BÁO CÁO BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

Họ và tên: Cao Đức Minh - 1050080062

Lớp: 10ĐH\_CNPM1

Link youtube:

Link github:

Yêu cầu kết quả thực hành:

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.

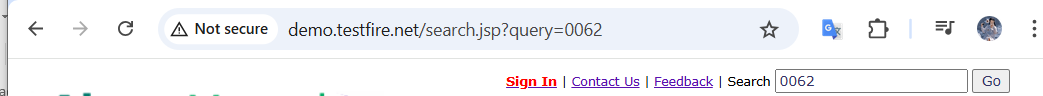
Hãy giải thích:

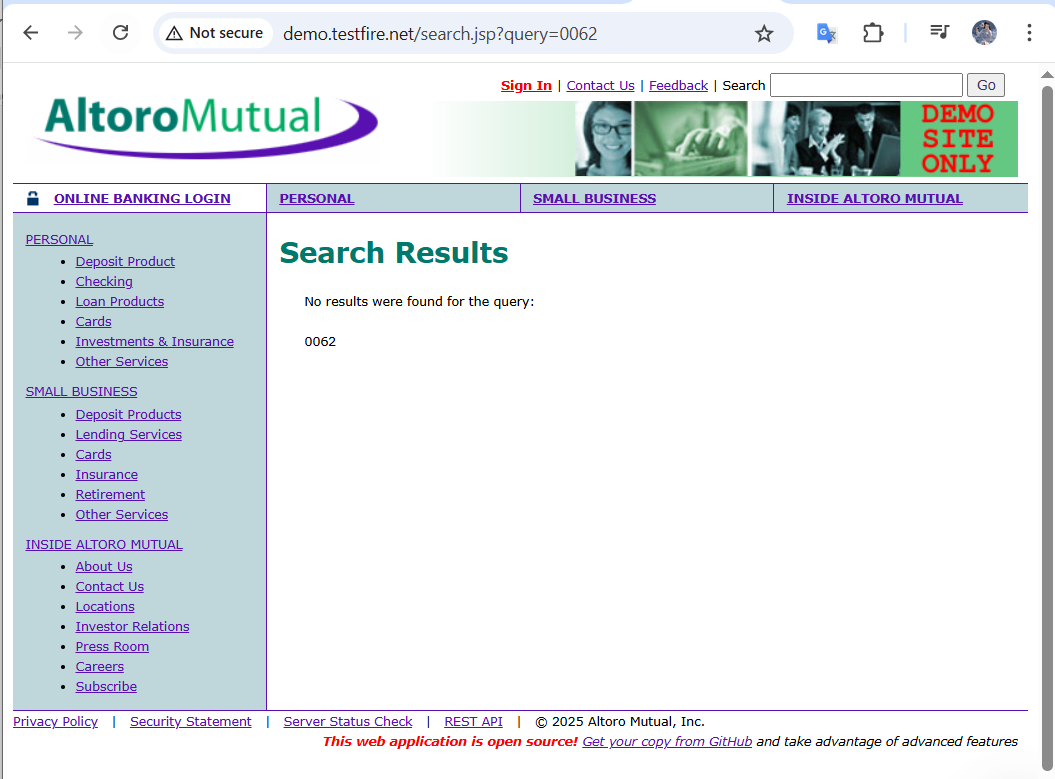
- Xác định các tham số đầu vào: 0.25 điểm

Tham số đầu vào ban đầu: 0062, 1234, <script>alert('1234')</script>

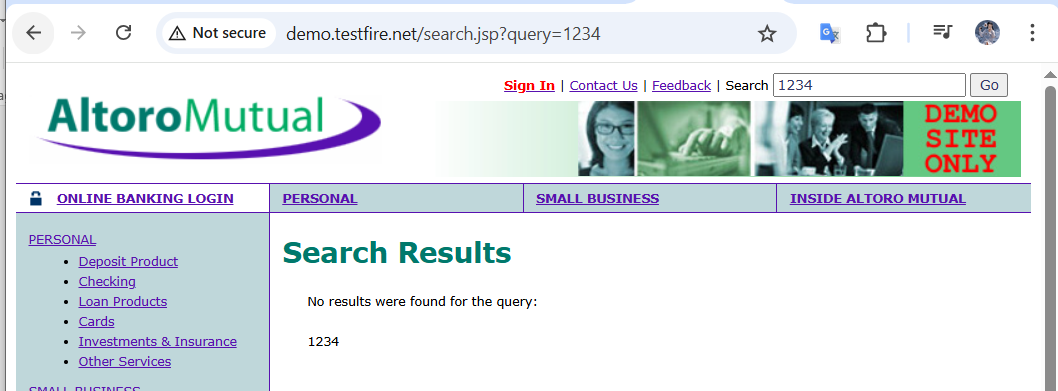
- Xác định giá trị đầu vào xuất hiện trong trang kết quả: 0.25 điểm

