BÁO CÁO BÀI TẬP

**Môn học: Bảo mật Web và Ứng dụng**

**Kỳ báo cáo: Bài tập về nhà 2**

**Tên chủ đề: Bài tập XSS**

*GV: Nghi Hoàng Khoa*

*Ngày báo cáo: 30/03/2023*

**Nhóm: FinalFantasy**

1. **THÔNG TIN CHUNG:**

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

Lớp: NT213.N21.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Vũ Hoàng Thạch Thiết | 20521957 | 20521957@gm.uit.edu.vn |
| 2 | Nguyễn Hùng Thịnh | 20521963 | 20521963@gm.uit.edu.vn |
| 3 | Phạm Văn Xuân | 20522184 | 20522184@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | Level 1: Hello, world of XSS | 100% | Thiết | Thịnh wu |
| 2 | Level 2: Persistence is key | 100% | Thiết | Thịnh wu |
| 3 | Level 3: That sinking feeling… | 100% | Thiết | Thịnh wu |
| 4 | Level 4: Context matters | 100% | Xuân | Thịnh wu |
| 5 | Level 5: Breaking protocol | 100% | Xuân | Thịnh wu |
| 6 | Level 6: Follow the rabbit | 100% | Xuân | Thịnh wu |

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

BÁO CÁO CHI TIẾT

## [1/6] Level 1: Hello, world of XSS

**# Tiêu đề:** Tấn công XSS với trang web không xử lý input đầu vào để hiện pop-up javascript

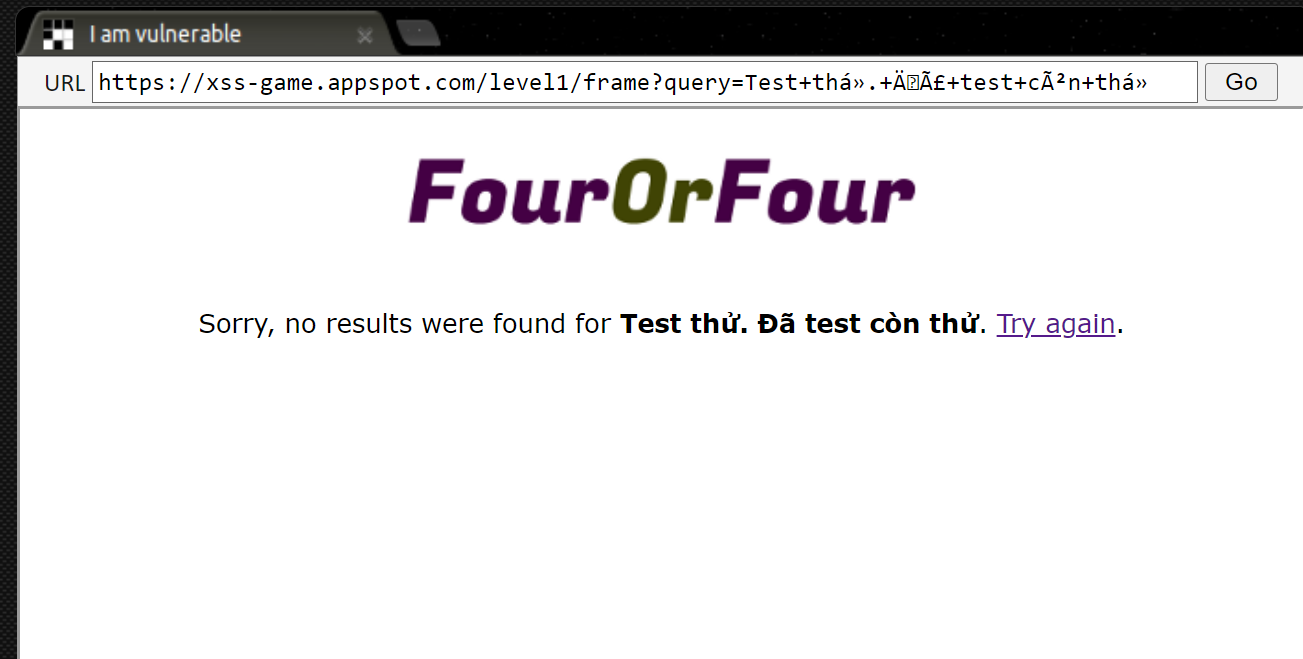
**# Mô tả lỗ hổng:**

**### Tóm tắt:** Thực hiện tiêm đoạn script để hiện Javascript alert() khi tìm kiếm thông tin.

**### Các bước thực hiện và hình ảnh minh chứng**

1. Bước 1: Thực hiện search để xem cách website hoạt động

+ Search với từ khóa thường: Thấy output có hiện lại nội dung input



1. Bước 2: Thử search với thẻ <h1>Liệu h1 có chạy </h1>

+ Có thể thấy. H1 được hiển thị và không bị xử lý.



