BÁO CÁO BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

Họ và tên: Vũ Trọng Phương

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`

2. http://php.testsparker.com

3. http://testasp.vulnweb.com

4. http://testasp.vulnweb.com

5. http://testphp.vulnweb.com

6. http://www.webscantest.com

7. http://testhtml5.vulnweb.com

8. http://aspnet.testsparker.com

9. http://zero.webappsecurity.com

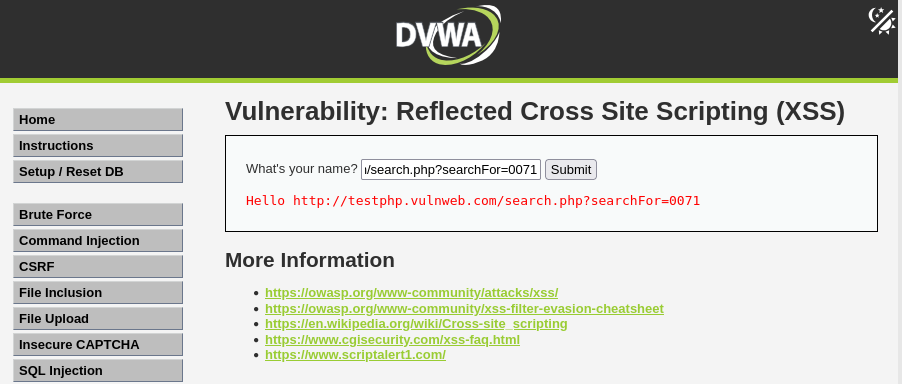
Câu 1

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

Hãy giải thích:

- Xác định các tham số đầu vào: 0.25 điểm

Chọn trang web <http://testphp.vulnweb.com>   
nhập <http://testphp.vulnweb.com/search.php?searchFor=0071> vào XSS



Tham số đầu vào chính là **searchFor** trong search.php, vì nó dễ truy cập và có khả năng cao được phản ánh trong phản hồi.

Nhập Mã số sinh vien mình vào là 0071



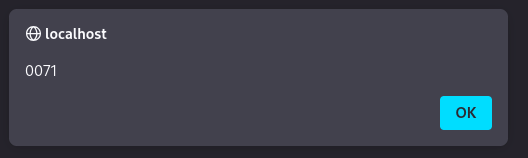
Đầu vào là 0071

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: 0.25 điểm

<http://localhost/dvwa/vulnerabilities/xss_r/?name=0071#>

- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

<script>alert('0071')</script>



Bằng cách nhập link

http://localhost/dvwa/vulnerabilities/xss\_r/?name=%3Cscript%3Ealert%28%270071%27%29%3C%2Fscript%3E#

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

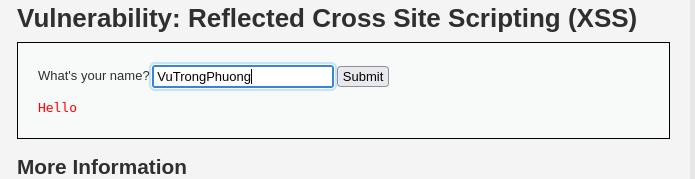
* Đây là một đoạn mã JavaScript hợp lệ.
  + Khi chèn vào input "MSSV" và trang web không lọc nội dung → mã được thực thi trên trình duyệt.
  + Lỗ hổng nằm ở việc giá trị người dùng nhập được phản hồi trực tiếp lên trang HTML mà không qua xử lý hay mã hóa an toàn, dẫn đến XSS Reflected.

Câu 2

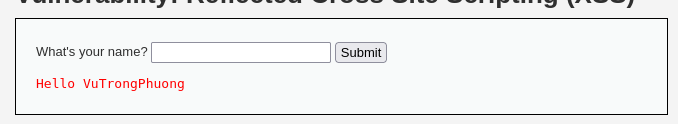
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa tên của sinh viên.

Điểm cho mỗi tham số đầu vào đã kiểm thử được:

- Xác định các tham số đầu vào: 0.25 điểm



Sau đó nhân Submit



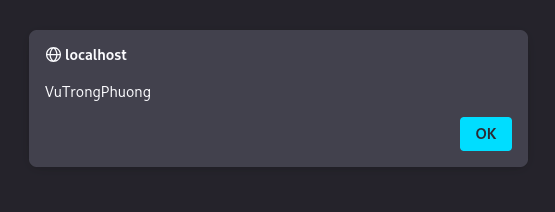
- Xác định giá trị đầu vào xuất hiện trong trang kết quả: 0.25 điểm

<http://localhost/dvwa/vulnerabilities/xss_r/?name=VuTrongPhuong#>

- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

Bằng cách nhập lệnh

<script>alert('VuTrongPhuong')</script>



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

* Đây là một đoạn mã JavaScript hợp lệ.
  + Khi chèn vào input "Tên" và trang web không lọc nội dung → mã được thực thi trên trình duyệt.
  + Lỗ hổng nằm ở việc giá trị người dùng nhập được phản hồi trực tiếp lên trang HTML mà không qua xử lý hay mã hóa an toàn, dẫn đến XSS Reflected.

Câu 3

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

Hãy giải thích:

- Xác định các tham số đầu vào: 0.25 điểm

Nhập Mã số sinh vien mình vào là 0071



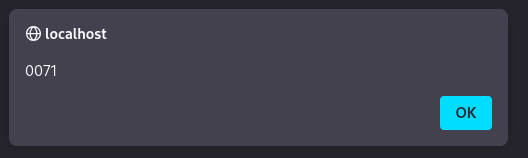
Đầu vào là 0071

- Xác định giá trị đầu vào xuất hiện trong trang kết quả: 0.25 điểm

<http://localhost/dvwa/vulnerabilities/xss_r/?name=0071#>

- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

<script>alert('0071')</script>



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

* Đây là một đoạn mã JavaScript hợp lệ.
  + Khi chèn vào input "MSSV" và trang web không lọc nội dung → mã được thực thi trên trình duyệt.
  + Lỗ hổng nằm ở việc giá trị người dùng nhập được phản hồi trực tiếp lên trang HTML mà không qua xử lý hay mã hóa an toàn, dẫn đến XSS Reflected.