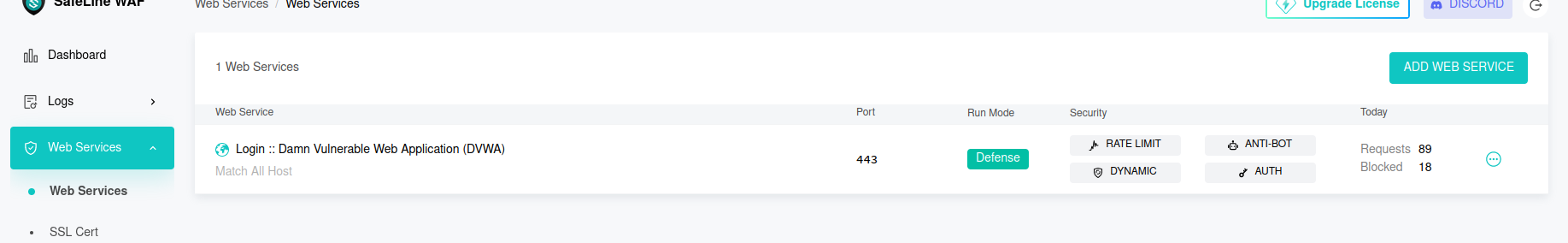
**Chuẩn bị:**

WAF sử dụng: Safeline WAF (open source)

Web thử nghiệm: DVWA

-Cấu hình: cài đặt safeline phát hiện tấn công trên port 443(có thể thay đổi port) của DVWA



**Các kịch bản :**

Kịch bản 1.Phát hiện tấn công XSS

Kịch bản 2: Phát hiện tấn công Command Injection

Kịch bản 3: Phát hiện tấn công SQL Injection

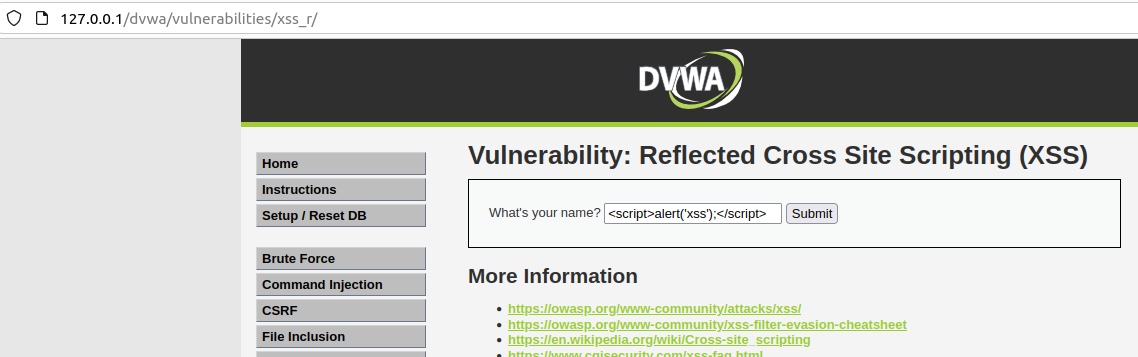
Kịch bản 4: Phát hiện tấn công File Upload

