BÁO CÁO THỰC HÀNH

**Môn học: Bảo mật Web và ứng dụng**

**Bài tập: XSS + CSRF**

*GVHD: Nghi Hoàng Khoa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.O22.ATCL- Nhóm 3

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Bùi Hoàng Trúc Anh | 21521817 | 21521817@gm.uit.edu.vn |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |
| 3 | Nguyễn Ngọc Trà My | 21520353 | [21520353@gm.uit.edu.vn](mailto:21520772@gm.uit.edu.vn) |
| 4 | Huỳnh Minh Tân Tiến | 21521520 | 21521520@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | **Yêu cầu 1** | 100% |
| 2 | **Yêu cầu 2** | 100% |
| 3 | **Yêu cầu 3** | 100% |
| 4 | **Yêu cầu 4** | 100% |
| 5 | **Yêu cầu 5** | 100% |
| 6 | **Yêu cầu 6** | 100% |
| 7 | **Yêu cầu 7** | 100% |
| 8 | **Yêu cầu 8** | 100% |
| 9 | **Yêu cầu 9** | 100% |
| 10 | **Yêu cầu 10** | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. **Reflected XSS into HTML context with nothing encoded**

Nhập “<script>alert(1)</script>” vào ô tìm kiếm và nhấn nút Search

**A screenshot of a computer

Description automatically generated**

Thì ta sẽ được kết quả:

A close-up of a computer screen

Description automatically generated

1. **Stored XSS into HTML context with nothing encoded**

Chọn View post.  
Nhập “<script>alert(1)</script>” vào ô bình luận và nhập tên, email và website rồi nhấn nút Post Comment

