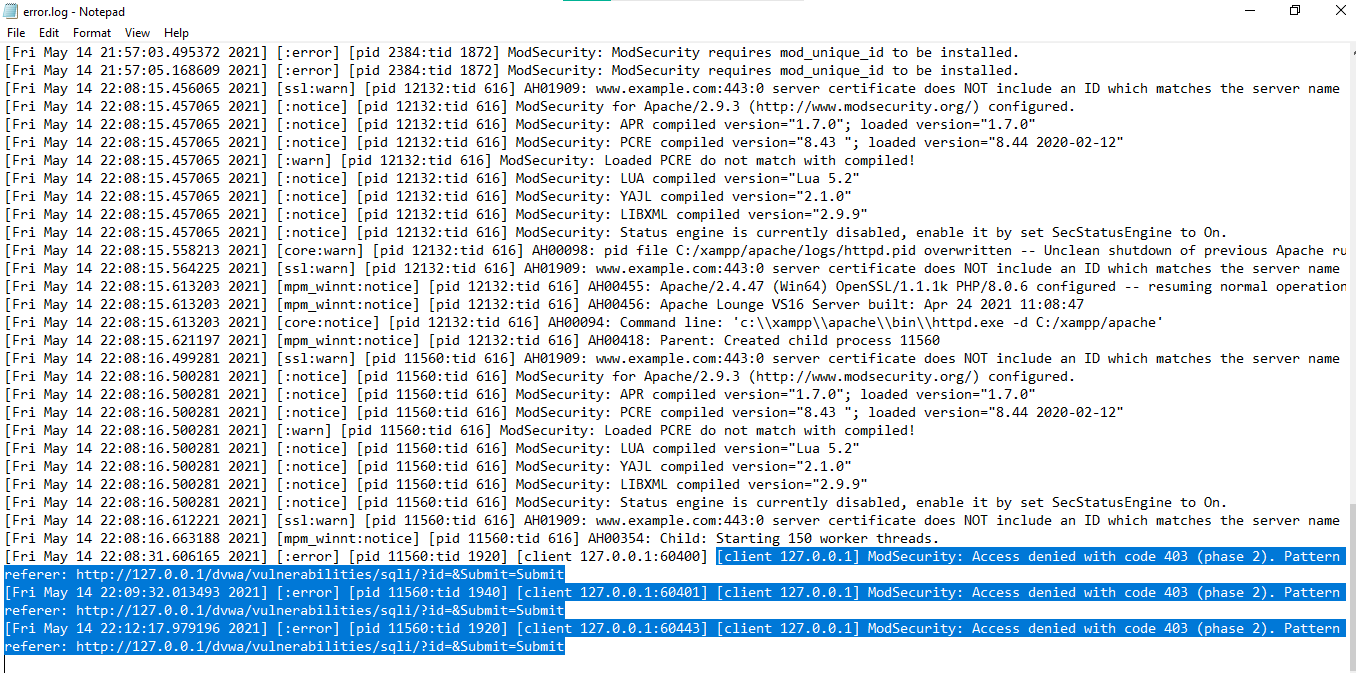
Tiến hành restart lại Xampp Apache. Thử nghiệm lại tấn công SQL Injection và XSS như ở phần 1.

 Kết quả như hình:



Trả về kết quả bị cấm.

Và file request bị chặn:



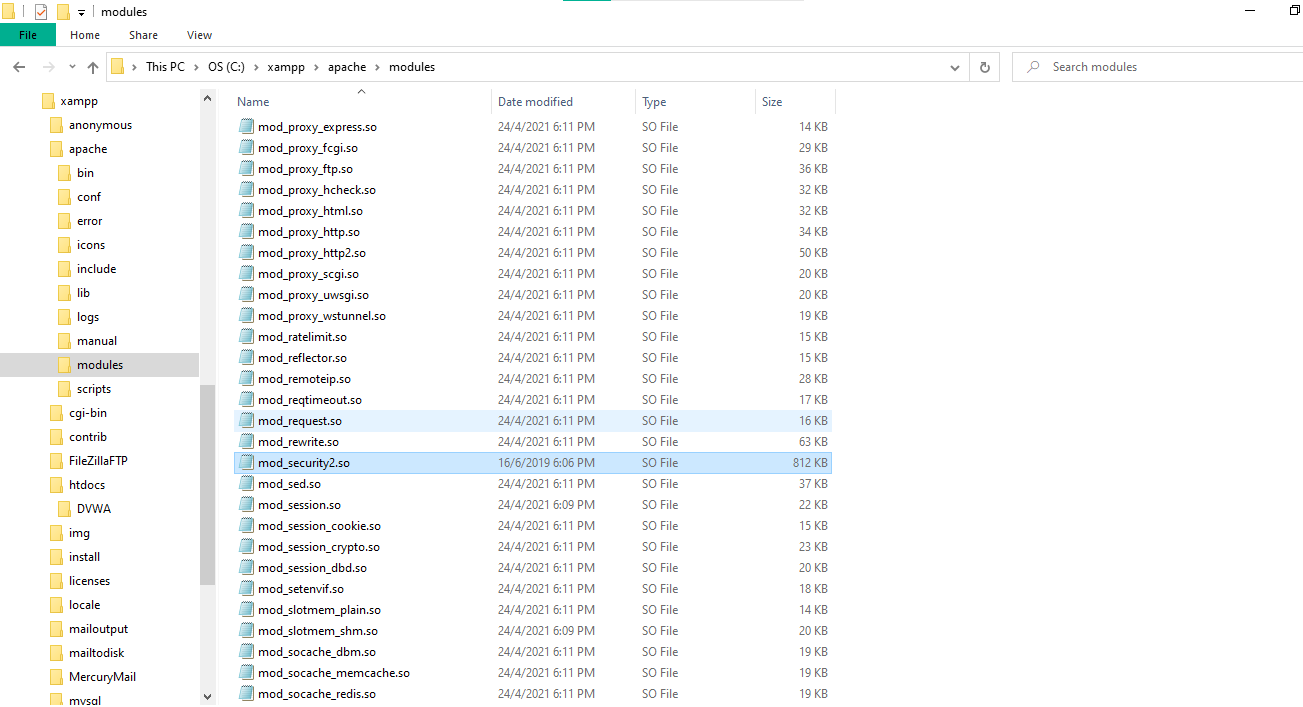
# **Bài 2: Phát hiện và chống xâm nhập Web Server với Mod Security**