**Thực hành**

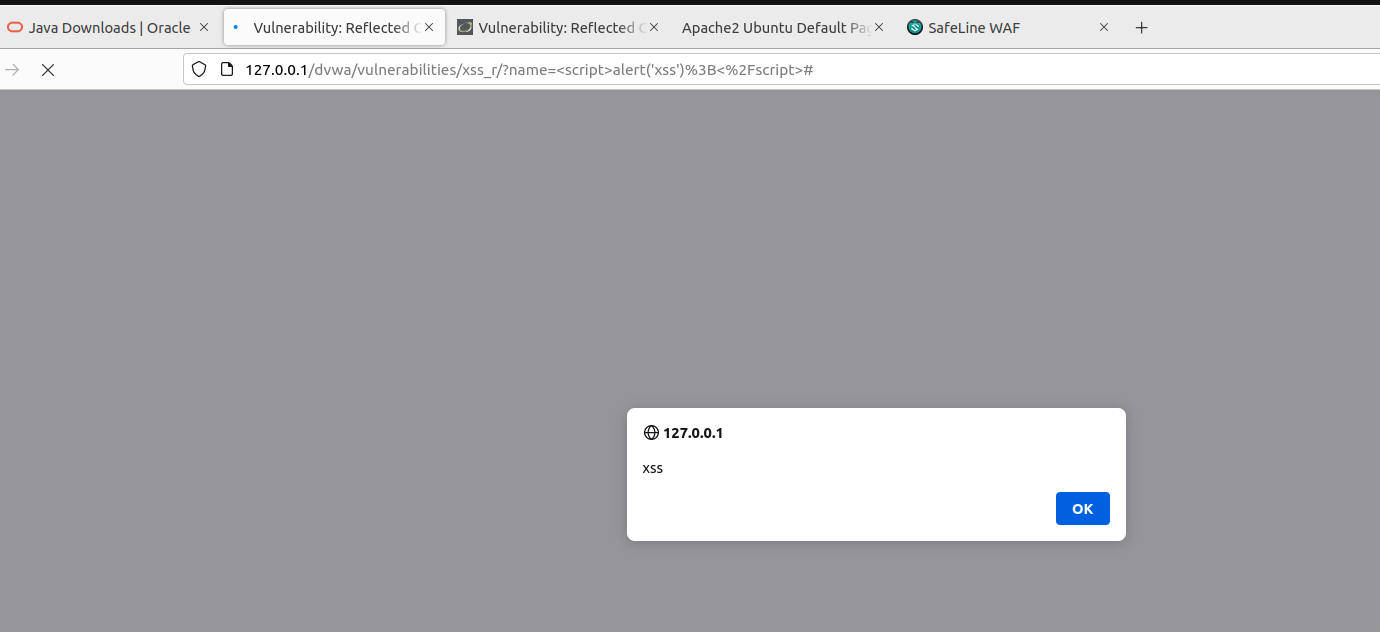
**Kịch bản 1: Phát hiện tấn công XSS:**

* Tấn công vào dvwa ở port 80:

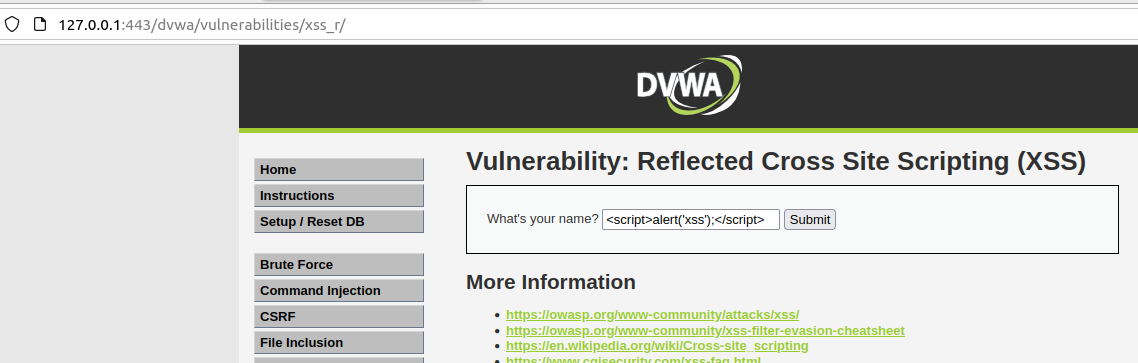
Sử dụng <script>alert('xss');</script>



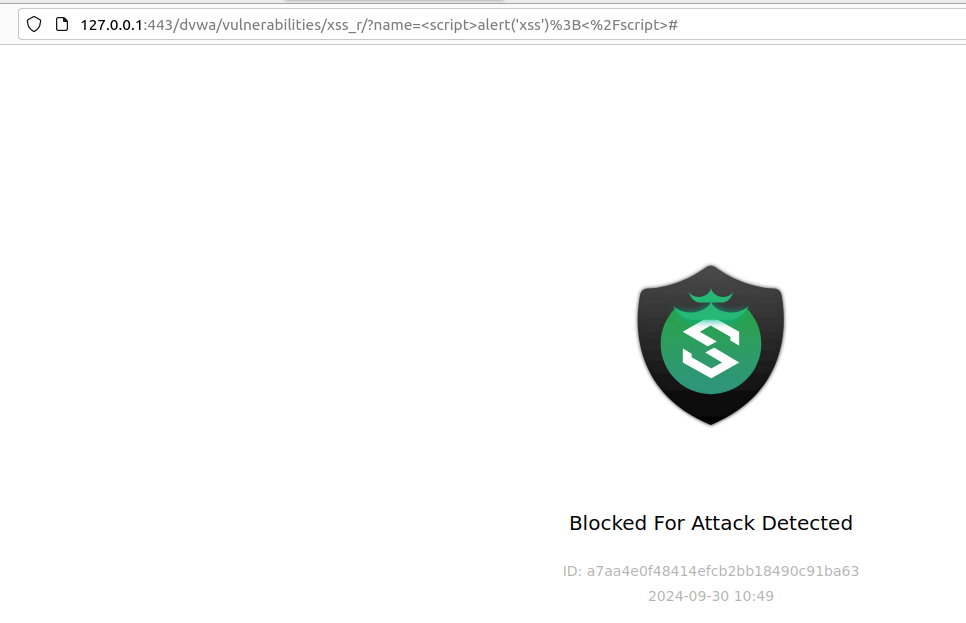
Kết quả:



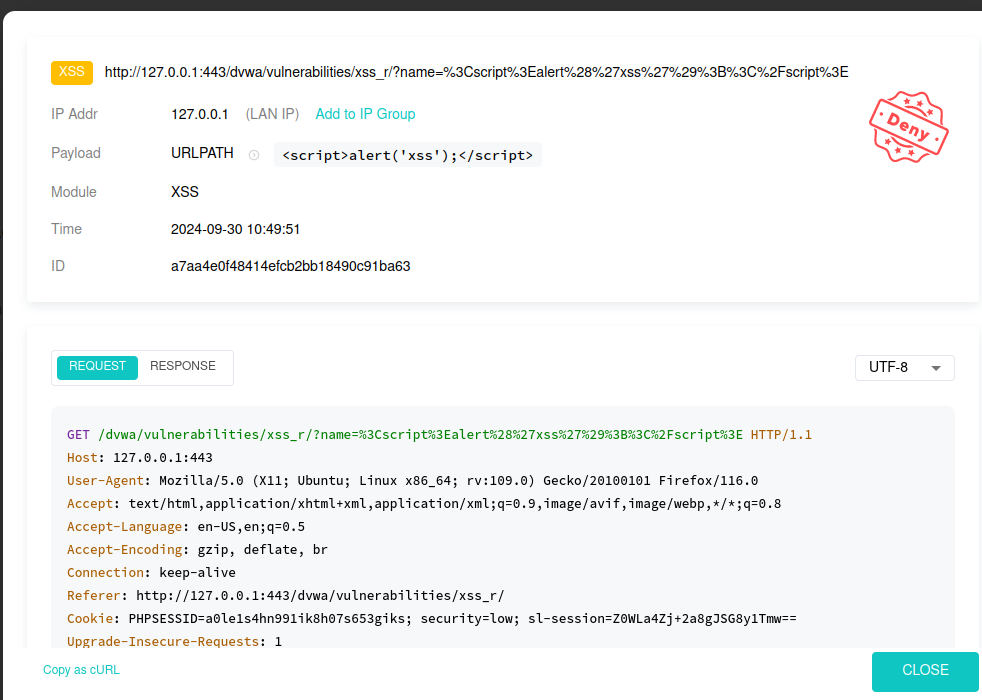
* Tấn công vào dvwa ở port 443(port cài Safeline WAF)