A screenshot of a computer

Description automatically generated

Ta nhấn nút Back to blog thì ta sẽ nhìn thấy thông báo alert

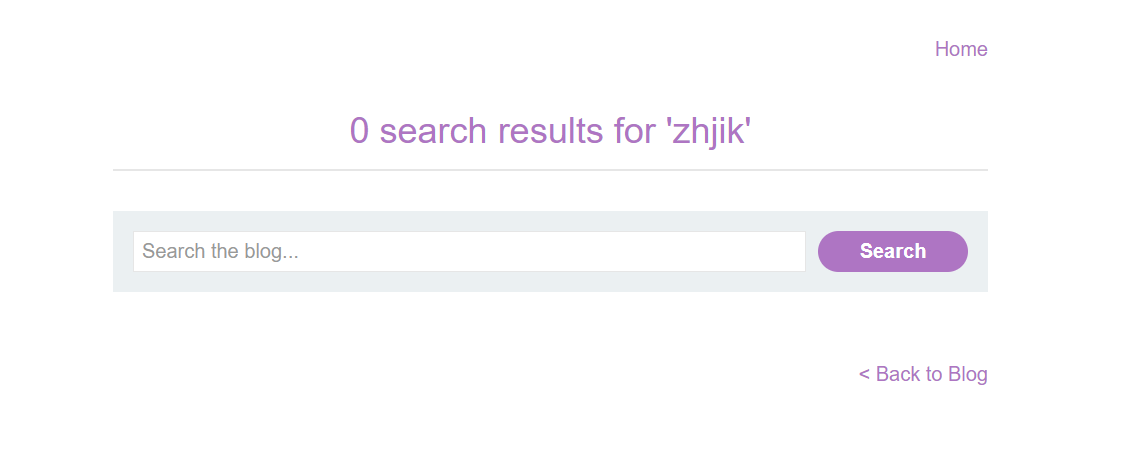
A close-up of a message

Description automatically generated

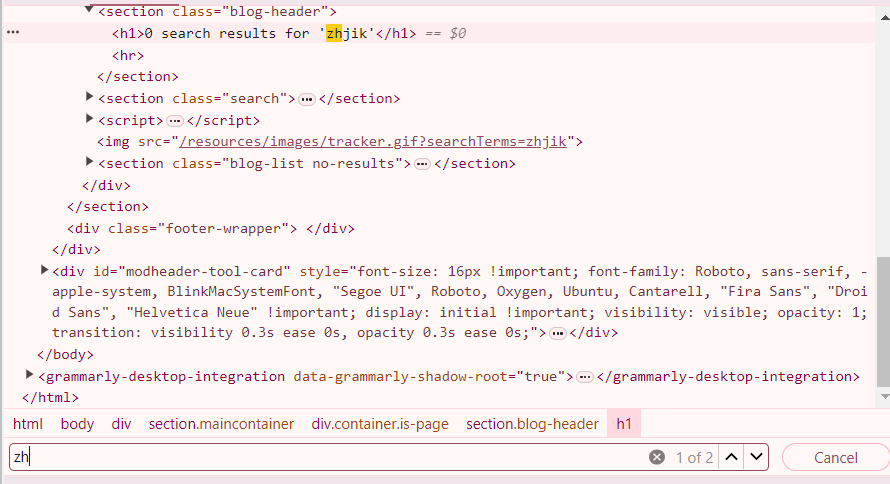
A close-up of a computer code