0062

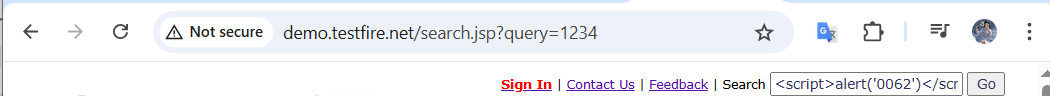


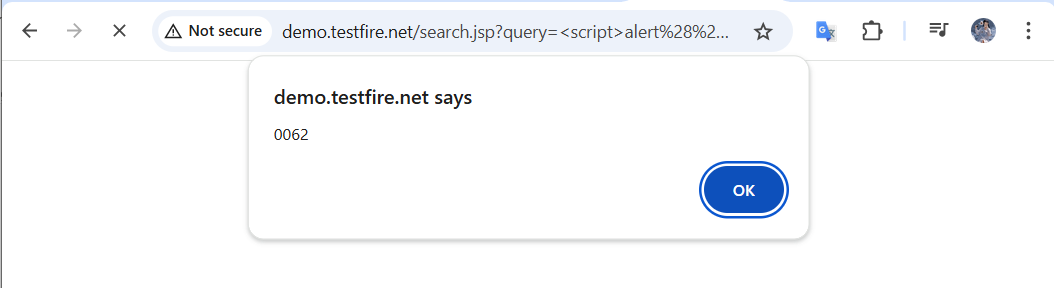


1234



<script>alert(‘0062’)</script>



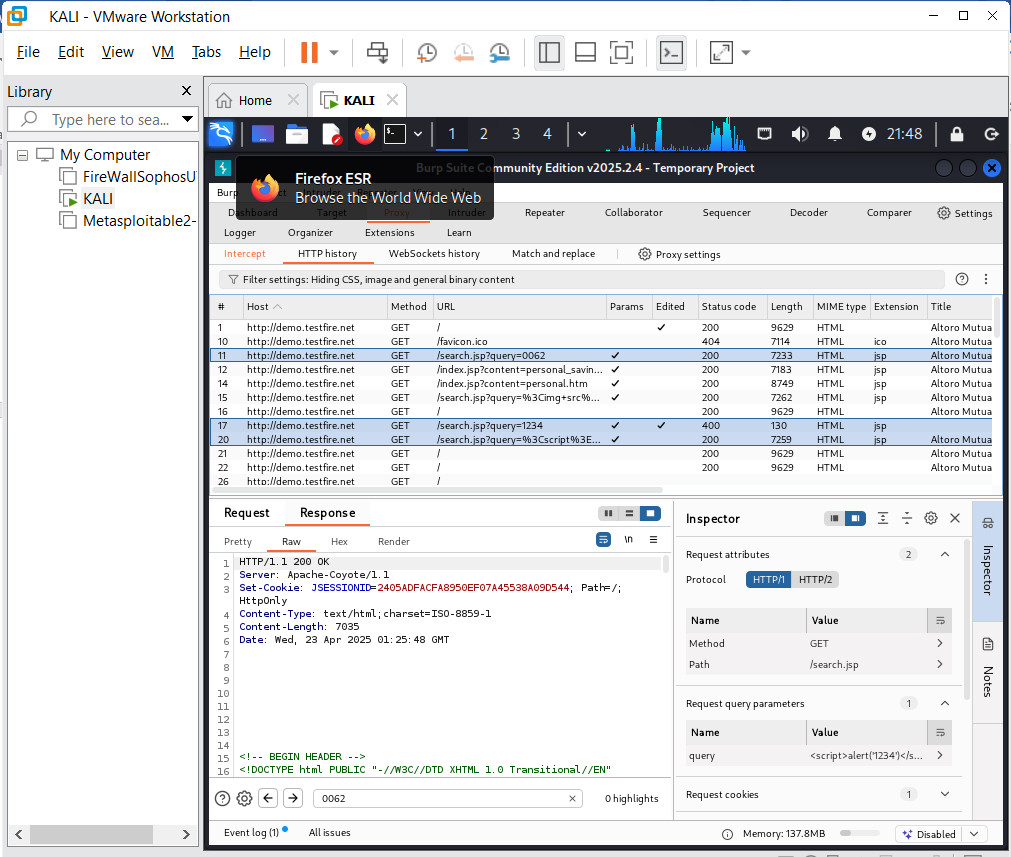


- Các bước kiểm thử và phán đoán: 0-1 điểm theo các bước kiểm thử và logic trong phán đoán

Truy cập vào trang web [**http://demo.testfire.net**](http://demo.testfire.net)