Kết quả : SafeLine đã phát hiện và chặn user tấn công XSS

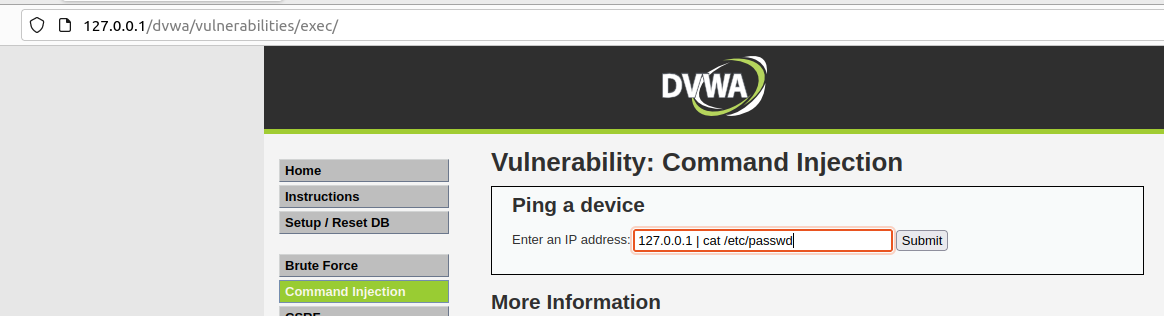


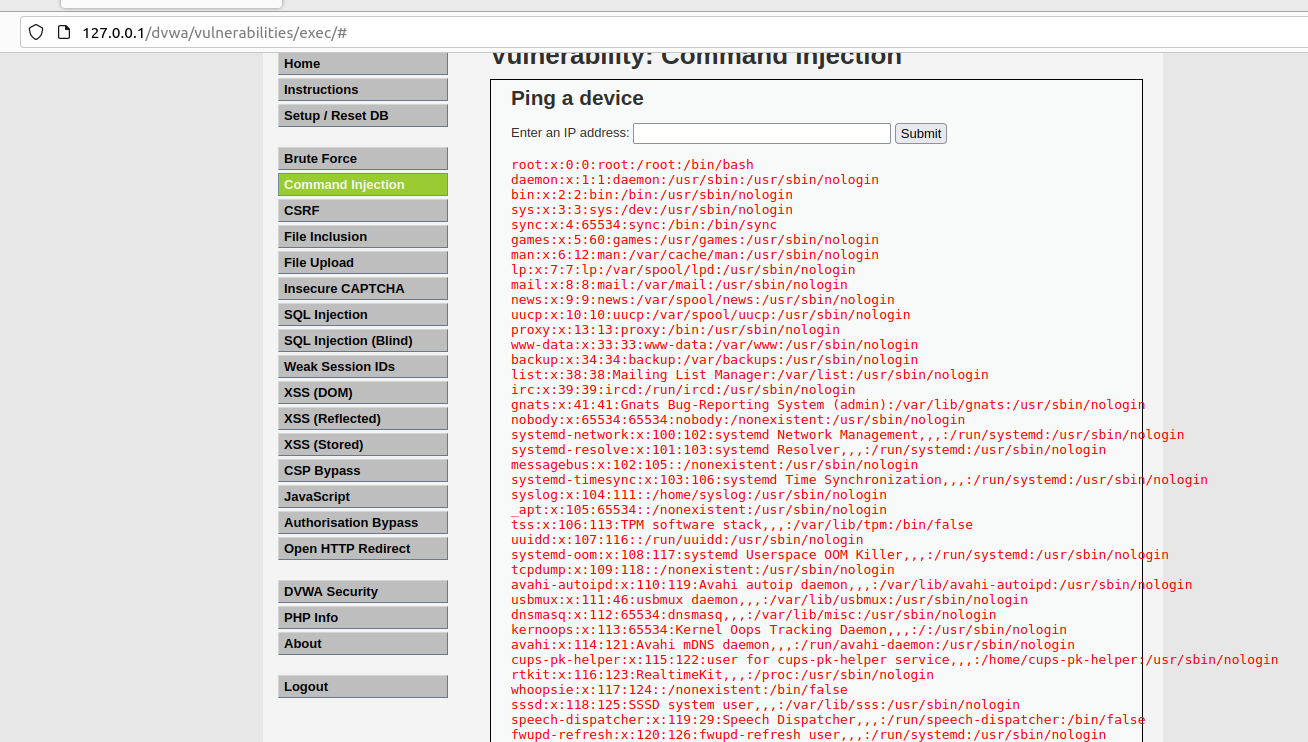
Ở giao diện SafeLine ta có thể theo dõi chi tiết tấn công :



**Kịch bản 2: tấn công Command Injection**

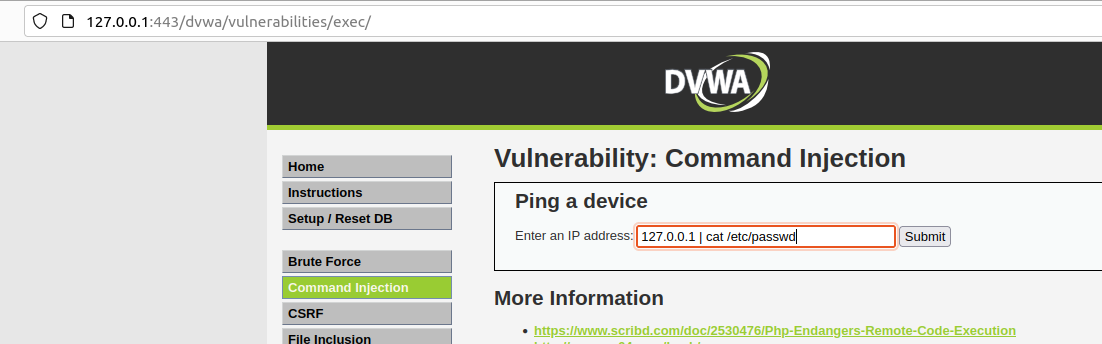
-Tấn cổng ở port 80:



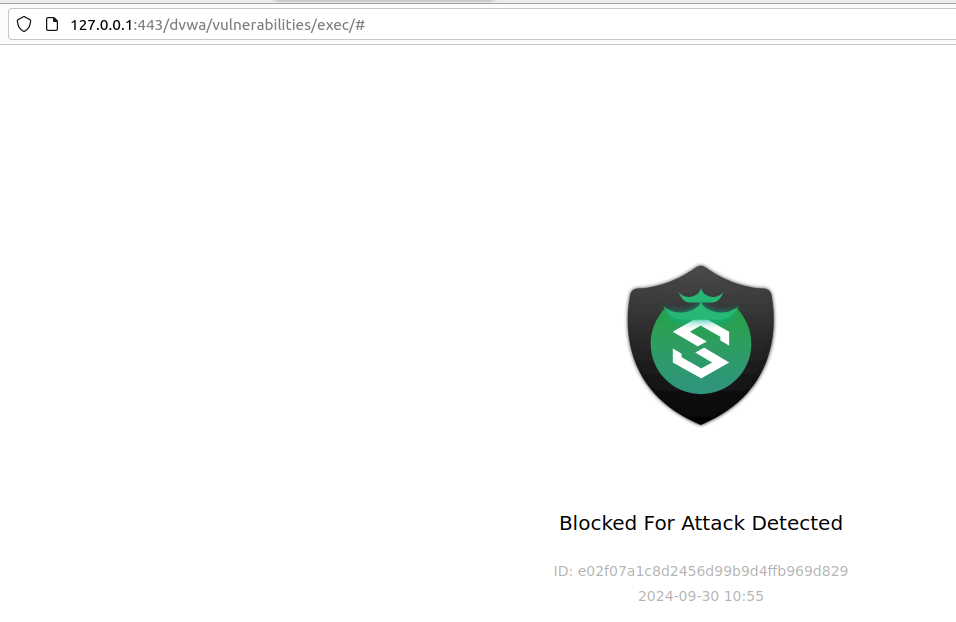
-Kết quả : 

Ta có thể xem được tất cả các thông tin tài khoản người dùng lưu trữ tên máy.

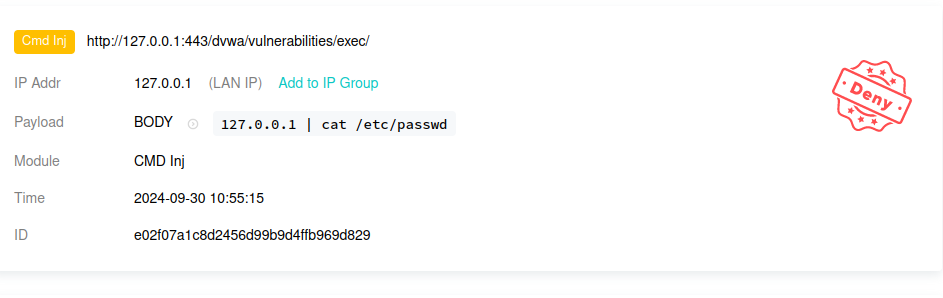
-Khi tấn công vào port có cài Safeline WAF(port 443):



Kết quả : WAF phát hiện và đã chặn tấn công command injection

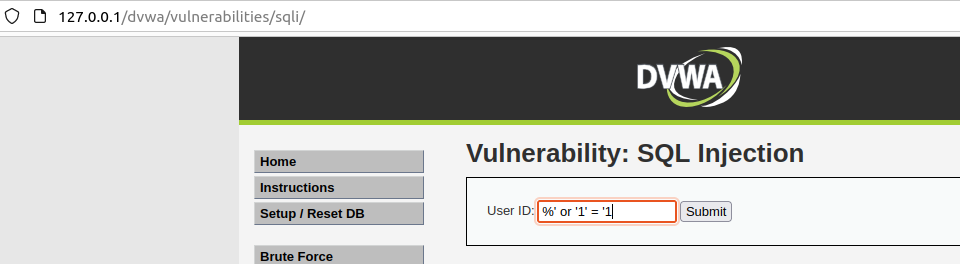


-Ở giao diện Safeline WAF:

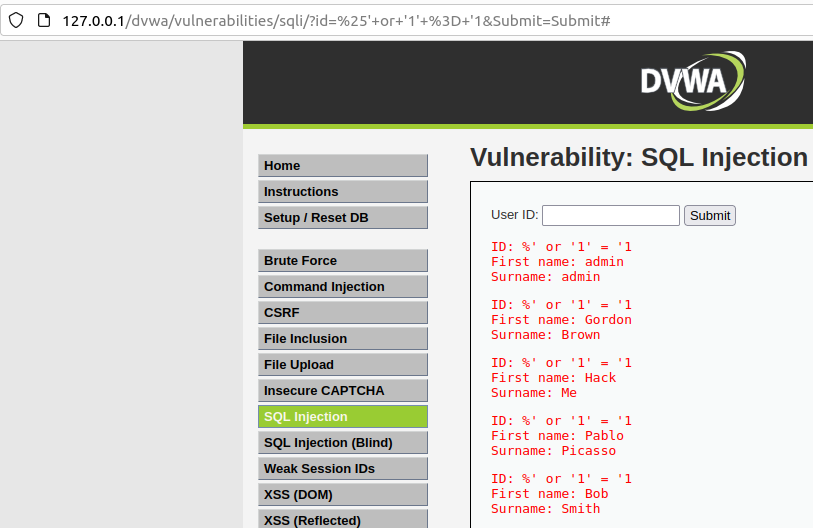


Kịch bản 3: tấn công SQL Injection

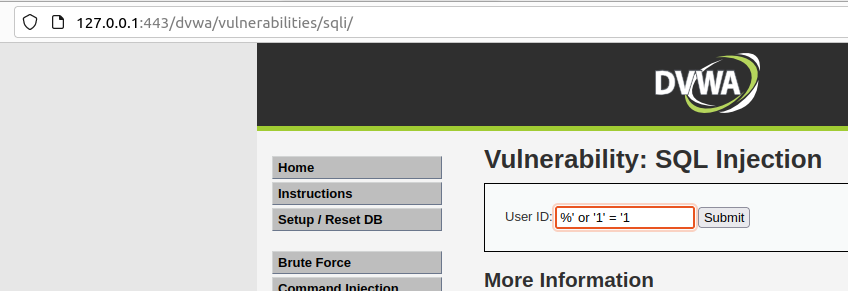
-Tấn công ở port 80:



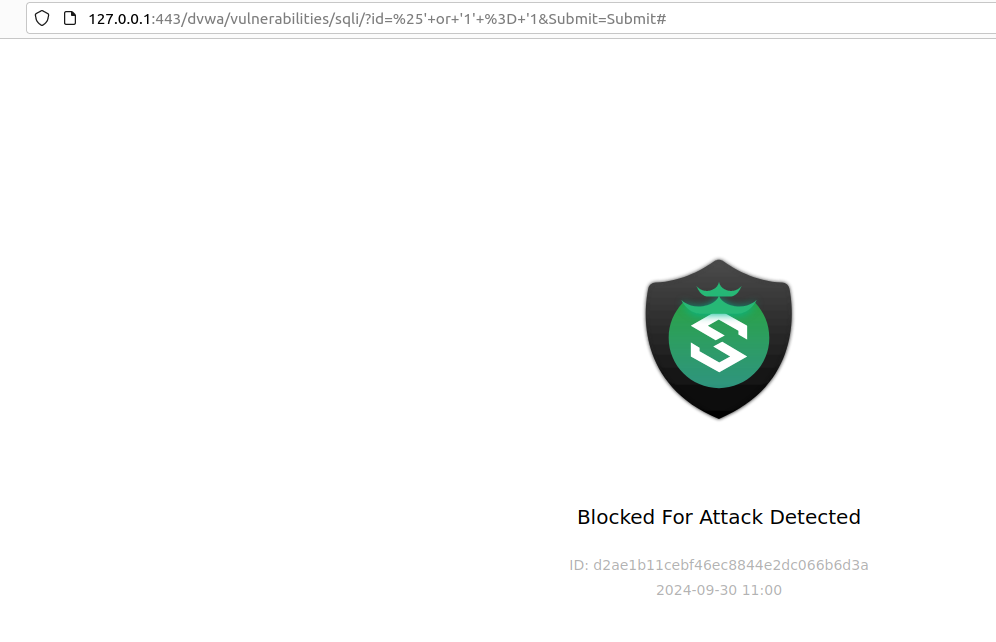
Kết quả : ta có thể xem được firstname và surname của tất cả người dùng



