**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

**Họ và tên*:*** Hoàng Hải Đăng

Lớp K10\_CNPM3

***Yêu cầu kết quả thực hành:***

Báo cáo kết quả thực hành có tên theo định dạng HoTenSV\_MSSV\_Lab06.docx

Trình bày quá trình kiểm thử theo mẫu sau

**Phần 1: Kiểm thử XSS**

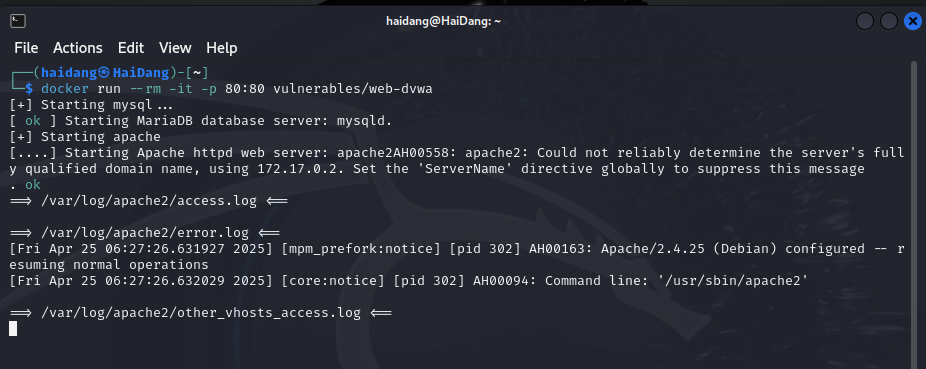
Thực hiện kiểm thử lỗ hổng XSS trên website: chọn 1 trong các trang sau để thử nghiệm

1. [http://demo.testfire.net](http://demo.testfire.net/)`
2. [http://php.testsparker.com](http://php.testsparker.com/)
3. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
4. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
5. [http://testphp.vulnweb.com](http://testphp.vulnweb.com/)
6. [http://www.webscantest.com](http://www.webscantest.com/)
7. [http://testhtml5.vulnweb.com](http://testhtml5.vulnweb.com/)
8. [http://aspnet.testsparker.com](http://aspnet.testsparker.com/)
9. [http://zero.webappsecurity.com](http://zero.webappsecurity.com/)

**Câu 1**

Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV.

Bước 1: Chạy DVWA bằng lệnh docker run --rm -it -p 80:80 vulnerables/web-dvwa

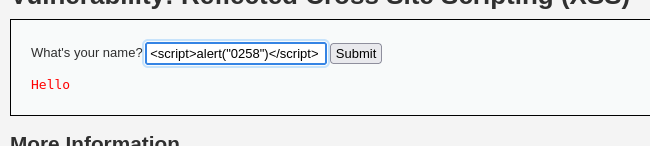


Truy cập vào DVWA

Đăng nhập DVWA

Truy cập vào website DVWA, chọn mục XSS(Reflected)

Nhập lệnh <script> alert(“0258) </script> để hiện ra thông báo 4 số cuối của mã số sinh viên



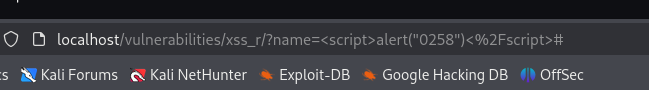
Bấm submit



Kết quả cảu thông báo

Hãy giải thích:

**-** Xác định các tham số đầu vào: name

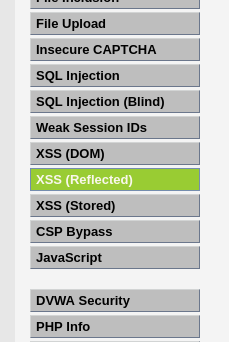


- Xác định giá trị đầu vào xuất hiện trong trang kết quả: alert(“0258”)

**-** Các bước kiểm thử và phán đoán theo các bước kiểm thử và logic trong phán đoán

Bước 1: Đăng nhập vào DVWA

Bước 2: Chọn vào XSS (Reflected)



Bước 3: Nhập vào ô input đoạn lệnh <script> alert(“0258”) </script>

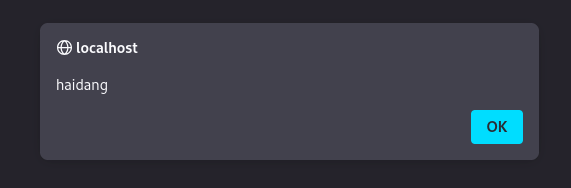
- Giá trị kiểm thử cho thấy lỗ hổng và giải thích: Hộp thoại thông báo hiện lên với nội dung "0258" Lý do Ứng dụng **không lọc hoặc mã hóa** đầu vào, chèn trực tiếp vào HTML → **thực thi JavaScript**

**Câu 2**

Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa tên của sinh viên. Điểm cho mỗi tham số đầu vào đã kiểm thử được:

Truy cập vào website DVWA, chọn mục XSS(Reflected)

