BÁO CÁO BÀI THỰC HÀNH SỐ 9

KIỂM THỬ LỖ HỔNG XSS và CSRF

Họ và tên: Lý Gia Hưng - 1050080053

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

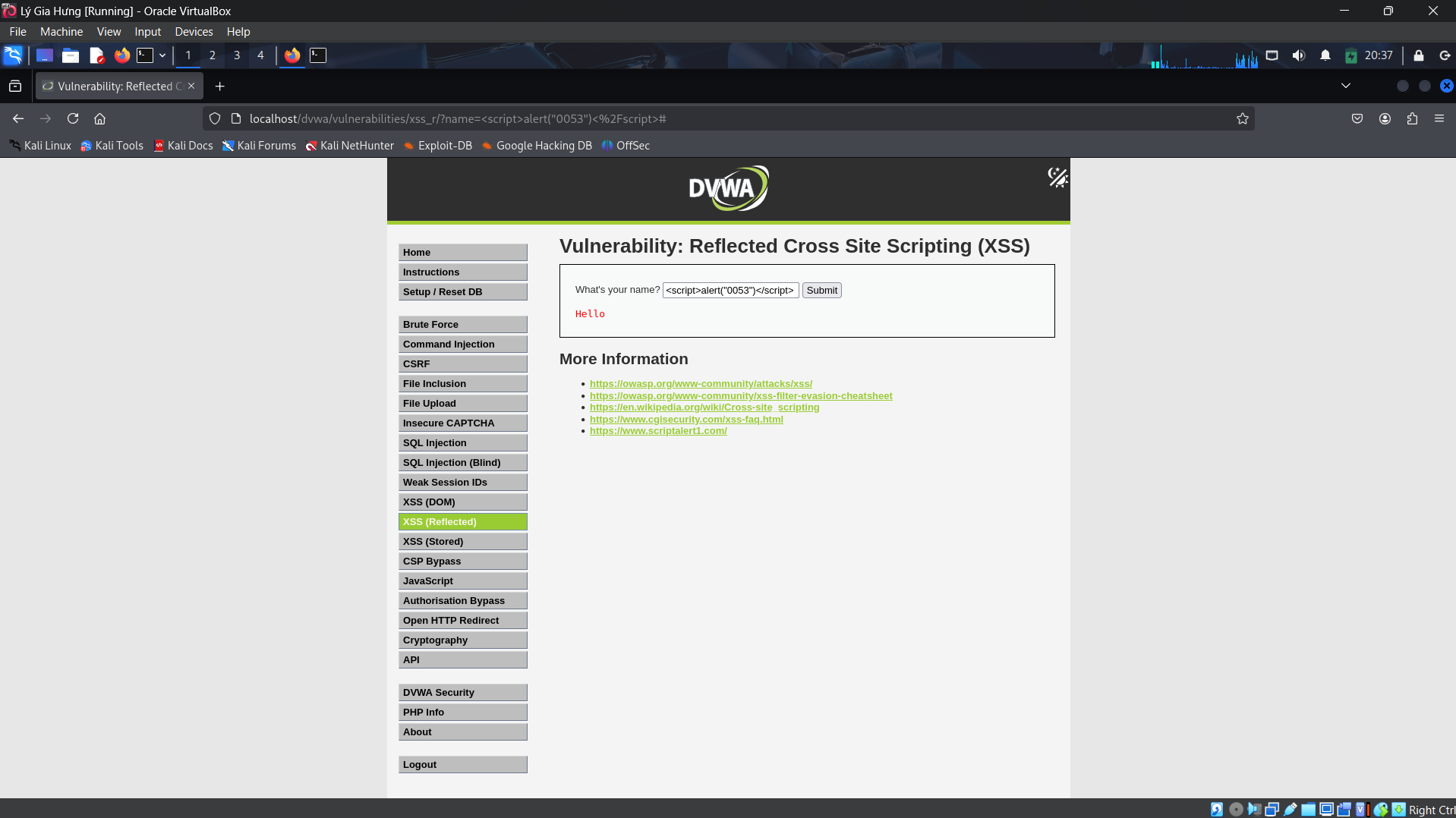
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV.

Hãy giải thích:

