Group Project 7

TEST SECURITY

Danh sách thành viên nhóm:

1. Trịnh Quý Thiện (Nhóm trưởng)

2. Trần Viết Thịnh

3. Đặng Văn Nhớ

4. Nguyễn Thành Nhân

5. Nguyễn Văn Quang Thái

Lỗ hổng tìm được

# **1.Buffer Overflow**

- lỗi Buffer overflow hay tiếng Việt gọi là lỗi tràn bộ nhớ đệm/lỗi tràn bộ đệm là khi mà bộ nhớ bị ghi đè nhiều lần trên ngăn xếp. Lỗi này thường xuyên xảy ra do người dùng gửi một lượng lớn [dữ liệu](https://bkhost.vn/blog/data-du-lieu/) tới server ứng dụng, điều này làm cho dữ liệu bị bắt phải đè lên các vị trí bộ nhớ liền kề đó.

## **Nguyên nhân gây ra lỗi Buffer Overflow**

* Không thực hiện đầy đủ, hoặc không kiểm tra biên.
* Các ngôn ngữ lập trình như C, bản thân nó đã luôn có những tiềm ẩn các lỗ hổng mà hacker dễ dàng có thể tấn công vào. [Trong ngôn ngữ lập trình](https://bkhost.vn/blog/cac-ngon-ngu-lap-trinh-pho-bien-nhat-hien-nay/) C còn tồn tại các hàm không kiểm tra những buffer được cấp phát trên stack có kích thước lớn hơn dữ liệu được copy và bộ đệm hay không.

## **Các cách khai thác lỗi Buffer Overflow**

### **Khai thác lỗi Buffer Overflow trên stack**

* Để gây ra tình trạng lỗi tràn bộ đệm, hacker có thể ghi đè một biến địa phương nằm gần bộ đệm trong stack, biến này làm thay đổi hành vi của hệ thống để tạo điều kiện tấn công cho kẻ xấu.
* Ghi đè lên địa chỉ trả về trong khung stack. Khi hàm trả về, thực thi sẽ vẫn tiếp tục tại địa chỉ mà hacker đã chỉ định, thông thường địa chỉ này thuộc khu vực bộ đệm chứa dữ liệu người dùng.

### **Lỗi Buffer Overflow trên Heap**

* Bộ nhớ heap là bộ phận thường để chứa dữ liệu của chương trình, nó được cấp phát tự động bởi các ứng dụng thời gian chạy.
* Hacker thực hiện tấn công bằng cách phá những dữ liệu này để làm ứng dụng ghi đè lên các dữ liệu của nội bộ (ví dụ như các con trỏ của danh sách liên kết).

## **Các biện pháp chống tràn bộ nhớ đệm**

* Chỉ nên sử dụng các thư viện an toàn: thư viện được viết tốt, được test thử với các dạng dữ liệu trừu tượng mà các thư viện này tự động quản lý bộ nhớ.
* Để hạn chế nhất việc phát sinh lỗi Buffer overflow, chương trình cần phải đảm bảo diễn ra việc xác nhận đầu vào. Khi có bất kì một field, form đăng ký, các phương pháp khác yêu cầu nhập đầu vào thì đều mang những nguy cơ tiềm ẩn về lỗ hổng cho việc tấn công. Không chỉ là những yếu tố như [HTTP header](https://bkhost.vn/blog/http-header/), field, giao diện [XML](https://bkhost.vn/blog/xml-la-gi/) mà tất cả các giá trị input ở bất kì khu vực nào của ứng dụng phần mềm thì các bạn cũng cần phải có sự kiểm tra kĩ lưỡng.

2.

Khái niệm: Clickjacking là một hình thức tấn công đánh lừa người dùng nhấp chuột vô ý vào một đối tượng trên website. Khi nhấp chuột vào một đối tượng trên màn hình, người dùng nghĩ là mình đang click vào đối tượng đó nhưng thực chất họ đang bị lừa click vào một đối tượng khác > đã bị làm mờ hay ẩn đi. Kẻ tấn công có thể sử dụng kỹ thuật tấn công này cho nhiều mục đích. Đánh cắp tài khoản người dùng, lừa click vào quảng cáo để kiếm tiền, lừa like page

Ngăn chặn:

### **X-Frame-Options**

X-Frame-Options HTTP header có thể dùng để biểu thị có hoặc không cho phép trình duyệt render các thẻ như <frame>, <iframe>, <object>. Nó được thiết kế đặc biệt để chống clickjacking.

### **Frame-Killing**

Trên các trình duyệt cũ, cách thường được sử dụng để bảo vệ người dùng khỏi clickjacking là thêm frame-killing JavaScript snippet vào pages.

Giải thích một chút: Khi trang web load, đoạn code trên sẽ kiểm tra domain của trang gốc có khớp với domain của cửa sổ trình duyệt hay không, nếu pass qua bước check thì được phép hiển thị.