1. Bước 3: Thử tiêm một script để hiện pop up một JS alert()

+ <script>alert("Fan thay Khoa")</script>

Graphical user interface

Description automatically generated

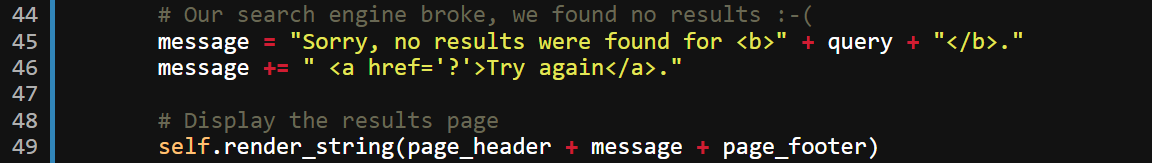
+ Inject thành công, hiện popup JS alert "Fan thầy Khoa"

Graphical user interface, text, application

Description automatically generated

**### Giải thích lỗ hổng**

1. Khi không tìm thấy nội dung tìm kiếm, string input sẽ được dùng để render trực tiếp trong kết quả trả về mà không có xử lý **escaping input** (xử lý các ký tự đặc biệt) và **kiểm tra**
2. Vị trí code gây lỗ hổng: Dòng 45, 49



**# Mức độ ảnh hưởng của lỗ hổng:** Gây ảnh hưởng đến trải nghiệm của người dùng, uy tín của dịch vụ

**# Khuyến cáo khắc phục:** Xử lý chuỗi đầu vào: escape string, validation.

## [2/6] Level 2: Persistence is key

**# Tiêu đề:** Persistence XSS Attack để hiển thị pop-up khi user click vào các comment chứa script độc hại được lưu trữ trên server.

**# Mô tả lỗ hổng:**

**### Tóm tắt:** Lưu Script độc dưới dạng comment để lưu trong server, khi một user khác truy cập sẽ gửi script độc về, trong trường hợp này, nếu nhấn vào comment có dẫn thuộc tính onclick sẽ hiện pop-up alert.

**### Các bước thực hiện và hình ảnh minh chứng**

1. Bước 1: Thử dùng đoạn script <script>alert("Fan thay Khoa")</script> thì thấy không có gì xảy ra. Nên cần chọn hướng khai thác khác

Graphical user interface, text, application, email

Description automatically generated

1. Bước 2: Post một comment là một thẻ <a> với event onclick để bật alert khi click vào: <a href="#" onclick="alert()">From Thay Khoa Fan Club</a>

Graphical user interface, text, application

Description automatically generated

1. Bước 3: Khi user khác truy cập vào nhấp vào comment này, sẽ hiện alert:

Graphical user interface, text, application

Description automatically generated

**### Giải thích lỗ hổng:**

+ Nội dung mà user comment được lưu lại và hiển thị mà không xử lý escaping và xác thực. Nên có thể thực thi script với event "onclick" hoặc "onerror"

**# Mức độ ảnh hưởng của lỗ hổng:** Ảnh hưởng đến bất kỳ người dùng nào truy cập website vì script độc đã lưu trên server. Tương đối nghiêm trọng vì có thể gây ảnh hưởng đến trải nghiệm của người dùng, có thể khiến máy người dùng bị ép tải virus, người dùng bị dẫn đến một web lừa đảo khác,...

**# Khuyến cáo khắc phục:** Xử lý escape string và validate (kiểm tra) nội dung trước khi hiển thị lên web.

## [3/6] Level 3: That sinking feeling...

**# Tiêu đề:** Thay đổi URL để khai thác lỗ hổng XSS

**# Mô tả lỗ hổng:**

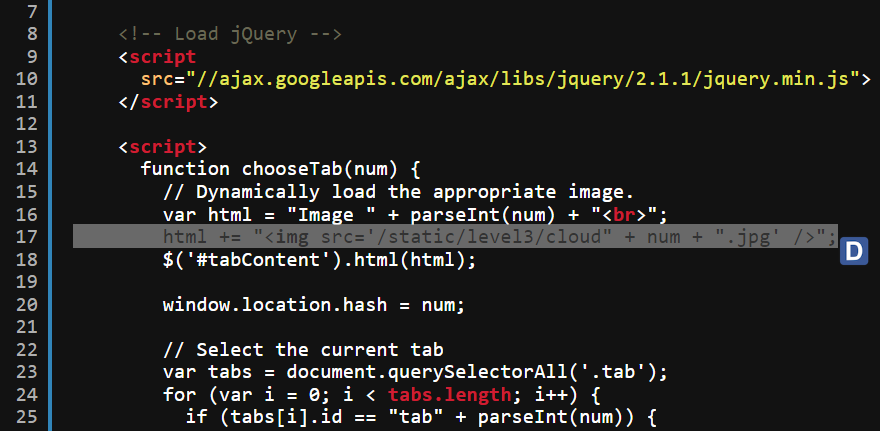
**### Tóm tắt:** Thực hiện thay đổi URL (tiêm script độc) để web hiển thị pop-up theo mục đích tấn công

