**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

***Họ và tên: Hoàng Văn Hiếu***

***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

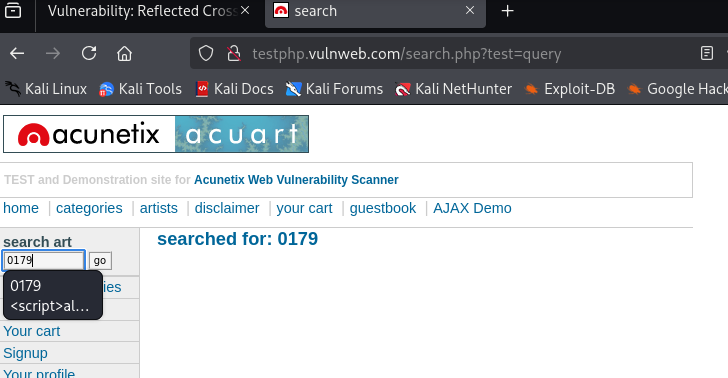
1. [http://demo.testfire.net](http://demo.testfire.net/)`
2. [http://php.testsparker.com](http://php.testsparker.com/)
3. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
4. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
5. [http://testphp.vulnweb.com](http://testphp.vulnweb.com/)
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**

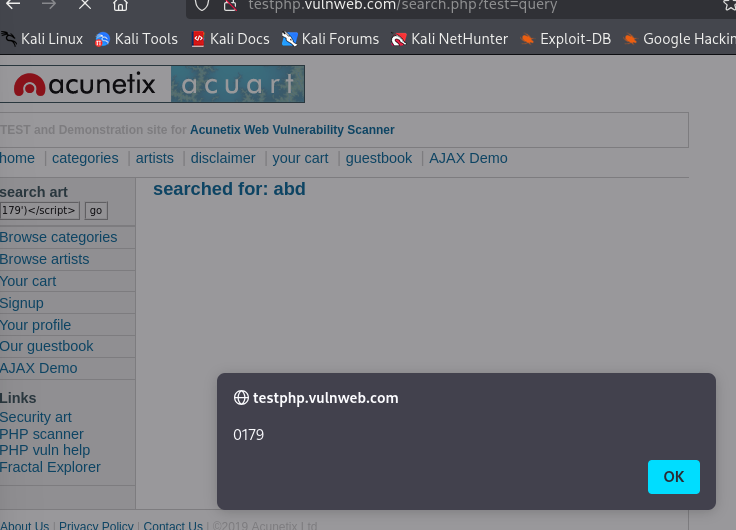
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV. Hãy giải thích:

**-** Xác định các tham số đầu vào: **0.25 điểm**

* **Tham số đầu vào nhập vào ô là 0179 -> hiển thị như hình**
* **tham số đầu vào test= trên URL**

****

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

****

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

**Bước 1:** Truy cập vào trang web và tìm trường đầu vào (input field).

**Bước 2:** Nhập đoạn mã sau vào trường đầu vào:

**<script>alert(‘1050179’)</script>**

**Bước 3:** Gửi dữ liệu và quan sát kết quả. Nếu thông báo alert(‘1050179’) xuất hiện, trang web đã bị lỗ hổng XSS.

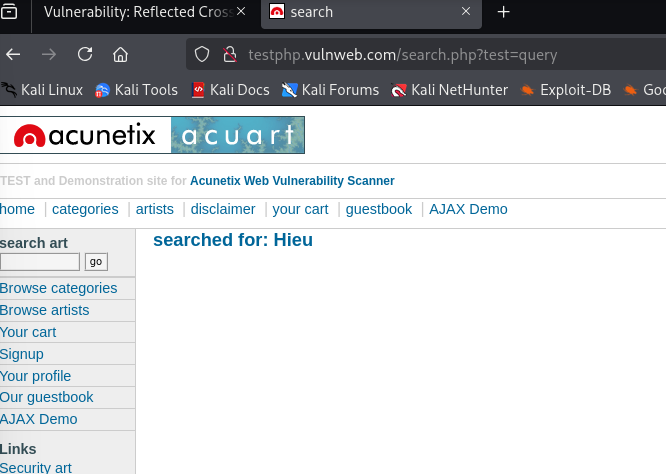
- Giá trị kiểm thử cho thấy lỗ hổng và giải thích: **0.5 điểm**

