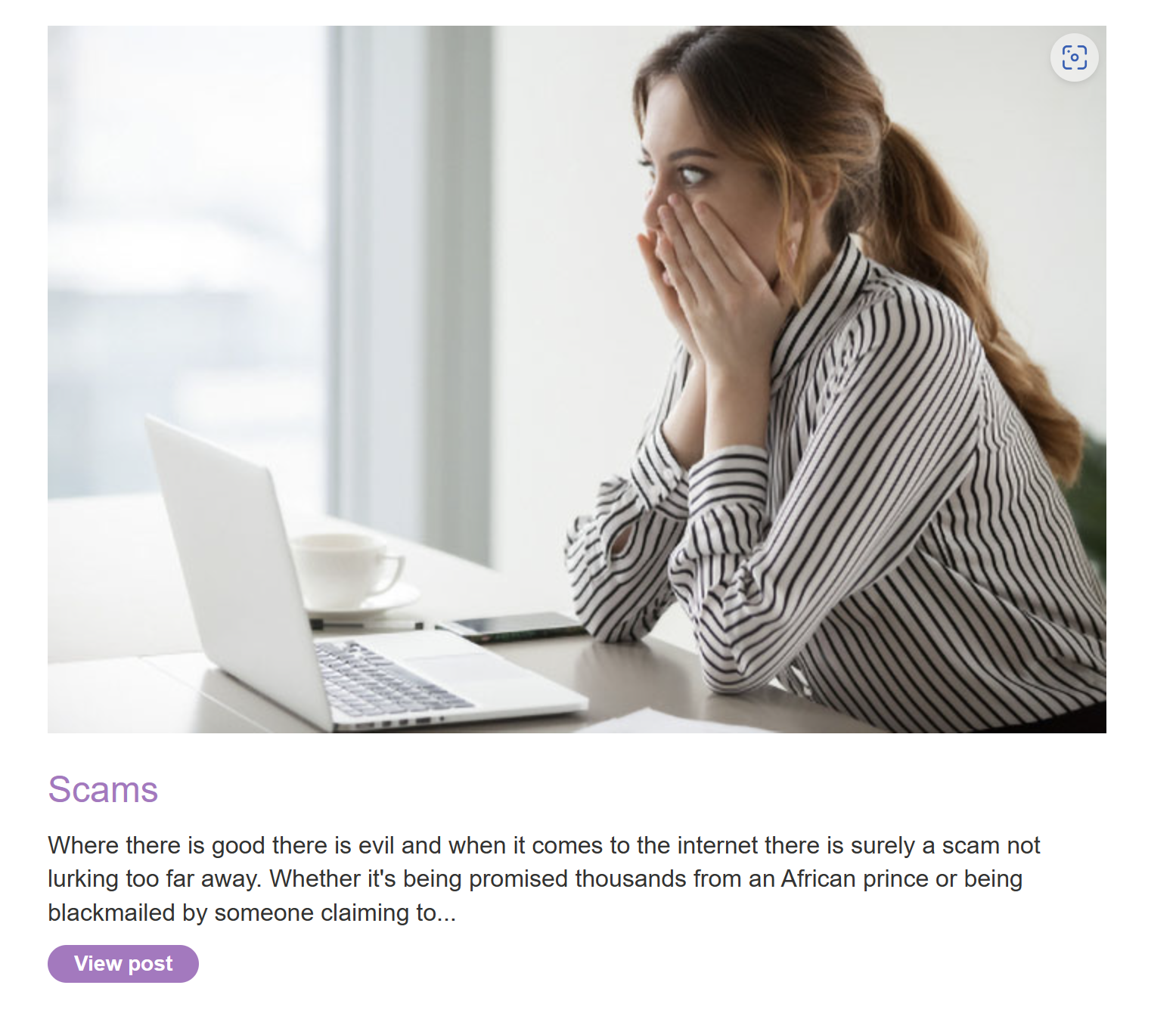
Bài tập 2:

Ta vào thử chức năng view post của trang web

  
Ta thử post một comment lên trang web để xem có gì xảy ra

A screenshot of a computer

Description automatically generated

A white background with black text

Description automatically generated

Kiểm tra inspector, ta thấy nội dung ta comment được sử dụng với thẻ <p>

A screenshot of a computer

Description automatically generated

Vậy ta có thể khai thác bằng cách sử dụng comment để chèn một thông báo.

A screenshot of a computer

Description automatically generated

Kết quả thu được

A screenshot of a computer

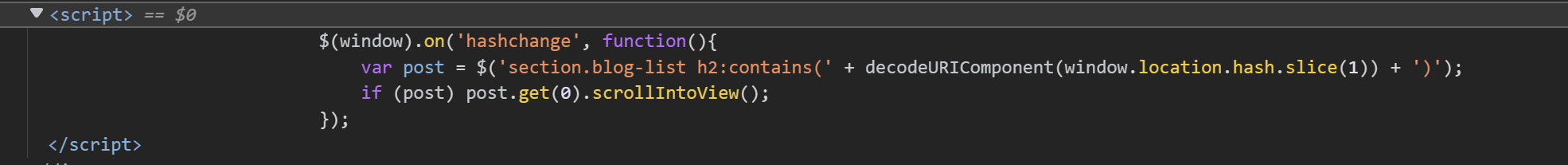
Description automatically generated

A person with her hands over her mouth

Description automatically generated

Bài tập 6:

Kiểm tra inspector, ta thấy một đoạn script như sau



Code trên được sử dụng để tìm và scroll đến một phần tử cụ thể dựa vào dấu hash(#) trong URL