**### Các bước thực hiện và hình ảnh minh chứng**

1. Bước 1: Ở bài này không có input hoặc field để nhập script độc hại, nên ta sẽ tìm một cách khác. Khi quan sát source code, ta thấy có một câu lệnh có thể khai thác được (line 17)

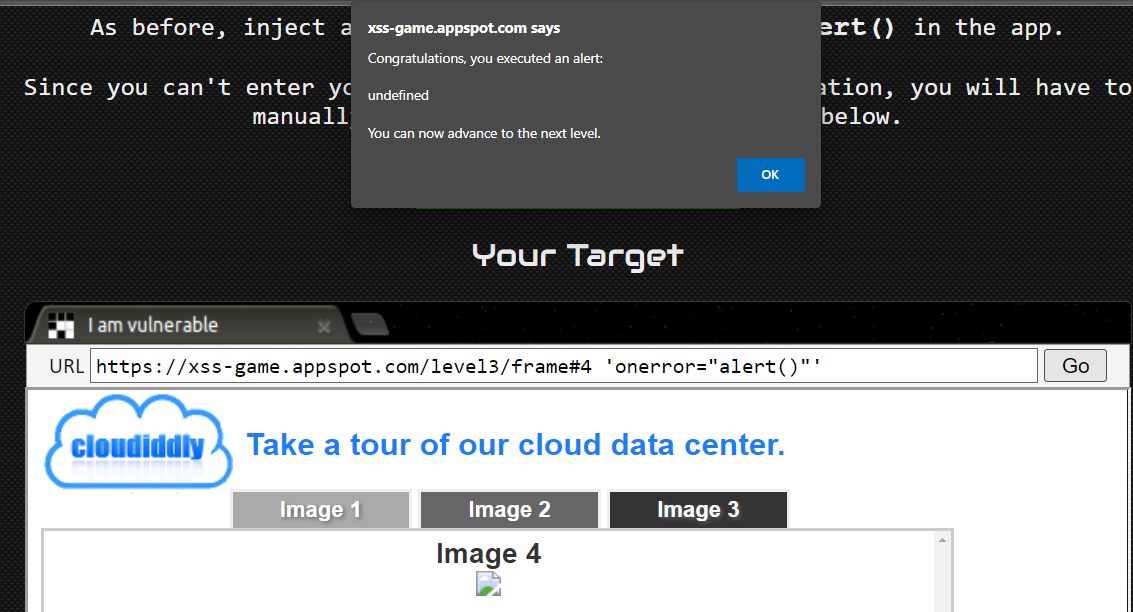
+ Hướng khai thác 1: do có 3 hình ảnh được đánh số từ 1-3, ta có thể đổi URL thành 4 hoặc các số khác 1-3 và kích hoạt event onerror

+ Hướng khai thác 2: vẫn giữ nguyên hình ảnh nhưng thêm event onclick.



1. Bước 2: Tiến hành thay đổi URL

+ Hướng 1: đổi num của hình ảnh và thêm event onerror



+ Hướng 2: vẫn hiển thị đúng hình ảnh và thêm event onclick vào hình ảnh đó. Ví dụ khi click vào ảnh 1

Graphical user interface

Description automatically generated

**### Giải thích lỗ hổng**

+ Ở line 17: vì biến num của frame để truy vấn cho hình ảnh, ta có thể lợi dụng nó để làm cho dẫn đến link ảnh không tồn tại và gọi event onerror. Hoặc đơn giản hơn là injection js code event onlick.

Text

Description automatically generated

**# Mức độ ảnh hưởng của lỗ hổng:** Ảnh hưởng đến người dùng click vào URL độc hại này, dẫn tới nhiều hậu quả khác, có thể là lừa đảo, chiếm đoạt tài soản, hoặc đánh cắp thông tin.

**# Khuyến cáo khắc phục:** Kiểm tra URL

## [4/6] Level 4: Context matters

**# Tiêu đề:** Tấn công thay đổi ngữ cảnh câu lệnh để thực thi lệnh theo cách attacker mong muốn để khai thác website

**# Mô tả lỗ hổng:**

**### Tóm tắt:** Tiêm input độc hại để code bên dưới hệ thống bị thay đổi (thêm) chức năng và hiển thị pop-up.

**### Các bước thực hiện và hình ảnh minh chứng**

1. Bước 1: Quan sát source code file timer.html ta thấy line 21 có thể khai thác được



+ Trong trường hợp này, nếu chúng ta nhập input là một số nguyên, thì event onload sẽ chạy hàm startTimer như sau: onload="startTimer('3');" Vì số 3 sẽ được parse sang số nguyên bằng hàm parseInt.