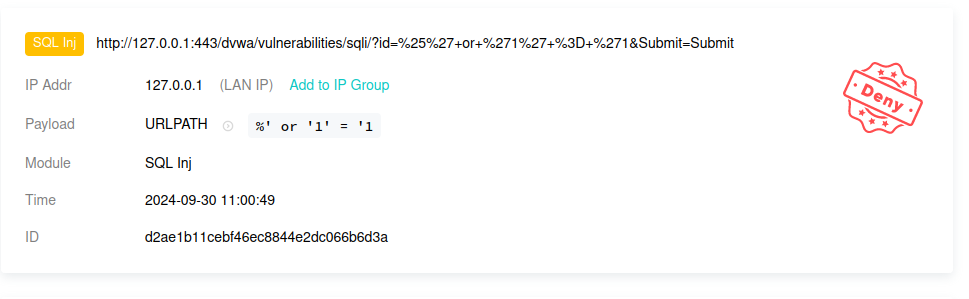
-Tấn công ở port đã cài Safeline WAF(443)



Kết quả : SafeLine đã phát hiện và chặn tấn công

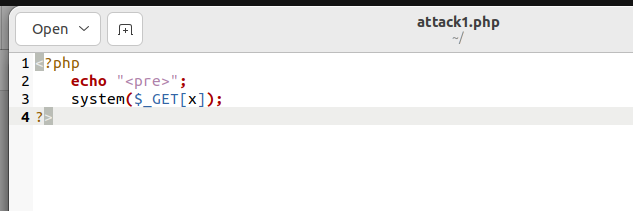


Ở giao diện SafeLine có thể theo dõi chi tiết tấn công

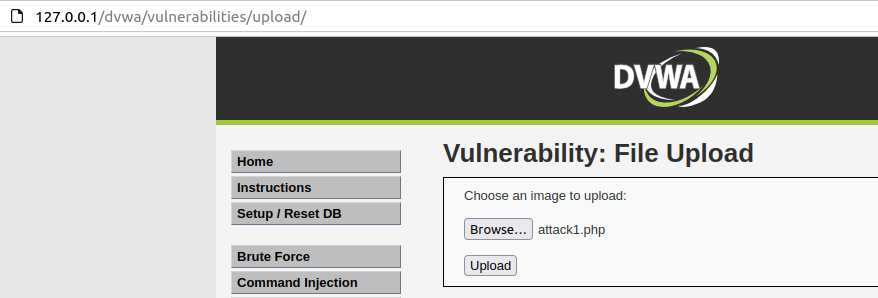


**Kịch bản 4: Phát hiện tấn công File Upload**

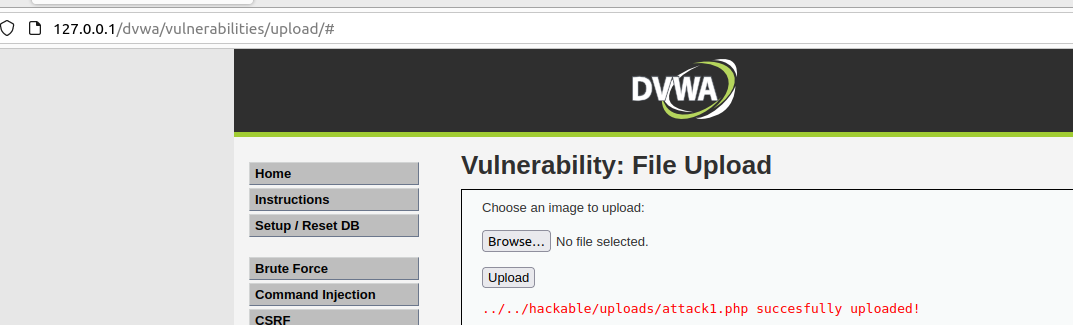