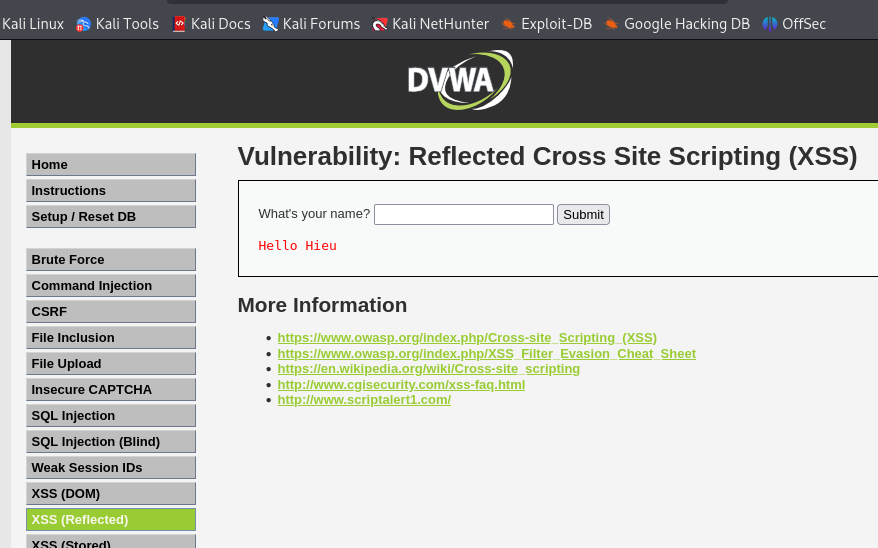
Nếu thông báo alert('1050179') hiển thị trên màn hình, điều này chứng tỏ lỗ hổng XSS tồn tại. Điều này cho thấy rằng trang web không thực hiện kiểm tra hoặc mã hóa đúng cách đầu vào của người dùng.

**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:

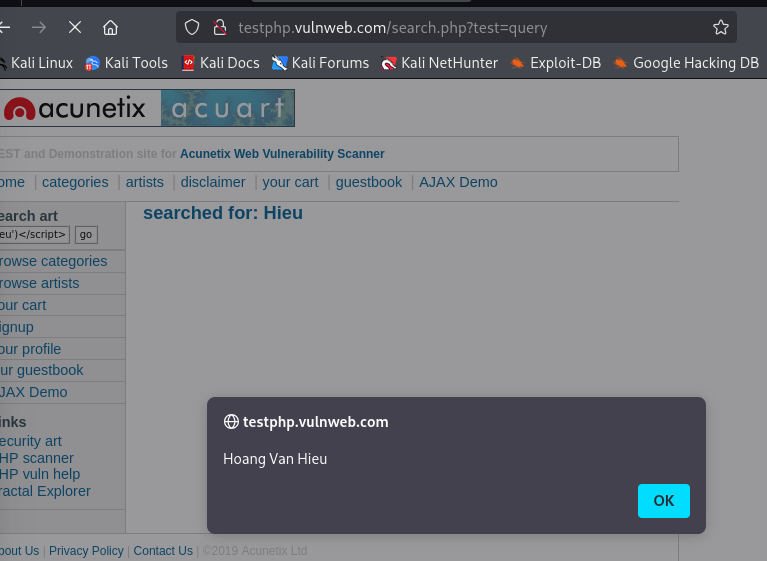
**-** Xác định các tham số đầu vào: **0.25 điểm**

****

****

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

**<script>alert('Hoang Van Hieu')</script>**

****

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

**Bước 1:** Truy cập vào trang web và tìm trường đầu vào (input field).

**Bước 2:** Nhập đoạn mã sau vào trường đầu vào:

**<script>alert(‘Hoang Van Hieu’)</script>**

**Bước 3:** Gửi dữ liệu và quan sát kết quả. Nếu thông báo alert(‘Hoàng Văn Hiếu’) xuất hiện, điều đó có nghĩa là bạn đã khai thác được lỗ hổng XSS.