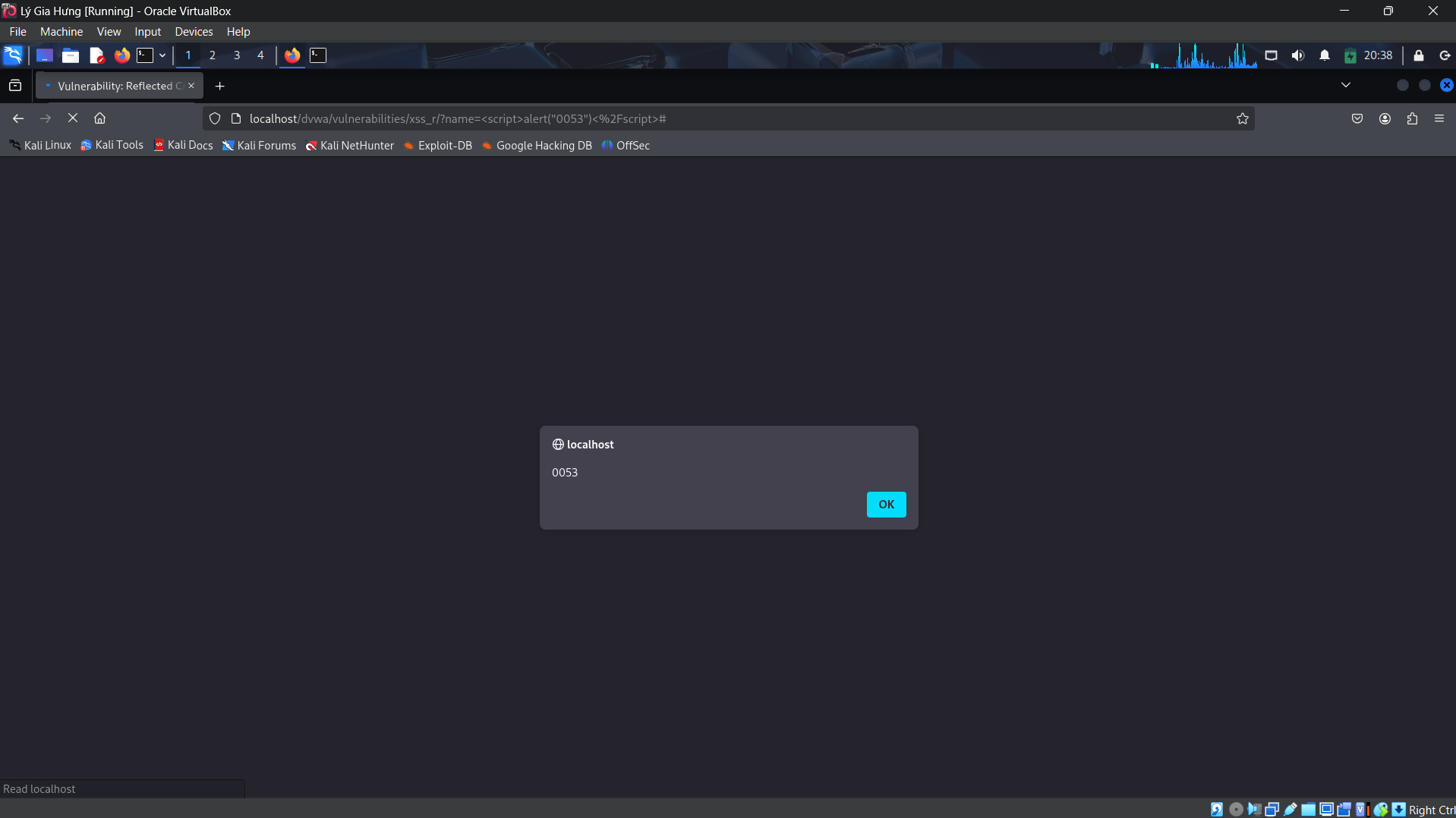
- Xác định các tham số đầu vào: 0.25 điểm

Giá trị đầu vào là 0053

<script>alert("0053")</script>



- 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 các trang web có trường nhập dữ liệu ví dụ DVWAA screenshot of a computer

AI-generated content may be incorrect.

-Bước 2: Vào mục nhập trường message ví dụ XSS(Reflected)

A screenshot of a computer

AI-generated content may be incorrect.

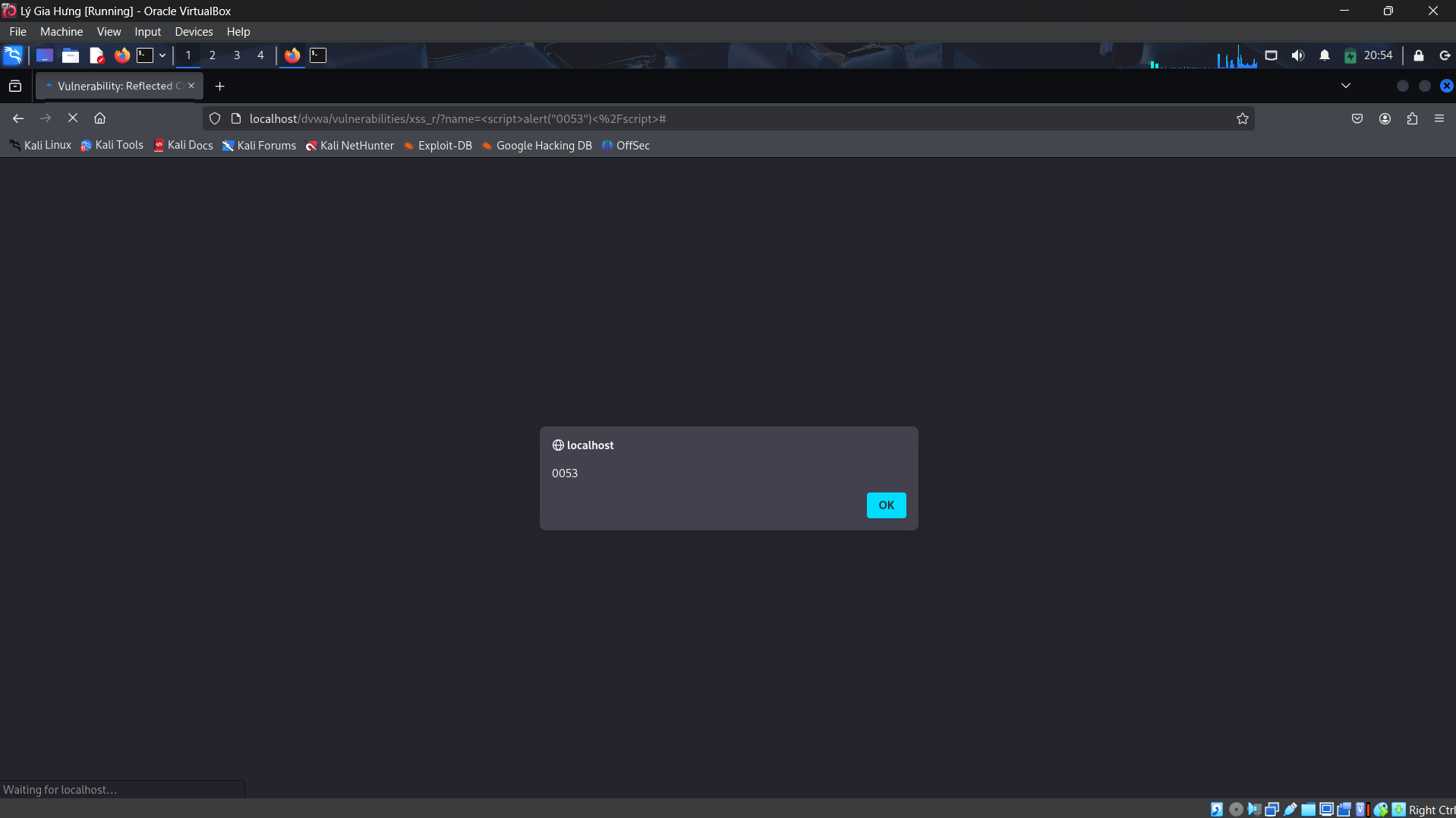
-Bước 3: nhập vào đoạn message <script>alert(“0053”)</script>

