**BÁO CÁO BÀI THỰC HÀNH SỐ 9**

**KIỂM THỬ LỖ HỔNG XSS và CSRF**

***Họ và tên: Đào Ngọc Hòa***

***Lớp: 1050080050***

***Link: https://youtu.be/e\_HS9D6Wv1M***

***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**

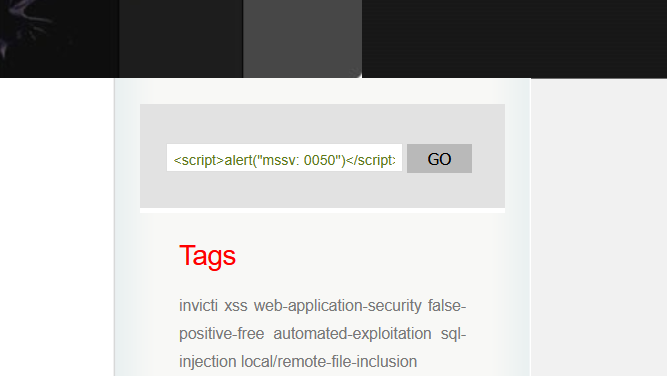
Thực hiện kiểm thử lỗ hổng XSS trên website: chọn 1 trong các trang sau để thử nghiệm

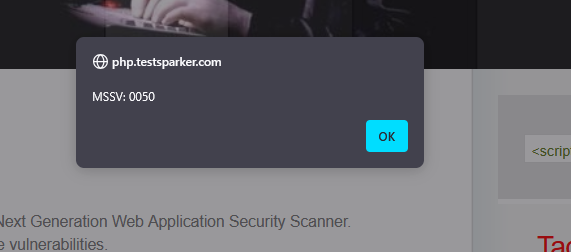
1. [http://demo.testfire.net](http://demo.testfire.net/)`
2. [http://php.testsparker.com](http://php.testsparker.com/)
3. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
4. [http://testasp.vulnweb.com](http://testasp.vulnweb.com/)
5. [http://testphp.vulnweb.com](http://testphp.vulnweb.com/)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

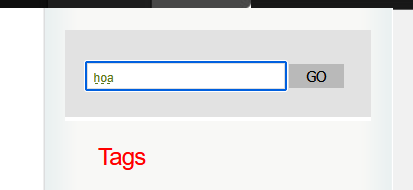
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV trên trang web [http://php.testsparker.com](http://php.testsparker.com/).

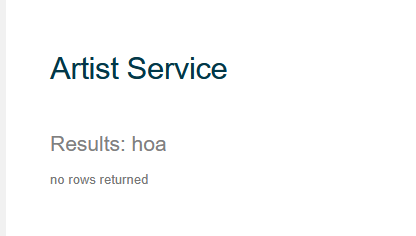
**-** Tham số đầu vào sẽ là 4 số cuối mã số sinh viên ở đây sẽ là 0050.





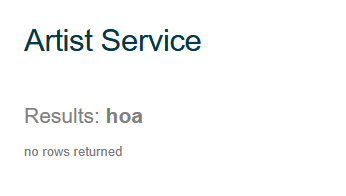
* Thực hiện kiểm thử hiển thị kết quả trong với ô input





* thử in đậm nội dung hiển thị





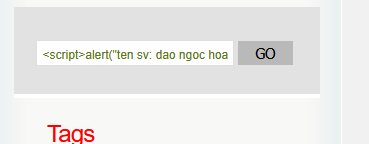
* Dữ liệu do người dùng nhập (như khi nhập từ ô input) được phản hồi lại trực tiếp lên giao diện mà không được kiểm tra, lọc hoặc mã hóa đúng cách.
* Thay vì hiển thị nội dung khi người dùng nhập ví dụ khi nhập vào <script>alert("MSSV: 0050")</script> thì kết quả trả về phải là “<script>alert("MSSV: 0050")</script>” nhưng trang web lại thực thi đoạn code và hiển thị ra một thông báo với nội dung “0050”

**Câu 2**

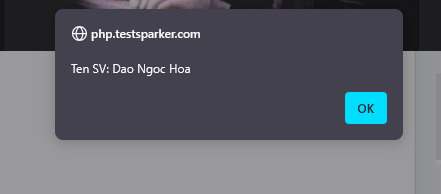
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa tên sinh viên trên trang web [http://php.testsparker.com](http://php.testsparker.com/).