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

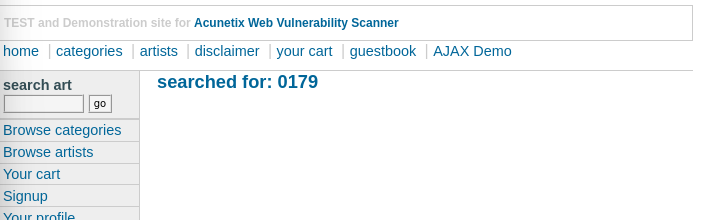
Nếu thông báo alert(‘Hoang Van Hieu’) xuất hiện, điều này cho thấy trang web có lỗ hổng XSS. Mã JavaScript đã được thực thi mà không bị lọc hoặc mã hóa đúng cách.

**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:

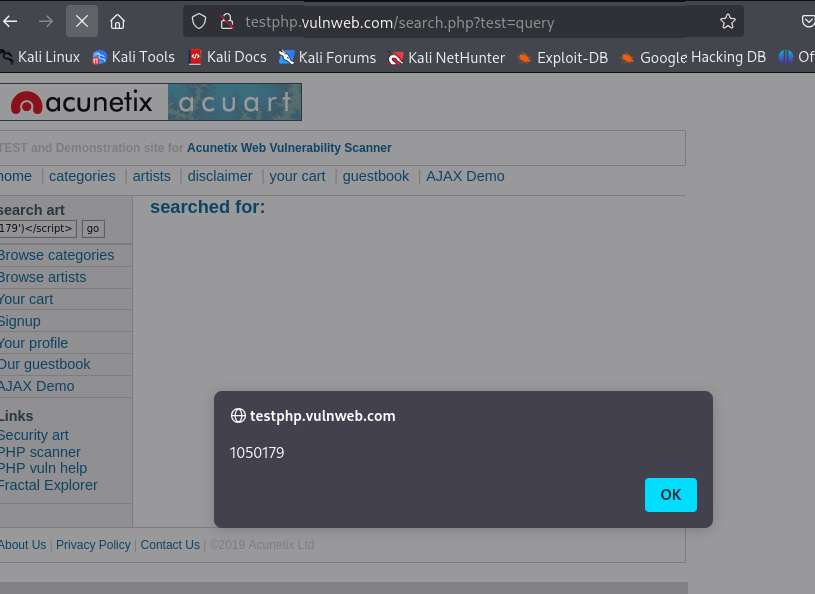
**-** Xác định các tham số đầu vào: **0.25 điểm**

* **nhập vào seach art 0179 và hiển thị nhưu hình**

****

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

**<script>alert(‘0179’)</script>**

****

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

**Bước 1:** Truy cập vào trang web và tìm trường đầu vào (input field).

**Bước 2:** Nhập đoạn mã sau vào trường đầu vào:

**<script>alert(‘0179’)</script>**

**Bước 3:** Gửi dữ liệu và quan sát kết quả. Nếu thông báo alert(‘0179’) xuất hiện, trang web đã bị lỗ hổng XSS.

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

Nếu thông báo alert('0179') hiển thị trên màn hình, điều này chứng tỏ lỗ hổng XSS tồn tại. Điều này cho thấy rằng trang web không thực hiện kiểm tra hoặc mã hóa đúng cách đầu vào của người dùng.

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

Nếu thông báo alert(‘0179’) xuất hiện, điều này chứng tỏ trang web bị lỗ hổng XSS. Lỗi này xảy ra khi trang web không kiểm tra hoặc mã hóa dữ liệu đầu vào từ người dùng một cách an toàn.

**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

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/)