|  |  |
| --- | --- |
|  | |
| **HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  **Khoa Công nghệ Thông tin 2**  **---------------------------------------** | |
|  | |
|  | |
| **AN TOÀN ỨNG DỤNG WEB VÀ CƠ SỞ DỮ LIỆU** | |
| **ĐỒ ÁN MÔN HỌC** | |
| **Khai thác lỗ hỏng website bán máy tính** | |
|  | |
|  | |
| **Giảng viên:** | **ThS Phan Nghĩa Hiệp** |
| **Sinh viên thực hiện:** | **Vương Hữu An-N20DCAT002** |
|  |
|  |
|  |  |
|  |  |
| **Lớp:** | **D20CQAT01-N** |
|  | |
| **TP. HỒ CHÍ MINH - 2023** | |

# NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ...........................................................................................................................................

........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ........................................................................................................................................... ...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

...........................................................................................................................................

**Giảng viên hướng dẫn**

*(Ký và ghi rõ họ tên)*

# LỜI CẢM ƠN

Đầu tiên, chúng em xin gửi lời cảm ơn chân thành đến trường PTITHCM đã đưa môn *An toàn ứng dụng web và cơ sở dữ liệu* vào trương trình giảng dạy. Bên cạnh đó để thực hiện và hoàn thành tốt đồ án này, chúng em cũng nhận được sự giúp đỡ và hướng dẫn rất tận tình của các thầy cô thuộc khoa Công Nghệ Thông Tin 2. Các thầy cô thuộc bộ môn chuyên ngành đã cung cấp cho chúng em các thông tin, kiến thức vô cùng quý báu và cần thiết trong suốt thời gian qua để chúng em có thể thực hiện và hoàn thành đồ án của mình. Đặc biệt, chúng em xin gửi lời cảm ơn sâu sắc đến giảng viên bộ môn - Thầy Ths. Phan Nghĩa Hiệp - người đã trực tiếp hướng dẫn chúng em trong suốt thời gian học tập và thực hiện đồ án vừa qua.

Trong thời gian tham gia lớp học *An toàn ứng dụng web và cơ sở dữ liệu* của thầy, chúng em đã có thêm cho mình nhiều kiến thức bổ ích, tinh thần học tập hiệu quả, nghiêm túc. Đây chắc chắn sẽ là những kiến thức quý báu, là hành trang để chúng em có thể vững bước sau này. Bộ môn *An toàn ứng dụng web và cơ sở dữ liệu* là môn học thú vị, vô cùng bổ ích và có tính thực tế cao. Đảm bảo cung cấp đủ kiến thức, gắn liền với nhu cầu thực tiễn của sinh viên.

Tuy nhiên, do vốn kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ. Mặc dù chúng em đã cố gắng hết sức nhưng chắc chắn bài báo cáo khó có thể tránh khỏi những thiếu sót và nhiều chỗ còn chưa chính xác. Kính mong thầy thông cảm, xem xét và góp ý để bài báo cáo của chúng em được hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

# LỜI GIỚI THIỆU

Trong thời đại ngày nay, Internet đã trở nên quen thuộc và là một công cụ hữu ích phục vụ các hoạt động, nhu cầu sống của tất cả mọi người, đặc biệt là nhu cầu mua sắm chiếm một phần không nhỏ. Nắm bắt được nhu cầu này, nhóm đã lên ý tưởng và đưa ra kế hoạch thực hiện xây dựng một trang web bán máy tính. Trong quá trình phát triển ứng dụng web bán máy tính, nhóm đã nhận thấy những vấn đề nguy hiểm đe dọa đến cơ sở dữ liệu cũng như ứng dụng web bán máy tính. Điều này đã đặt ra vấn đề cấp thiết cần làm như thế nào để bảo đảm an toàn thông tin cho ứng dụng web và thông tin người sử dụng. Đồ án này được thực hiện nhằm mục đích giới thiệu rõ hơn về những mối nguy đến ứng dụng web, máy chủ web và cơ sở dữ liệu, từ đó đưa ra cách phòng chống cũng như các phương thức bảo mật cho ứng dụng web bán máy tính.