Chuẩn bị : tạo 1 file php nhằm mục đích



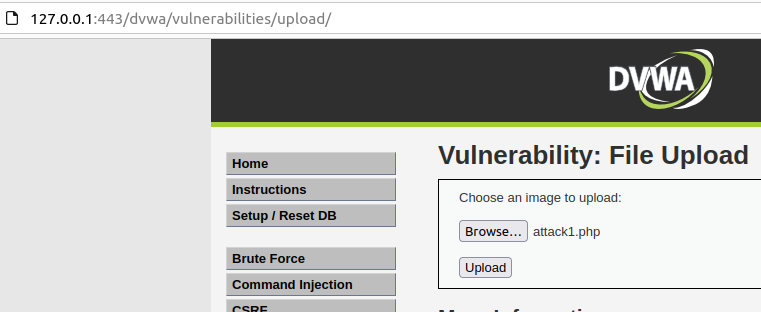
-Tấn công ở port 80 :

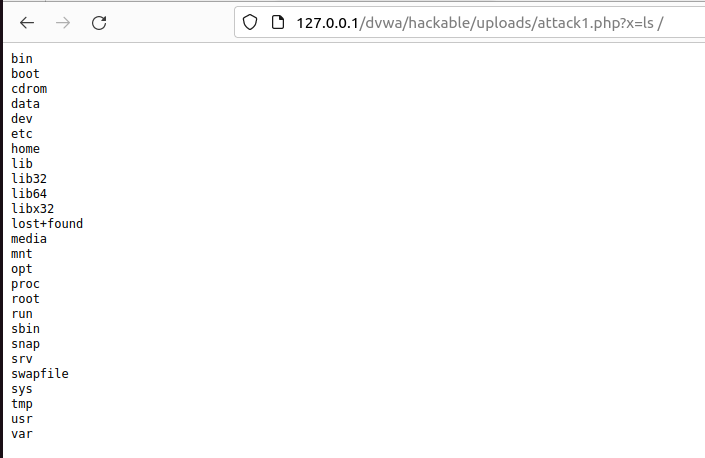


Kết quả :

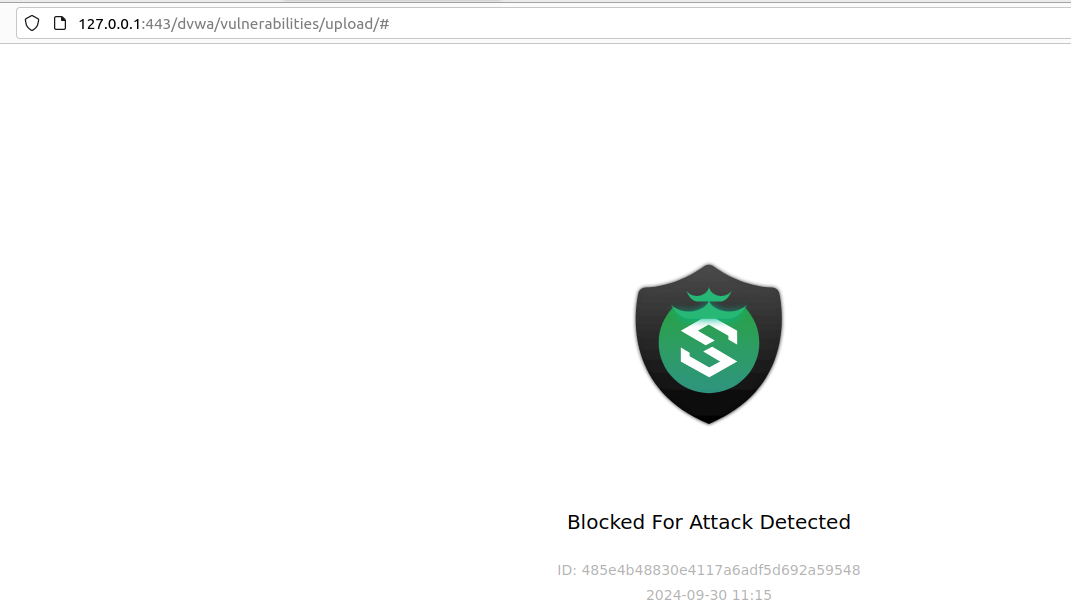


-Tấn công ở port đã cài WAF (443)





Kết quả : SafeLine đã phát hiện và đã chặn tấn công



Chi tiết tấn công ở giao diện SafeLine