Description automatically generated

1. **DOM XSS in document.write sink using source location.search**

Đầu tiên, ta thử nhập vào một giá trị string bất kì

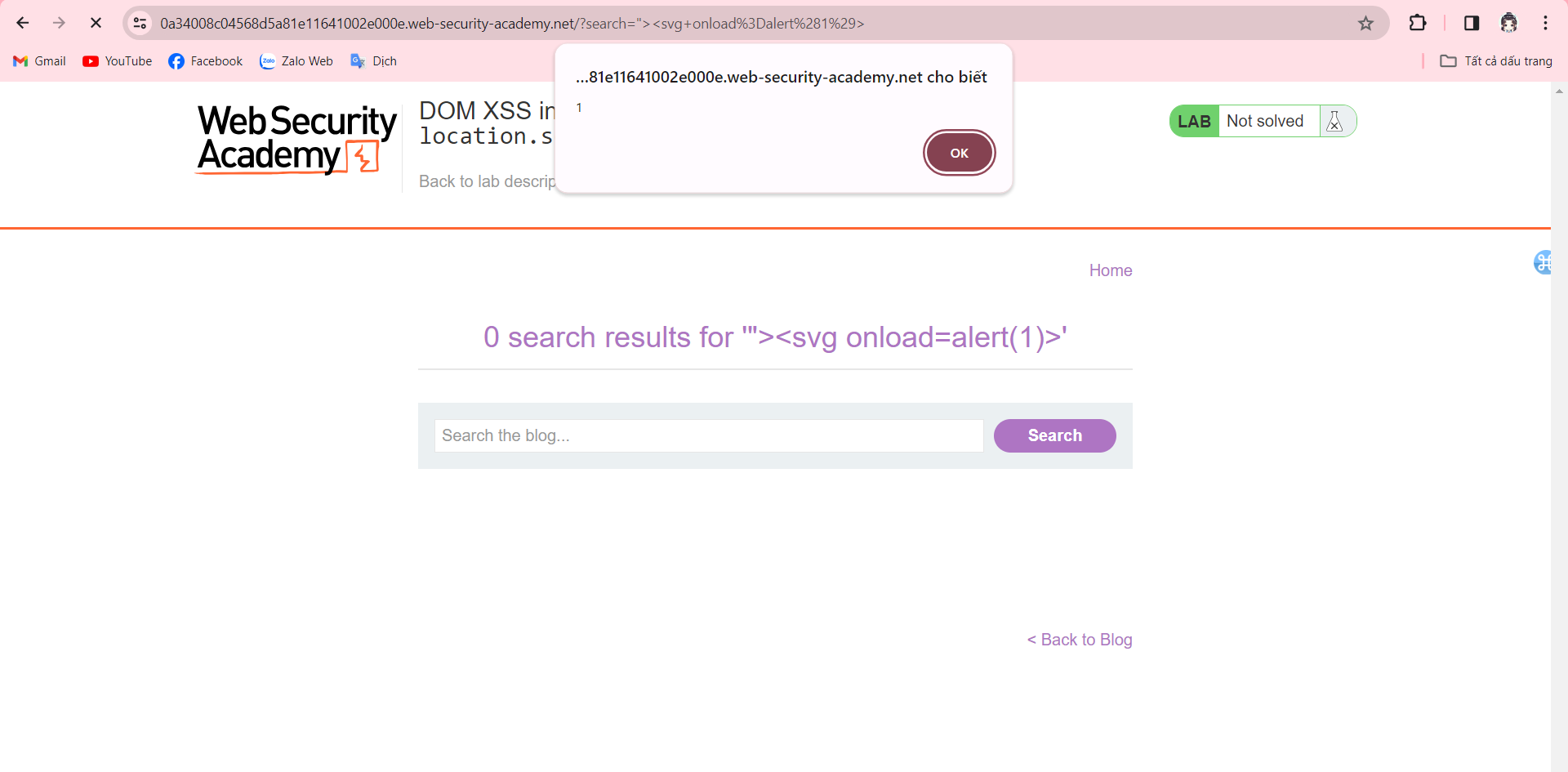
Nhận thấy rằng chuỗi vừa được nhập ghi vào trong thuộc tính img src. Do không có cơ chế kiểm tra nên ta có thể khai thác lỗi XSS