Nhập lệnh <script> alert(“haidang”) </script> để hiện ra thông báo tên sinh viên



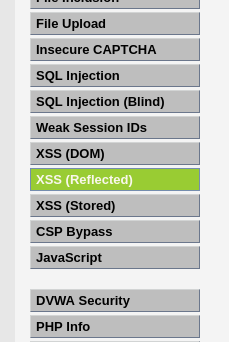
**-** Xác định các tham số đầu vào: name

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: <script> alert(“haidang”) </script>

**-** Các bước kiểm thử và phán đoán:

Bước 1: Đăng nhập vào DVWA

Bước 2: Chọn XXS (reflected)



Bước 3: nhập vào ô input lệnh <script> alert(“haidang”)</script>

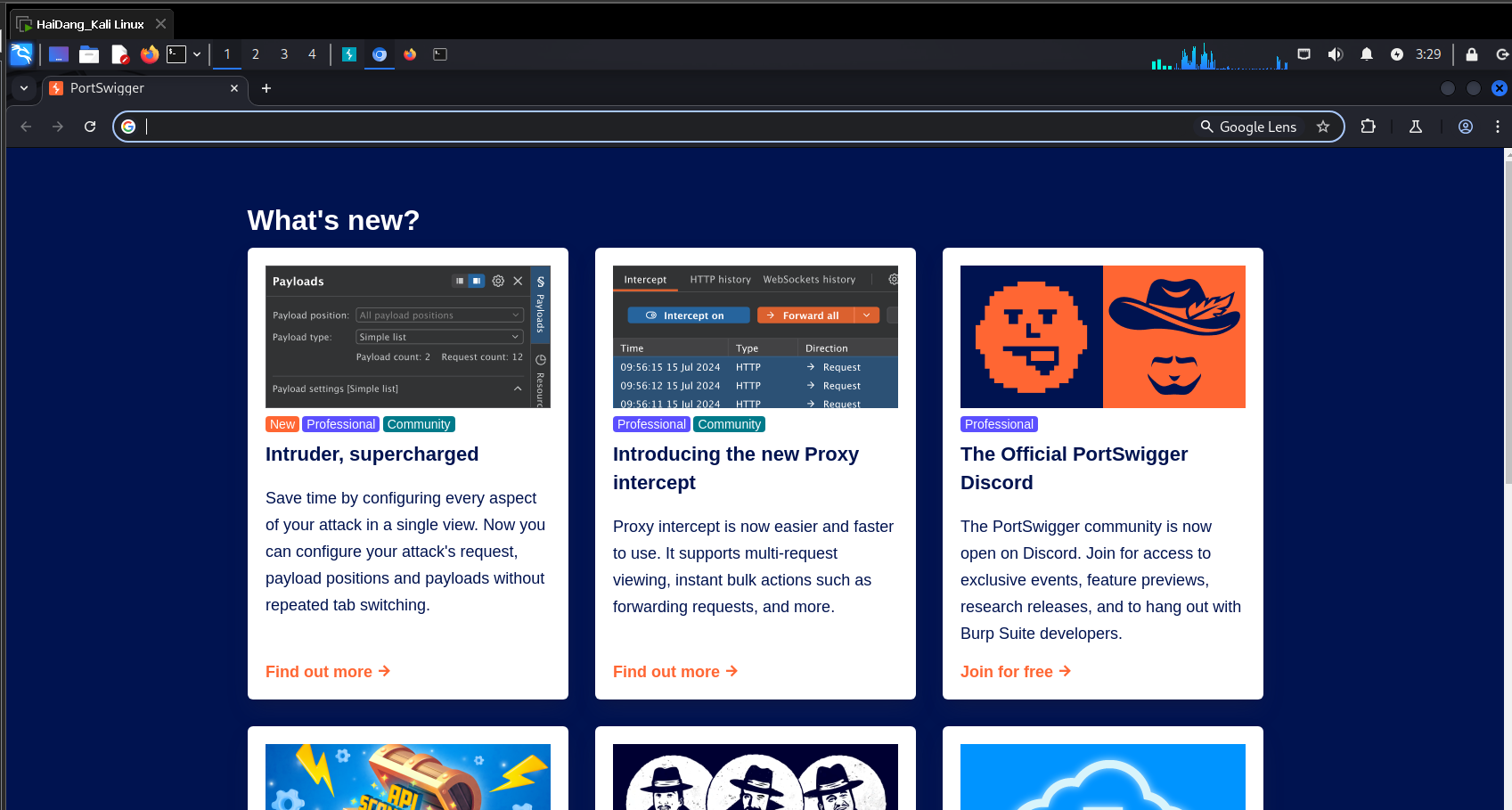
- Giá trị kiểm thử cho thấy lỗ hổng và giải thích: **0.5 điểm**

**Phần 2: Kiểm thử CSRF (2 điểm)**

Trình bày các bước thực hiện và kết quả kiểm thử lỗ hổng CSRF trên website chọn 1 trong các trang sau để thử nghiệm

Bật Intercept

Open browser



Truy cập trang web [http://php.testsparker.com](http://php.testsparker.com/)