A screenshot of a computer

AI-generated content may be incorrect.

-Bước 4: nhấn submit gửi lên server quan sát xem có thông báo xuất hiện trang màn hình không

🡪 Nếu có xuất hiện chứng tỏ trang web không mã hoá hoặc lọc dữ liệu người dùng gây ra lỗ hổng XSS



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

Giá trị kiểm thử là <script>alert(“0053”)</script>

+ Kết quả trình duyệt thực thi đoạn mã và hiện hộp thoại cảnh báo 0053

+ Giải thích: server hiển thị lại input người nhập mà không mã hoá HTML như là chuyển hoá < thành &lt và > thành &gt. Điều này làm cho trình duyệt thực thi mã JavaScript độc hại làm cho kẻ tấn công chèn và thực thi script nguy hiểm gây ra lỗ hổng XSS

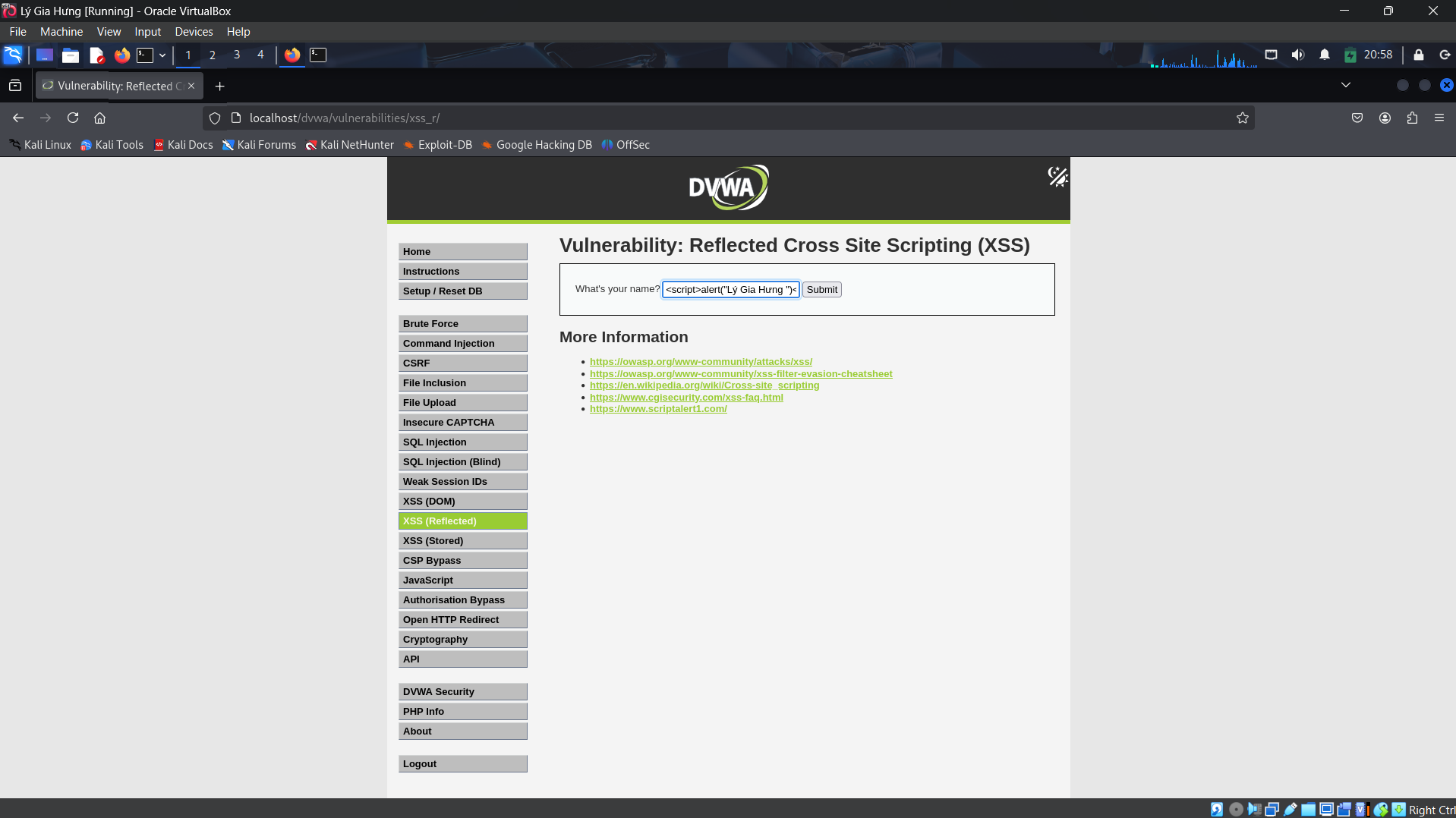