Ta nhập vào chuỗi sau: "><svg onload=alert(1)>

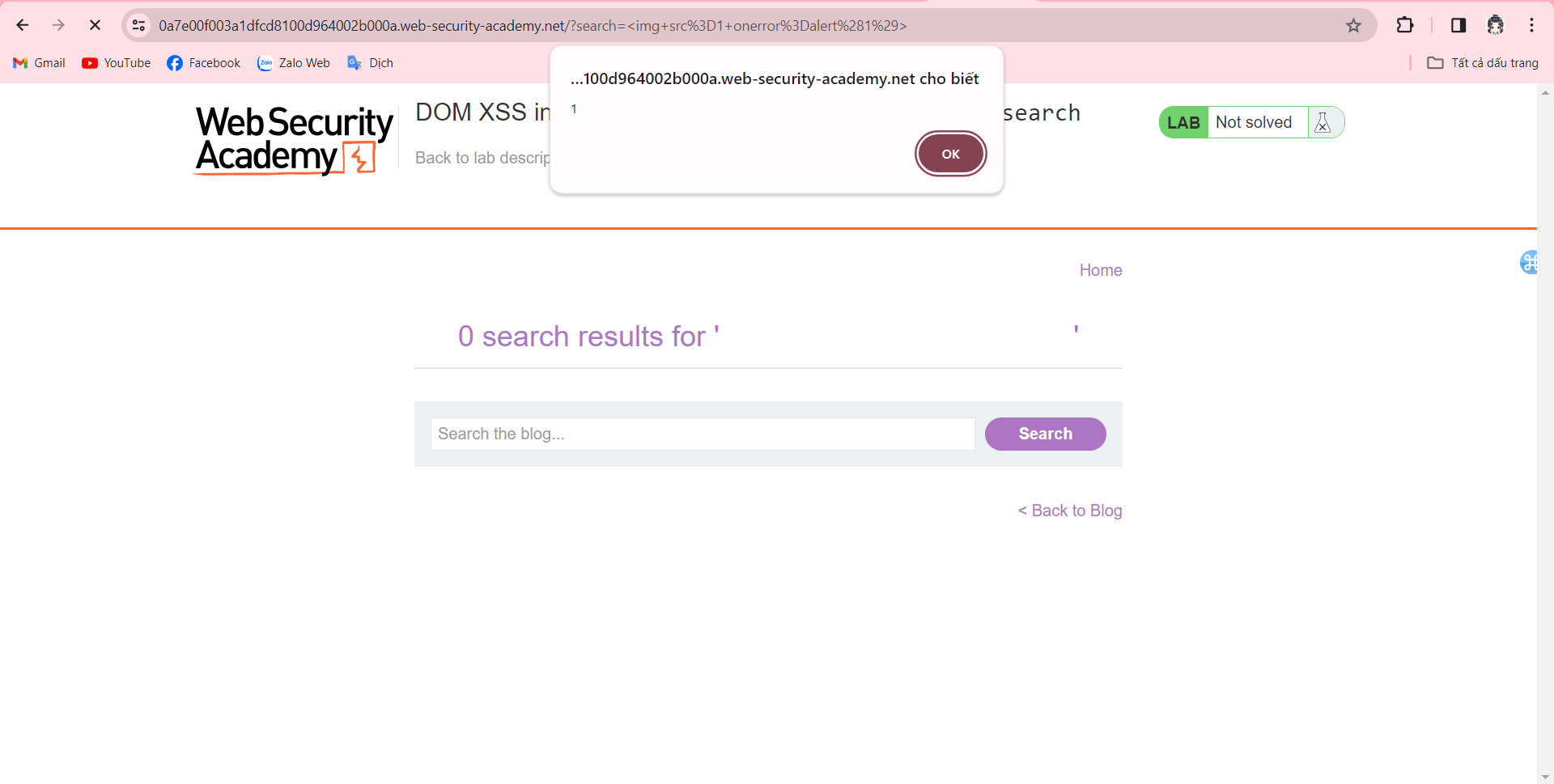
”> : dấu đóng ngoặc để kết thúc <img>

<svg onload=alert(1)>: thêm vào sự kiện onload một đoạn mã JavaScript alert(1)



1. **DOM XSS in innerHTML sink using source location.search**

Ta nhập vào: <img src=1 onerror=alert(1)>

Trình duyệt web không thể tải hình ảnh được chỉ định trong thuộc tính src, nó sẽ kích hoạt sự kiện onerror, và mã JavaScript alert(1) sẽ được thực thi

1. **DOM XSS in jQuery anchor href attribute sink using location.search source**

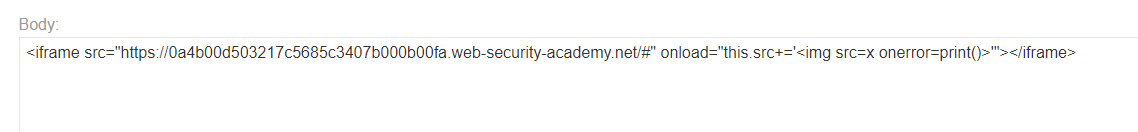
Nhập javascript:alert(document.cookie) vào returnPath sau đó nhấn Enter và nhấn vào nút back ta sẽ nhận được kết quả trả về như sau:



Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, Trang web

Description automatically generated

1. **DOM XSS in jQuery selector sink using a hashchange event**

Truy cập vào exploit server sau đó thêm đoạn code sau vào phần Body, store lại và gửi cho victim   


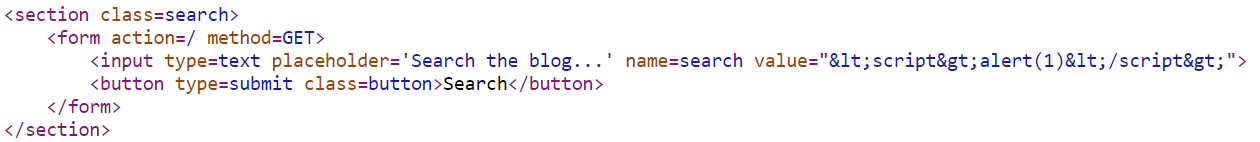
1. **Reflected XSS into attribute with angle brackets HTML-encoded**

Nhập “<script>alert(1)</script>” vào thanh tìm kiếm và nhấn Search, ta được kết quả sau

A screenshot of a computer

Description automatically generated

Chọn “Page Source” để quan sát ta thấy chuỗi tìm kiếm đã được chuyển vào value và mã hóa đi các dấu đóng mở “<” “>”.



Ta có 1 hàm onmouseover trong html với syntax như sau:

A screenshot of a computer

Description automatically generated

Do dấu “ không bị mã hóa khi nhập vô thanh tìm kiếm, ta nhập: "onmouseover="alert(1)

Do khi nhập vào thanh tìm kiếm, dữ liệu được chuyển xuống value có code như sau value="abc". Vậy nếu đặt vào chuỗi tìm kiếm 1 cặp dấu ngoặc nữa thì giá trị value sẽ vô nghĩa và dấu ngoặc còn lại sẽ được ghép với dấu ngoặc thứ 2 mà ta nhập vào: value= ""onmousemove="alert(1)"