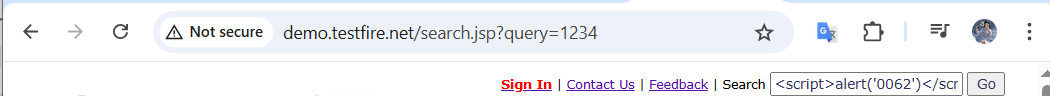
Nhập thử các giá trị đầu vào như: 0062, 1234, <script>alert(‘0062’)</script>

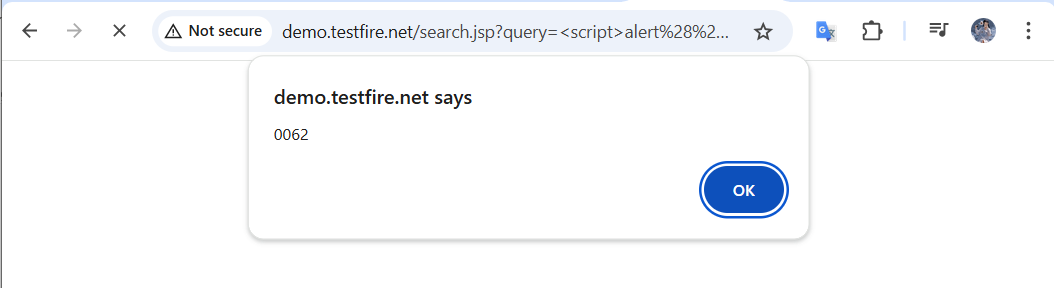
Kiểm tra trong burpsuite



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

Giá trị kiểm thử: <script>alert(‘0062’)</script>





Cho thấy rằng trang web có một lỗ hổng XSS vì mã JavaScript đã được thực thi

Câu 2

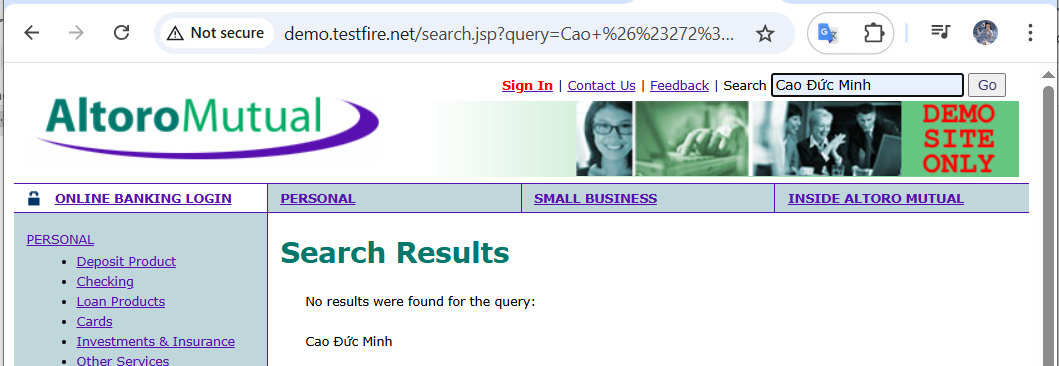
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa tên của sinh viên.

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

- Xác định các tham số đầu vào: 0.25 điểm

Tham số đầu vào: Cao Đức Minh

- 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

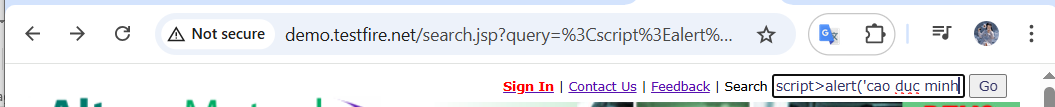
Truy cập trang web [**http://demo.testfire.net**](http://demo.testfire.net)

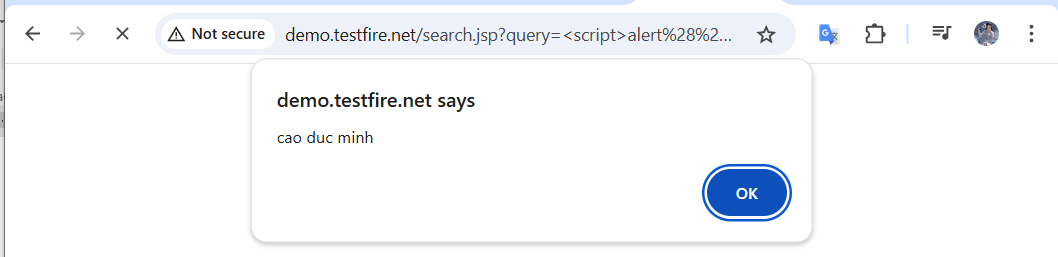
Nhập giá trị đầu vào và xem kết quả hiển thị

Nhập giá trị kiểm thử XSS <script>alert(‘Cao Đức Minh’)</script>

Xem kết quả kiểm thử

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





Chứng tỏ trang web có lỗ hổng XSS đối với dữ liệu nhập vào là chữ: ‘tên sinh viên’

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

- 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

- 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

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