Câu 2

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

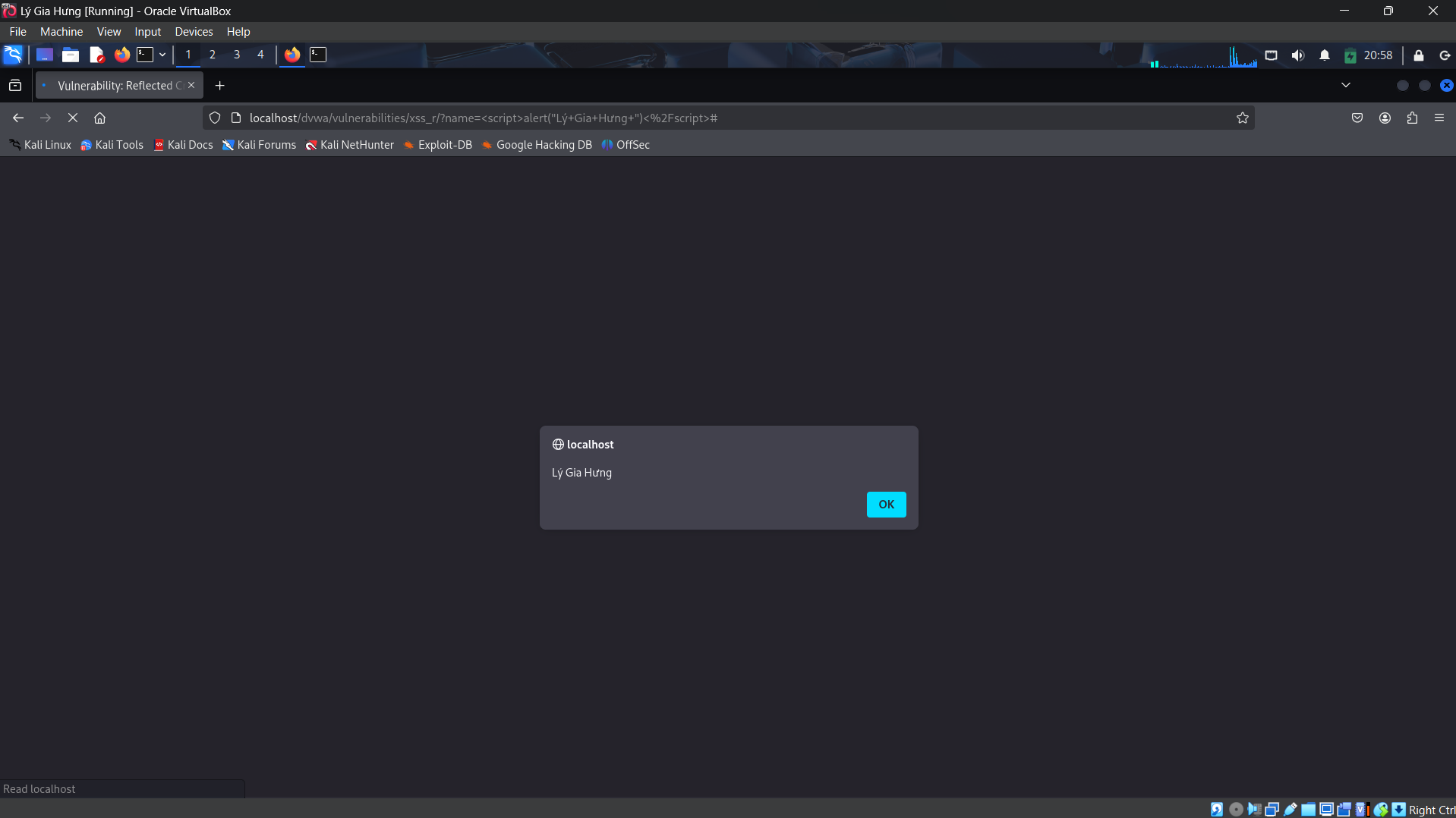
Điểm cho mỗi tham số đầu vào đã kiểm thử được:

- Xác định các tham số đầu vào: 0.25 điểm

Giá trị đầu vào là “Lý Gia Hưng”



- 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:vào trang web có trường nhập dữ liệu như DVWA

+Bước 2: vào mục XSS(Reflected) nếu là DVWA

+Bước 3: nhập <script>alert("Lý Gia Hưng")</script>

+Bước 4: nhấn submit gửi lên server nếu hiện ra thông báo đúng với giá trị nhập vào là “Lý Gia Hưng” nghĩa là trang web có lỗ hổng XSS

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

🡪 Từ kết quả cho thấy trang web không xử lý encoding làm cho giá trị có dấu dễ dàng làm cho các hacker chèn mã độc vào