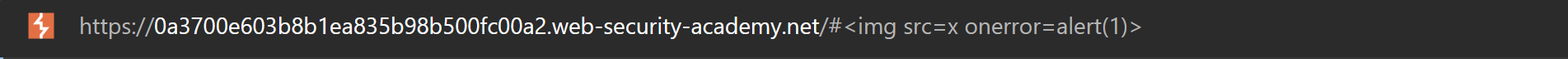
**decodeURIComponent(window.location.hash.slice(1)):** Ở đây, code sử dụng slice(1) để loại bỏ dấu hash khỏi chuỗi. Thêm vào đó, decodeURIComponent được sử dụng để giải mã kí tự bị mã hóa của URL. Ví dụ về việc ta sử dụng slice(1)

http://example.com/#test -> slice(0) -> test

http://example.com/#test -> slice(1) -> #test

http://example.com/#test -> slice(2) -> est

Ta thử chèn thêm đoạn mã sau vào URL của trang web:



Trang web trả lại thông báo sau, vậy suy đoán của ta là đúng

A grey screen with white text

Description automatically generated

Ta tiến hành đi đến exploit server, trong phần body ta nhập đoạn mã sau

A screenshot of a computer

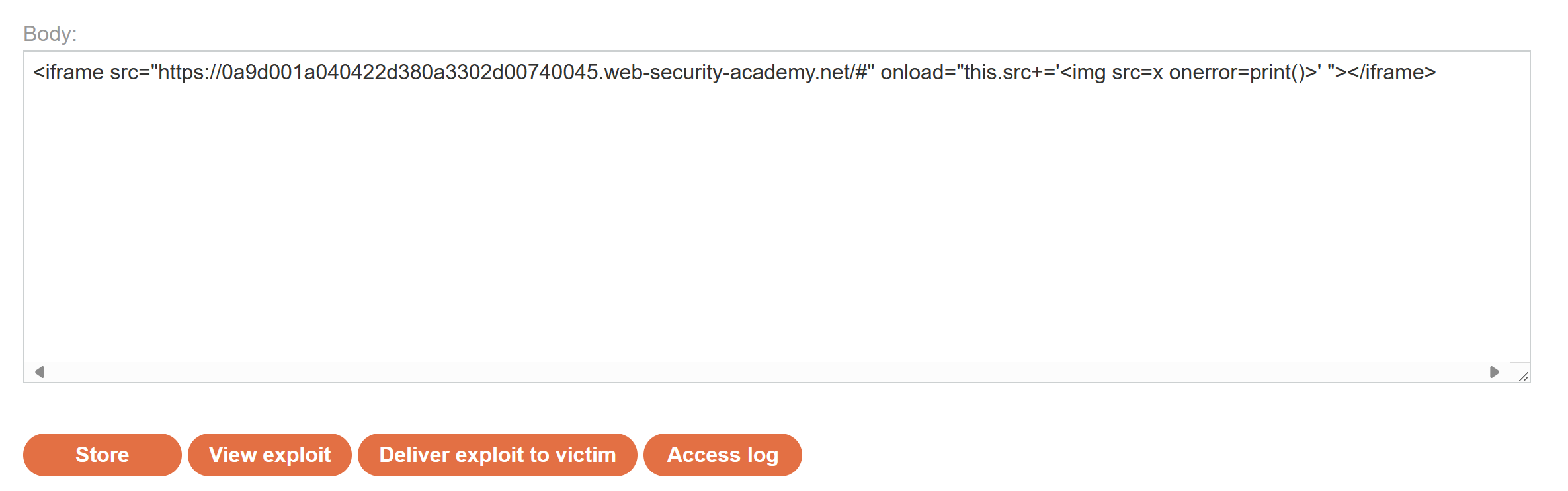
Description automatically generated

Giải thích: Ta sử dụng thẻ iframe nhúng trang web ban đầu đến trang exploit và thực hiện thêm những phần tử phía sau. Sau khi nhúng thành công, các phần tử trong onload cũng sẽ được kích hoạt, cụ thể ở đây sẽ in ra ô thông báo

A screen shot of a computer

Description automatically generated

Lúc này, ta thay đổi alert(1) trong thẻ img dùng để in ô thông báo thanh hàm print()



Kết quả thu được

A person stretching her arms

Description automatically generated

A person stretching her arms

Description automatically generated

Bài tập 10

Đầu tiên, ta đăng nhập bằng tài khoản mà bài lab cung cấp

A white rectangle with two white stripes

Description automatically generated

Ta đi đến phần my account sẽ thấy có chức năng update email. Ta thử update email và sử dụng burpsuite để bắt gói tin

A screenshot of a computer

Description automatically generated

Ta bắt được gói tin như sau

A screenshot of a computer

Description automatically generated

Ta đi đến exploit server và nhập đoạn mã dưới đây vào body

A screenshot of a computer

Description automatically generated

Giải thích: Đoạn mã trên thực hiện tạo một form để post lên trang của người dùng với một email mới (attack@gmail.com). Sau khi tải xong trang, biểu mẫu sẽ được submit.

Ta bấm “View exploit” để xem playload của ta có sử dụng được chưa

A screenshot of a login page

Description automatically generated

Xem gói tin ở burpsuite, ta thấy email đã được update thành công

A screenshot of a computer

Description automatically generated

Ta bấm “Deliver exploit to victim” và thu được kết quả

A screenshot of a computer

Description automatically generated