+ Ý tưởng là ta thêm một hành động khác trong event onload, bằng cách thêm '); để cho biết đã khai báo xong hàm startTimer và thêm alert() sau đó:

onload="startTimer('3**');alert('Em chao thay Khoa**');"

Như vậy, hàm onload sẽ gọi hàm startTimer sau đó thực thi lệnh alert().

1. Bước 2: Nhập input là 3');alert('Em chao thay Khoa

Graphical user interface, text, application

Description automatically generated

**### Giải thích lỗ hổng**

+ Lỗ hổng này lợi dụng ngữ cảnh cú pháp và các kí tự đặc biệt để thực thi thêm lệnh mà kẻ tấn công mong muốn, lợi dụng cú pháp có sẵn của lệnh để viết thêm và tạo ra một lệnh mới hoạt động độc hại.

**# Mức độ ảnh hưởng của lỗ hổng:** Có thể lợi dụng để khai thác thông tin về trang web, khai thác cơ sở dữ liệu,…

**# Khuyến cáo khắc phục:** Kiểm tra input đầu vào, chỉ cho phép nhập số nguyên.

## [5/6] Level 5: Breaking protocol

**# Tiêu đề:** Lợi dụng tham số trên URL để thay đổi thực thi của website và hiện popup

**# Mô tả lỗ hổng:**

**### Tóm tắt:** Trong trang signup có anchor Next>> và link tới một trang dựa trên giá trị của tham số next trên URL. Ta thay đổi giá trị của next để gọi js alert.

**### Các bước thực hiện và hình ảnh minh chứng**

1. Bước 1: Quan sát URL trang signup và source code ở signup.html, ta thấy next=confirm và phần tử a ở dòng 15 gọi next để dẫn đến trang confirm, nên ta có ý tưởng là thay confirm bằng js alert.





1. Bước 2: Ta thay đổi URL với next=javascript:alert('')

https://xss-game.appspot.com/level5/frame/signup?next=javascript:alert('')

1. Bước 3: Bấm Go (để lưu lại URL) và nhập email signup, nhấn Next

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

**### Giải thích lỗ hổng:**

+ XSS đôi khi không nằm ở việc có xử lý và kiểm tra input hay chưa, mà cũng không cần thay đổi cấu trúc DOM, chỉ đơn giản là dựa vào luồng thực thi mà trang web được lập trình sẵn để chuyển sang thực hiện câu lệnh độc hại khác.

**# Mức độ ảnh hưởng của lỗ hổng:** Nghiêm trọng, kẻ tấn công có thể lợi dụng để lừa đảo người dùng, đánh cắp thông tin cá nhân, tài sản,…

**# Khuyến cáo khắc phục:** Không để code thực thi bằng cách dùng giá trị của tham số trên URL.

## [6/6] Level 6: Follow the rabbit

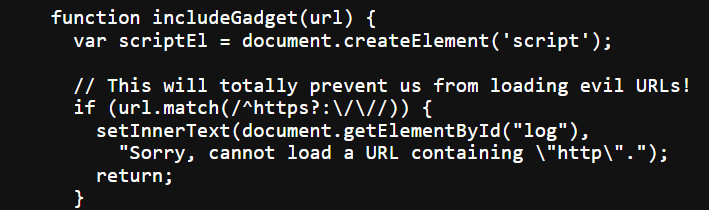
**# Tiêu đề:**

**# Mô tả lỗ hổng:**

**### Tóm tắt:**

**### Các bước thực hiện và hình ảnh minh chứng**

1. Bước 1: Quan sát mã nguồn, tâ thấy có hàm includeGadget(url) ngăn chặn user load HTTP URL, nhưng những định dạng khác thì không check.



1. Bước 2: Vậy ta sẽ load text mà không chứa http url, mà chứa js alert

Graphical user interface

Description automatically generated

**### Giải thích lỗ hổng:**

+ Lập trình viên ngăn chặn HTTP URL độc hại nhưng lại ko kiểm soát hết các trường hợp khác, khiến kẻ tấn công có cơ hội lợi dụng và thực thi XSS js alert

**# Mức độ ảnh hưởng của lỗ hổng:** Nghiêm trọng vì sẽ để lộ nhiều lỗ hổng trong website và làm mất tác dụng về an toàn thông tin như mục đích chặn HTTP URL ban đầu.

**# Khuyến cáo khắc phục:** Thêm các biện pháp xử lý URL ở những định dạng data khác nhau ngoài HTTP URL.

## Tài liệu tham khảo

* Slide bài giảng XSS trên lớp
* Hint của https://xss-game.appspot.com/

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

*Ví dụ: [*NT101.K11.ANTT*]-Session1\_Group3.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)