Rồi nhấn Search thì ta sẽ được thông báo

A screenshot of a web security search

Description automatically generated

1. **Stored XSS into anchor href attribute with double quotes HTML-encoded**

Khi ta nhập thử: <script>alert(1)</script> vào ô comment thì ta thấy nó không hiện ra thông báo alert:

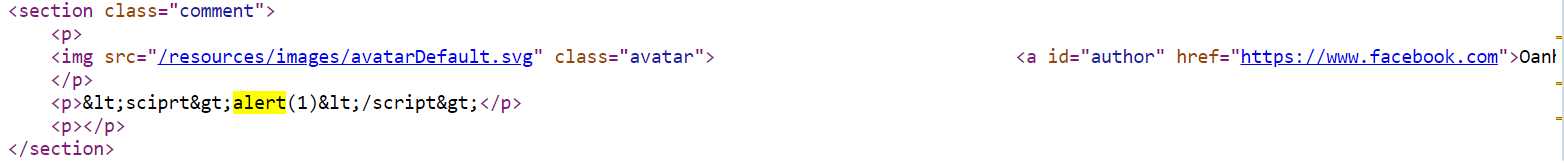
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Coi Page Source, ta thấy thẻ a href có đường dẫn đến website đã nhập ở input website. Thử truy cập vào sẽ chuyển đến website.



Vậy chúng ta sẽ inject script vào href của thẻ a (input của website) này với syntax như sau:

A computer screen shot of a computer code

Description automatically generated

Nhập thông tin như sau, rồi nhấn Post Comment.

A screenshot of a computer

Description automatically generated

Khi nhấn vô tên của người comment, ta sẽ thấy thông báo alert.

**A computer screen shot of a computer

Description automatically generated**

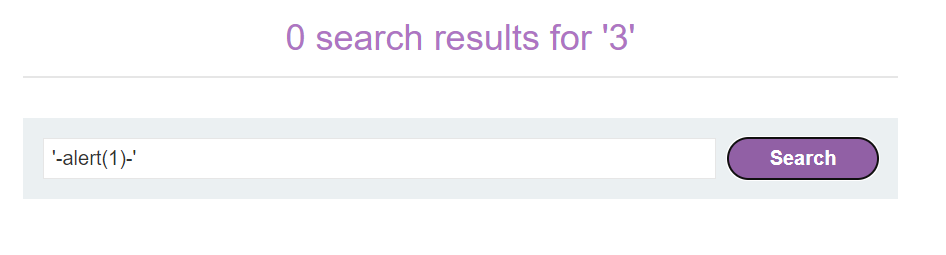
1. **Reflected XSS into a JavaScript string with angle brackets HTML encoded**

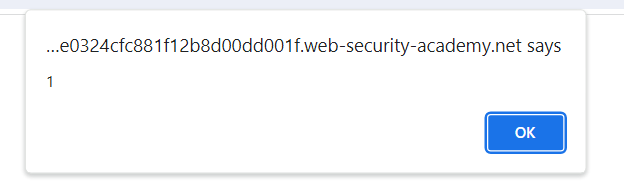
Theo gợi ý, đầu tiên nhập ngẫu nhiên 1 số vào search box, rồi dùng burp suite để intercept, sau đó bắt đầu phân tích và xử lý

Với đường dẫn là search = 1, sau khi send request đến web và kết quả nhận được là

phương thức document.write() để viết ra một thẻ <img> HTML, có thuộc tính src là một URL. URL này chứa một hình ảnh (có thể là một tracker pixel) được đặt ở địa chỉ "/resources/images/tracker.gif". Đi kèm với đó, giá trị của tham số searchTerms được mã hóa bằng phương thức encodeURIComponent() và được thêm vào URL thông qua chuỗi query.