2. Generic Padding Oracle

- Bằng cách thao túng phần đệm trên một chuỗi được mã hóa, kẻ tấn công có thể tạo ra một thông báo lỗi cho biết có khả năng xảy ra lỗ hổng 'padding oracle'. Một lỗ hổng như vậy có thể ảnh hưởng đến bất kỳ ứng dụng hoặc khung nào sử dụng mã hóa không đúng cách, chẳng hạn như một số phiên bản của ASP.net, Java Server Faces và Mono. Kẻ tấn công có thể khai thác vấn đề này để giải mã dữ liệu và khôi phục các khóa mã hóa, có khả năng xem và sửa đổi dữ liệu bí mật. Quy tắc này sẽ phát hiện lỗ hổng tiên tri phần đệm MS10-070 trong ASP.net nếu CustomErrors được bật cho điều đó.

- Mục tiêu khai thác: Các website asp.net chưa cập nhật bản vá Asp.net padding oracle

3. SQL Injection – SQLite

-SQL injection là một lỗi kỹ thuật do người lập trình vô tình (hoặc có thể cố ý) tạo ra khi lập trình một ứng dụng web, đây là lỗ hổng của việc kiểm tra đầu vào (input) của người dùng có chứa các ký tự đặc biệt gây ảnh hưởng đến hệ thống cơ sở dữ liệu.

--> Từ đó cho phép các hacker có thể vượt qua quá trình kiểm tra dữ liệu chỉ bằng vài ký tự đặc biệt. kết quả như bạn đã biết là gây ra các sự cố bảo mật dẫn đến rò rỉ dữ liệu của người dùng không hề mong muốn. Thông thường lỗi SQL injection thường xảy ra ở: Form đăng nhập/đăng ký, form tìm kiếm, form tra cứu dữ liệu,…

- Lỗ hổng là một ví dụ về một kịch bản từng được coi là không thực tế trong nhiều thập kỷ trước - phân bổ chuỗi đầu vào 1GB. Giờ đây, kịch bản trở nên khả thi do sự ra đời của hệ thống máy tính 64-bit.

1. Absence of Anti-CSRF Tokens- ( Cross Site Request Forgery)

Khái niệm: CSRF ( Cross Site Request Forgery) là kỹ thuật tấn công bằng cách sử dụng quyền chứng thực của người dùng đối với một website. CSRF là kỹ thuật tấn công vào người dùng, dựa vào đó hacker có thể thực thi những thao tác phải yêu cầu sự chứng thực. Hiểu một cách nôm na, đây là kỹ thuật tấn công dựa vào mượn quyền trái phép.

Giả mạo yêu cầu trên nhiều trang web là một cuộc tấn công liên quan đến việc buộc nạn nhân gửi yêu cầu HTTP đến đích đích mà họ không biết hoặc có ý định thực hiện một hành động với tư cách là nạn nhân. Nguyên nhân cơ bản là chức năng ứng dụng sử dụng các hành động URL/biểu mẫu có thể dự đoán theo cách có thể lặp lại. Bản chất của cuộc tấn công là CSRF khai thác lòng tin mà một trang web dành cho người dùng. Ngược lại, cross-site scripting (XSS) khai thác sự tin tưởng mà người dùng dành cho một trang web. Giống như XSS, các cuộc tấn công CSRF không nhất thiết phải xảy ra trên nhiều trang web, nhưng chúng có thể xảy ra.

- Các cuộc tấn công CSRF có hiệu quả trong một số trường hợp:

\* Nạn nhân có một phiên hoạt động trên trang đích.

\* Nạn nhân được xác thực qua HTTP auth trên trang đích.

\* Nạn nhân nằm trên cùng một mạng cục bộ với trang đích.

- CSRF chủ yếu được sử dụng để thực hiện một hành động chống lại trang web mục tiêu bằng cách sử dụng các đặc quyền của nạn nhân, nhưng các kỹ thuật gần đây đã được phát hiện để tiết lộ thông tin bằng cách giành quyền truy cập vào phản hồi. Nguy cơ tiết lộ thông tin tăng lên đáng kể khi trang đích dễ bị XSS, vì XSS có thể được sử dụng làm nền tảng cho CSRF, cho phép cuộc tấn công hoạt động trong giới hạn của chính sách cùng nguồn gốc.

5. Content Security Policy (CSP) Header Not Set

- Chính sách bảo mật nội dung (CSP) là một lớp bảo mật bổ sung giúp phát hiện và giảm thiểu một số loại tấn công nhất định, bao gồm Tấn công tạo tập lệnh chéo trang (XSS) và tấn công chèn dữ liệu. Các cuộc tấn công này được sử dụng cho mọi thứ, từ đánh cắp dữ liệu đến xóa trang web hoặc phân phối phần mềm độc hại. CSP cung cấp một bộ tiêu đề HTTP tiêu chuẩn cho phép chủ sở hữu trang web khai báo các nguồn nội dung đã được phê duyệt mà trình duyệt sẽ được phép tải trên trang đó — các loại được đề cập là JavaScript, CSS, khung HTML, phông chữ, hình ảnh và các đối tượng có thể nhúng như Java applet, ActiveX, tệp âm thanh và video.

6. Vulnerable JS Library

- Thư viện jquery được xác định, phiên bản 2.1.4 dễ bị tấn công.

7. XSLT Injection

Việc chèn bằng cách sử dụng phép biến đổi XSL có thể thực hiện được và có thể cho phép kẻ tấn công đọc thông tin hệ thống, đọc và ghi tệp hoặc thực thi mã tùy ý.