**-** Tham số đầu vào ở đây sẽ là tên của sinh viên “Dao Ngoc Hoa”.

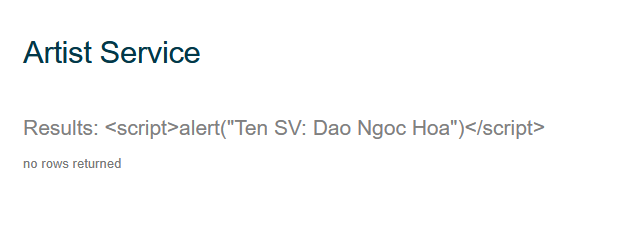
- Thực hiện chèn đoạn mã <script>alert("Ten SV: Dao Ngoc Hoa")</script>



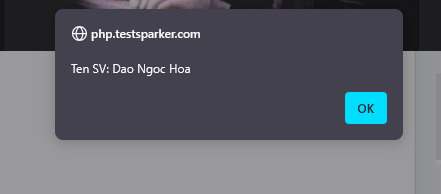
* Kết quả trả về sẽ là một alert có chứa nội dung có trong thẻ <script>



* Thay vì nội dung sẽ được mã hóa thành “&lt;script&gt;alert(&quot;Ten SV: Dao Ngoc Hoa&quot;)&lt;/script&gt;” để có thể hiển thị đúng nội dung nội dung trên trang web thì lại không thể mã hóa khiến cho việc hacker có thể chèn các đoạn mã độc vào trang web.

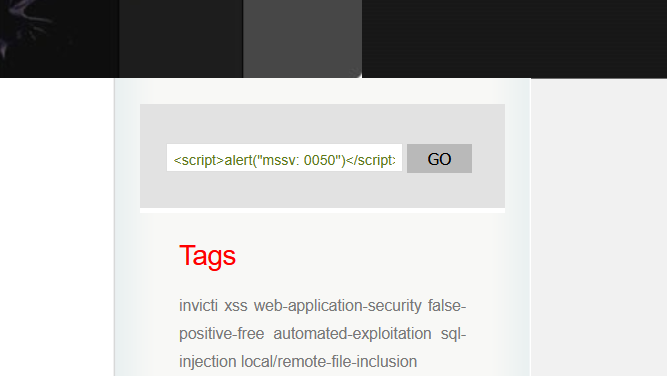


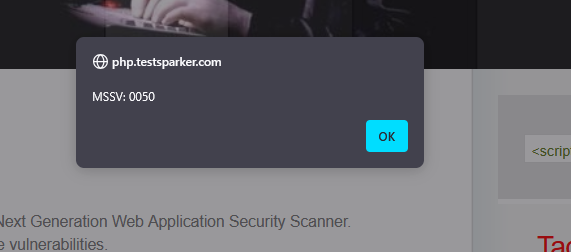
* Hình trên là ví dụ nếu nội dung <script>alert("Ten SV: Dao Ngoc Hoa")</script> được mã hóa thì nó sẽ hiển thị ra kết quả còn nếu không thì nó sẽ thực thi đoạn code và trả về kết quả như hình bên dưới.



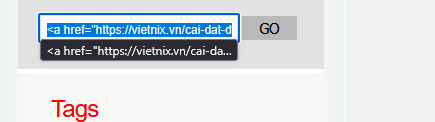
**Câu 3**

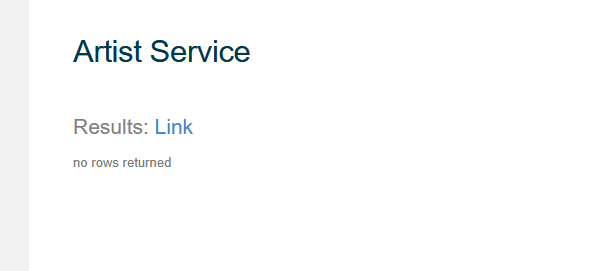
Tham số đầu vào sẽ là 4 số cuối mã số sinh viên ở đây sẽ là 0050.





* Thực hiện kiểm thử chèn link vào trang web
* Nhập vào ô input nội dung sau “<a href = "https://vietnix.vn/cai-dat-dvwa-tren-linux/" onclick="alert(1)">Link</a></h3>”





* Nếu ta ấn vào Link thì nó sẽ chuyển ta đến trang web mà ta đã chỉ định trong đường dẫn của phần tử href



* Đây là trang web mà ta đã chỉ định trong href.

**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/)