Câu 3

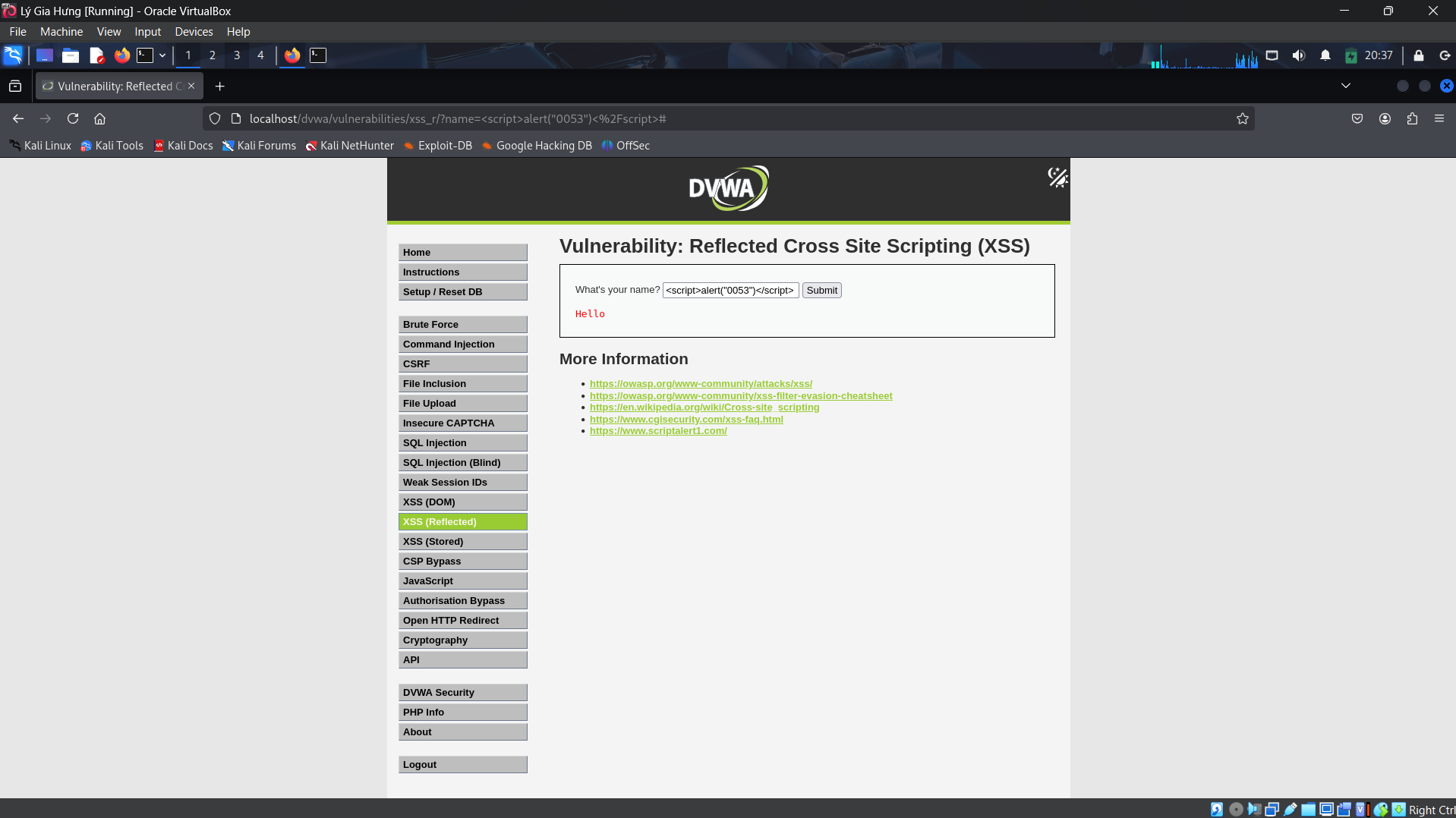
Thực hiện kiểm thử lỗ hổng XSS để thực thi đoạn mã hiển thị thông báo có chứa 4 số cuối MSSV.

Hãy giải thích:

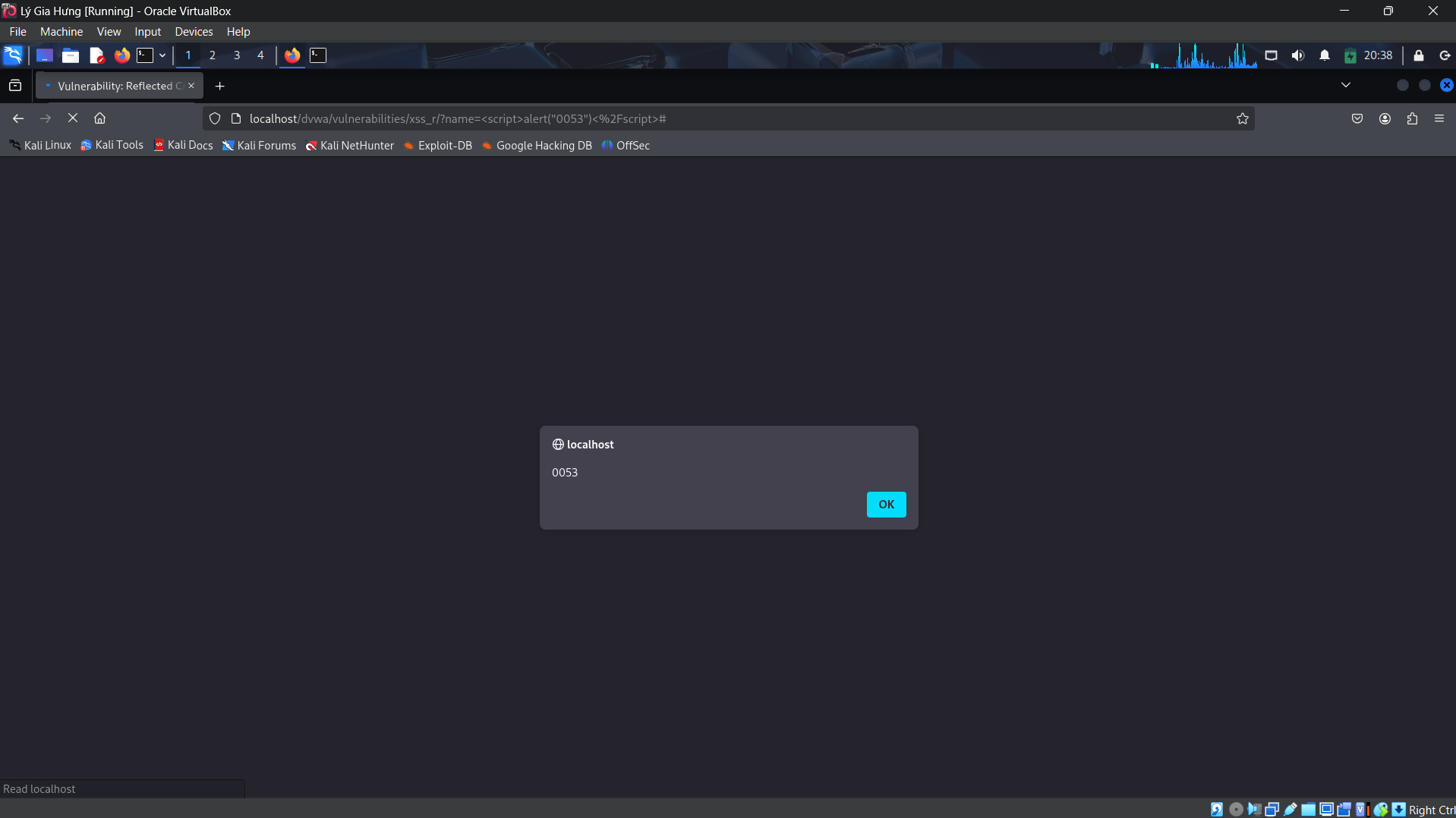
- Xác định các tham số đầu vào: 0.25 điểm

Giá trị đầu vào là 0053

<script>alert("0053")</script>



- 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 các trang web có trường nhập dữ liệu ví dụ DVWAA screenshot of a computer

AI-generated content may be incorrect.

-Bước 2: Vào mục nhập trường message ví dụ XSS(Reflected)

A screenshot of a computer

AI-generated content may be incorrect.

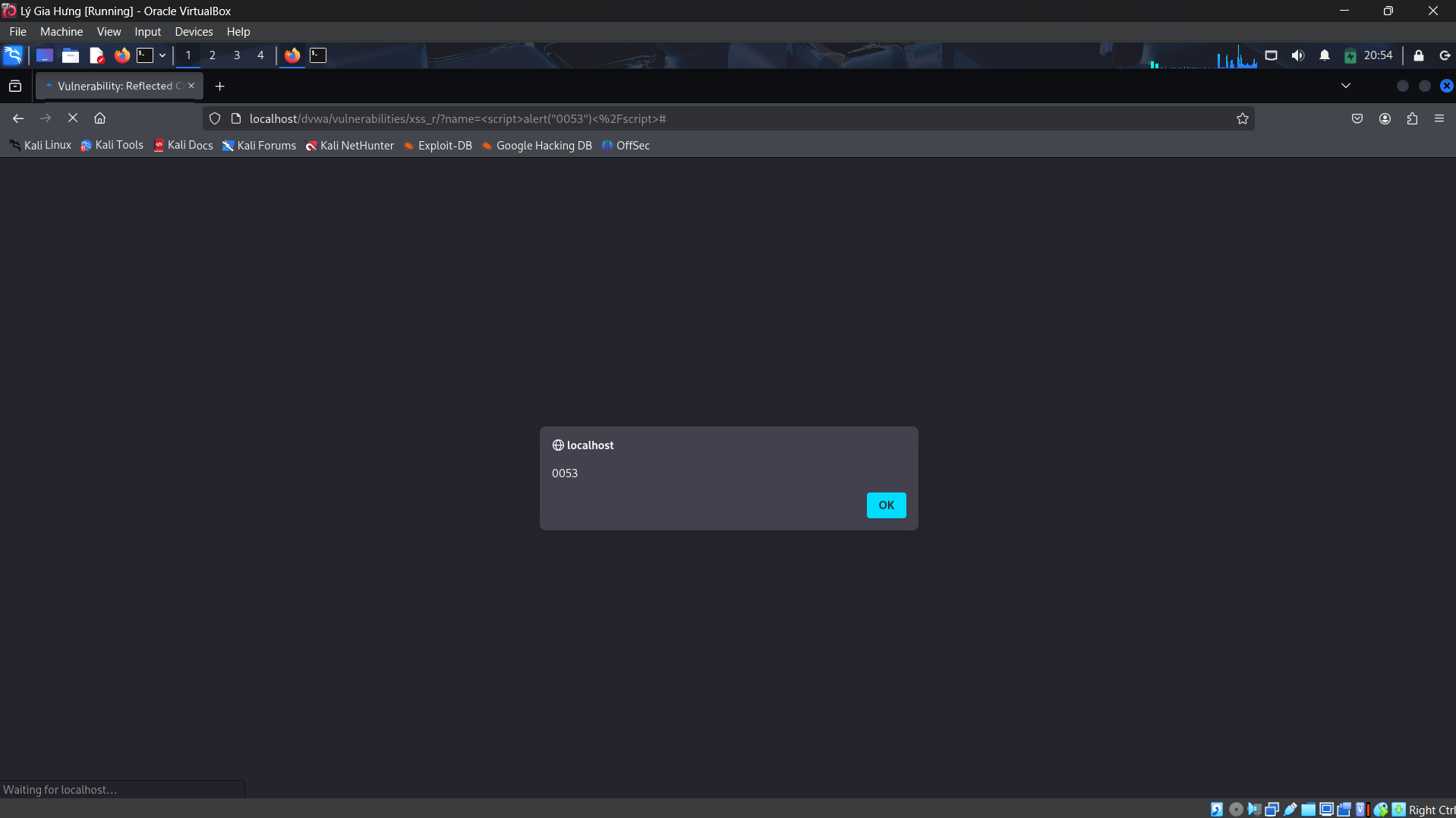
-Bước 3: nhập vào đoạn message <script>alert(“0053”)</script>