Link: https://quantrimang.com/phat-hien-va-chong-xam-nhap-web-server-voi-mod-security-15314

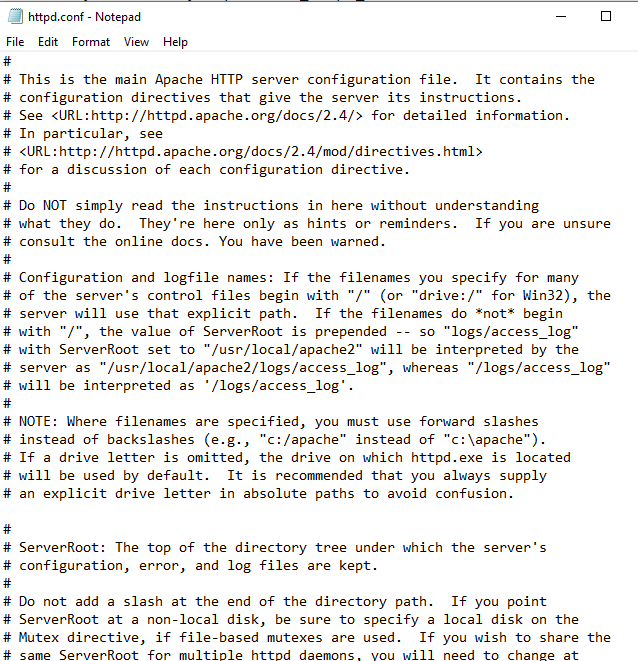
Cài đặt và cấu hình: tương tự như bài 1

Thực hiện install Mod-security

Sau đó copy file **mod\_security2.so** vào trong thư mục C:\xampp\apache\modules



Mở file httpd.conf để thực hiện cấu hình mod



Với đoạn code:

<IfModule mod\_security.c>

# cấu hình cho mod\_security

</IfModule>

Thêm dòng lệnh LoadModule security2\_module modules/mod\_security2.so

Một số lệnh cơ bản của Mod

Muốn dùng Mod thì bật giá trị:

SecFilterEngine On (or Off, DynamicOnly)

Tấn công trong Mod:

* Chống các kiểu tấn công thực thi:

SecFilter /etc/password

SecFilter /bin/ls

* Chống lại kiểu tấn công Directory traversal:

SecFilter "\.\./"

* Lọc các kí tự hay dùng trong shell code:

SecFilterForceByteRange 32 126

* Lọc các kí tụ hay dùng trong XSS attack:

SecFilter "<(.|\n)+>"

SecFilter "<[[:space:]]\*script"

* Chống lại kiểu tấn công XSS thông qua PHP session cookie:

SecFilterSelective ARG\_PHPSESSID "!^[0-9a-z]\*$"

SecFilterSelective COOKIE\_PHPSESSID "!^[0-9a-z]\*$"

* Hạn chế [sql injection](https://quantrimang.com/tan-cong-kieu-sql-injection-va-cac-phong-chong-trong-asp-net-34905) attack:

SecFilter "delete[[:space:]]+from"

SecFilter "insert[[:space:]]+into"

SecFilter "select.+from"

* Hạn chế MSSQL injection attack:

SecFilter xp\_enumdsn

SecFilter xp\_filelist

SecFilter xp\_availablemedia

SecFilter xp\_cmdshell

SecFilter xp\_regread

SecFilter xp\_regwrite

SecFilter xp\_regdeletekey

* Chống spam mail:

<Location /cgi-bin/FormMail>

SecFilterSelective "ARG\_recipient" "!@modsecurity\.org$"

</Location>

* Phát hiện xâm nhập:

SecFilterSelective OUTPUT "Volume Serial Number"

SecFilterSelective OUTPUT "Command completed"

SecFilterSelective OUTPUT "Bad command or filename"

SecFilterSelective OUTPUT "file(s) copied"

SecFilterSelective OUTPUT "Index of /cgi-bin/"

SecFilterSelective OUTPUT ".\*uid\=\("

* Nếu muốn ghi lại log:

SecAuditLog logs/audit.log

SecFilterDebugLog logs/modsec.log

SecFilterDebugLevel 0

* Muốn mod\_security phân tích POST request, dùng:

SecFilterScanPOST On

* Để mod\_security \*kiểm tra\* URL encoding và UTF-8.

SecFilterCheckURLEncoding On

SecFilterCheckUnicodeEncoding On

# **Bài 3: Giới thiệu và cài đặt Mod\_security (Phần 1)**

Link: <https://anninhmang.net/bao-mat/gioi-thieu-va-cai-dat-mod_security-phan-1/>

Cấu hình tương tự như bài 1 và bài 2 đã thực hiện.