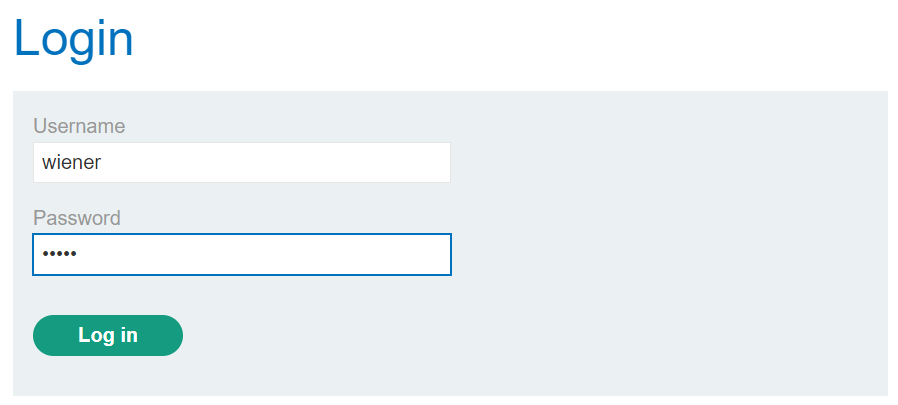
Nếu giá trị của SearchTerm là đoạn mã javascript '-alert(1)-' thì một cảnh báo sẽ hiện lên

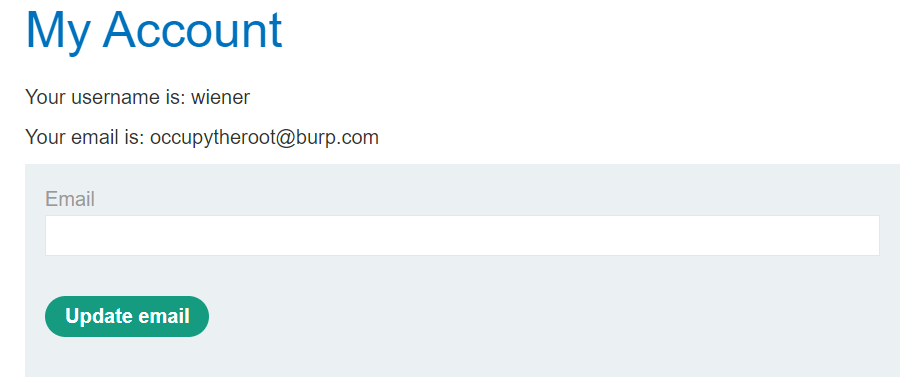




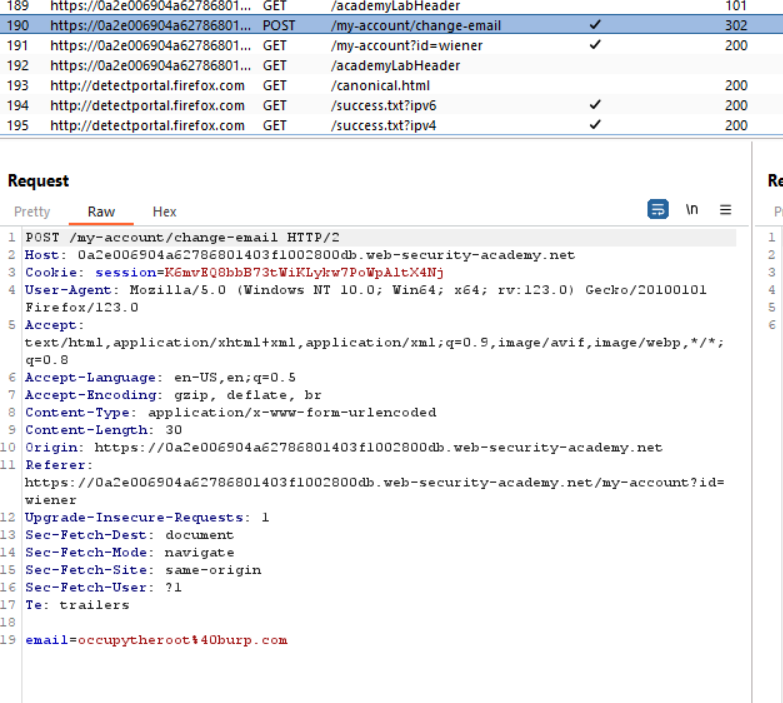
1. **CSRF vulnerability with no defenses**

Đầu tiên , đăng nhập với thông tin đã được cung cấp





Update email, sau đó kiểm tra proxy về request liên quan đến việc update email

Sau đó dùng template html burp suite đã cung cấp, truy cập vào trang exploit server, chỉnh sửa theo template và dán vào body

Ảnh có chứa văn bản, hàng, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

Kết quả

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động