A screenshot of a computer

AI-generated content may be incorrect.

-Bước 4: nhấn submit gửi lên server quan sát xem có thông báo xuất hiện trang màn hình không

🡪 Nếu có xuất hiện chứng tỏ trang web không mã hoá hoặc lọc dữ liệu người dùng gây ra lỗ hổng XSS



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

Giá trị kiểm thử là <script>alert(“0053”)</script>

+ Kết quả trình duyệt thực thi đoạn mã và hiện hộp thoại cảnh báo 0053

+ Giải thích: server hiển thị lại input người nhập mà không mã hoá HTML như là chuyển hoá < thành &lt và > thành &gt. Điều này làm cho trình duyệt thực thi mã JavaScript độc hại làm cho kẻ tấn công chèn và thực thi script nguy hiểm gây ra lỗ hổng XSS

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

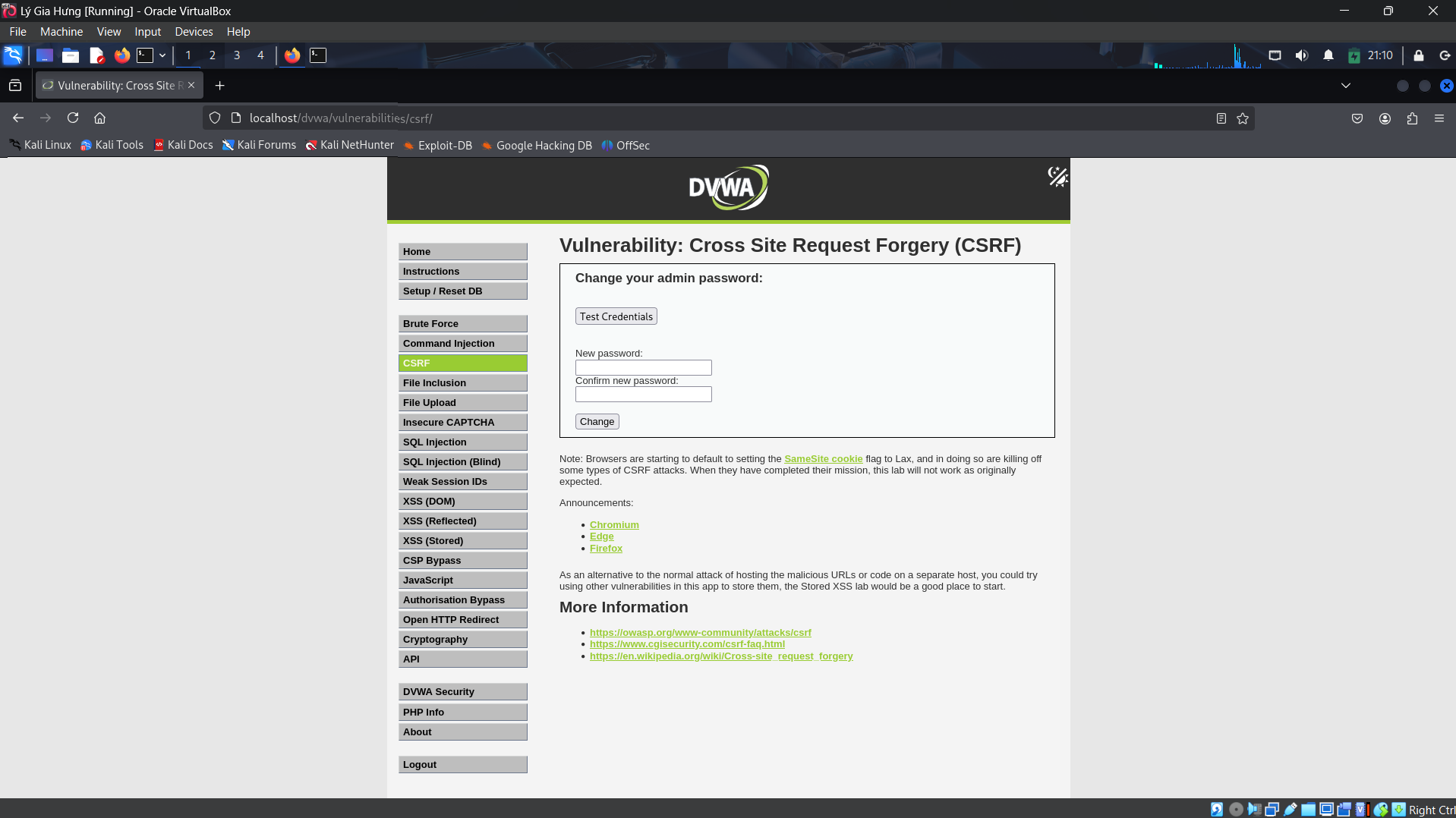
6. http://www.webscantest.com

7. http://testhtml5.vulnweb.com

8. http://aspnet.testsparker.com

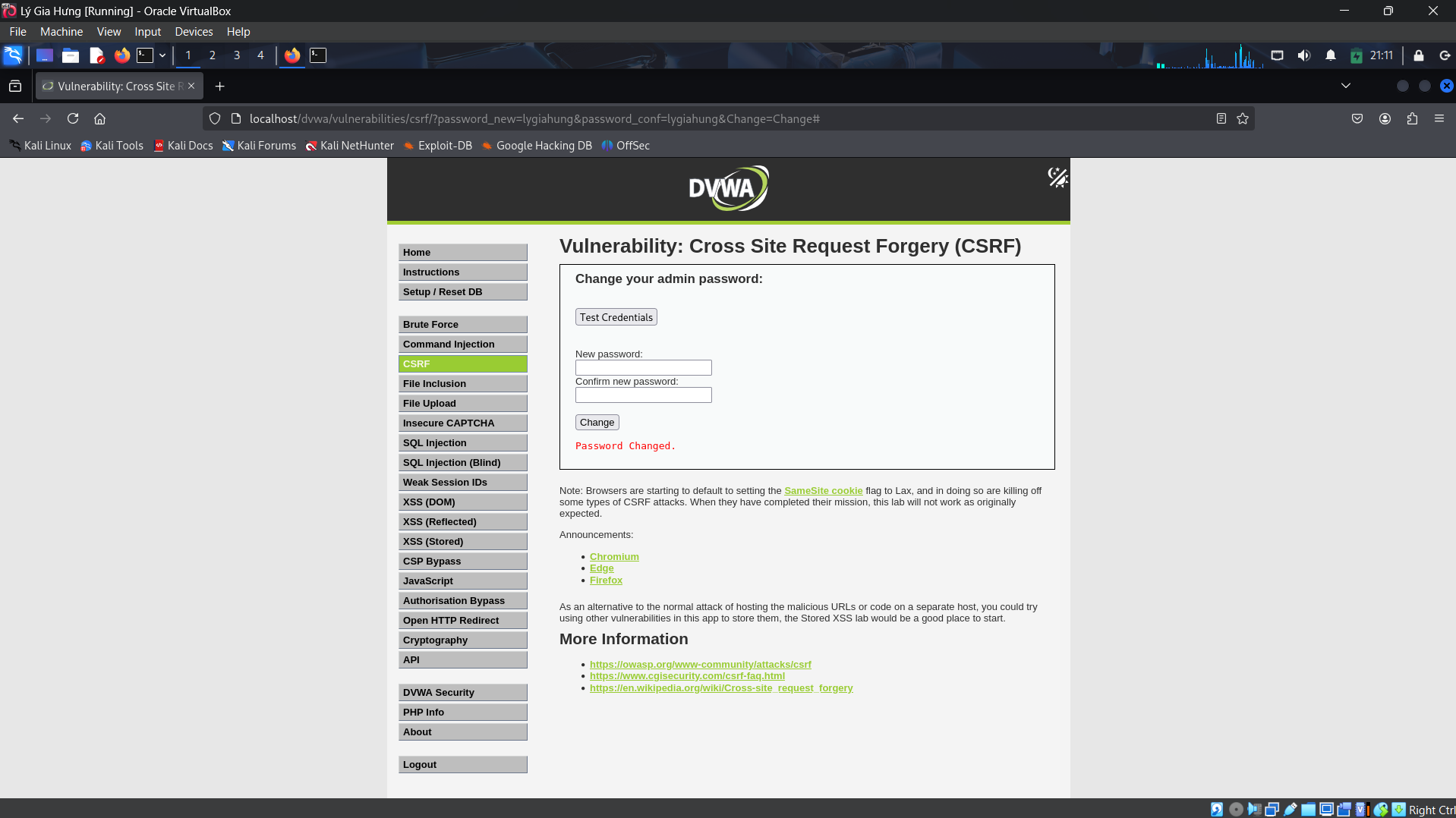
9. <http://zero.webappsecurity.com>

-Bước 1: truy cập vào trang web DVWA vào mục CSRF



-Bước 2: quan sát form ta thấy chỉ yêu cầu nhập newpass và confirm newpass

-Bước 3: đổi thử pass là lygiahung

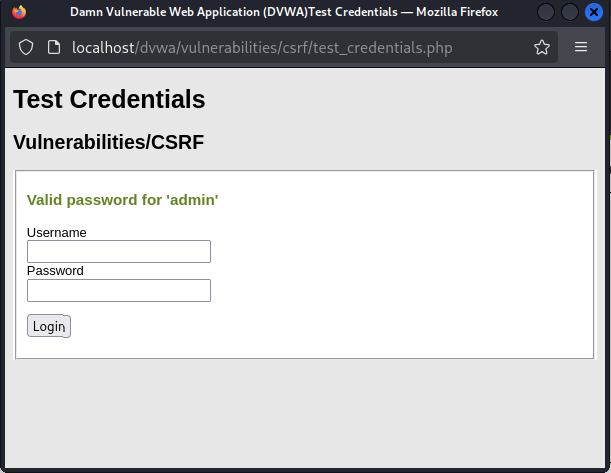


* Bị thay đổi dễ dàng không cần xác minh gì

-Bước 4: test thử đăng nhập đã đổi chưa. Nhấn vào nút Test Credetinals

+ Nhập lại pass cũ là: password sẽ thấy thông báo sai

+ Nhập lại pass mới là: lygiahung sẽ có thông báo valid



* Trang dễ bị khai thác