Nội dung của đồ án môn học này được biên soạn thành 3 phần ứng với 3 chương. Phần I – Bảo mật cơ sở dữ liệu ,phần II – Phòng chống tấn công ứng dụng và máy chủ web, và Phần III – Thực nghiệm trên ứng dụng web bán máy tính. Nội dung tóm tắt các chương như sau:

Chương 1 – *Bảo* *mật* *cơ* *sở* *dữ* *liệu* khái quát các mối nguy hại tới cơ sở dữ liệu như: mật khẩu yếu hoặc mặc định, SQL Injection, đặc quyền quá mức cho người dùng hoặc nhóm người dùng, cho phép các tính năng không sử dụng trong DBMS, leo thang đặc quyền, tấn công từ chối dịch vụ (denial of service) và không mã hóa dữ liệu. Bên cạnh đó chương cũng đề cập tới các kịch bản tấn công và phương pháp phòng chống những nguy cơ trên.

Chương 2 – *Phòng chống tấn công* *ứng* *dụng* *và* *máy* *chủ* *web* giới thiệu khái quát về một số dạng tấn công lên ứng dụng và máy chủ web mà nhóm đã lên kịch bản tấn công và đưa ra được cách phòng chống như: tấn công chèn mã HTML và XSS, tấn công CSRF, SQL Injection, tấn công các cơ chế xác thực và các lỗ hổng trong cấu hình máy chủ web.

Chương 3 – *Các biện pháp bảo mật máy chủ và trình duyệt web*

Bài báo cáo được biên soạn dựa trên những kiến thức được học từ môn An toàn Ứng dụng Web và cơ sở dữ liệu và một số môn học liên quan trong suốt quá trình học tập của nhóm tác giả tại Học viện Công nghệ Bưu chính Viễn thông. Trong quá trình biên soạn và triển khai mô hình, mặc dù nhóm tác giả đã rất cố gắng song không thể tránh khỏi những thiếu sót. Nhóm mong rằng sẽ nhận được ý kiến phản hồi và góp ý, cũng như ý kiến về cập nhật, hoàn thiện đồ án.

# 

# MỤC LỤC

[NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN 2](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130494)

[LỜI CẢM ƠN 3](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130495)

[MỤC LỤC 4](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130496)

[CHƯƠNG 1. LỖ HỎNG CƠ SỞ DỮ LIỆU 8](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130499)

[1.1 Các mật khẩu yếu hoặc ngầm định 8](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130500)

[1.2 Lỗi chèn mã SQL Injection 12](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130501)

[1.3 Đặc quyền quá mức cho người dùng hoặc nhóm người dùng 19](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130503)

[1.4 Cho phép các tính năng không sử dụng DBSM 20](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130504)

[1.5 Dữ liệu không được mã hóa 20](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130504)

[1.6 Tấn công từ chối dịch vụ DDOS 20](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130504)

[CHƯƠNG 2. TẤN CÔNG ỨNG DỤNG WEB 23](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130505)

[2.1 Chèn mã html hoặc XSS 23](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130506)

[2.2 SQL Injection 24](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130507)

[2.3 Tấn công vào cơ chế xác thực 25](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130508)

[2.4 Tấn công lợi dụng các khiếm khuyết thiết kế 26](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130509)

[CHƯƠNG 3. CÁC BIỆN PHÁP BẢO MẬT MÁY CHỦ VÀ TRÌNH DUYỆT WEB 30](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130513)

[3.1 Xác thực người dùng và phân quyền truy cập 30](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130514)

[3.2 Bảo mật phiên làm việc 32](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130515)

[3.3 Bảo mật máy chủ web 33](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130516)

[3.4 Bảo mật cơ sở dữ liệu web 34](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130517)

[3.5 Bảo mật hệ thống file 34](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130517)

[TÀI LIỆU THAM KHẢO 37](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130526)

[BẢNG PHÂN CÔNG CÔNG VIỆC 38](file:///C:\Users\HP\Downloads\Group12.docx#_Toc122130527)

**CHƯƠNG 1. LỖ HỎNG CƠ SỞ DỮ LIỆU**

* 1. **Các mật khẩu yếu hoặc ngầm định**

**Khái quát:**

Mật khẩu yếu hoặc ngầm định là những mật khẩu đơn giản, dễ đoán, hoặc được cài đặt sẵn từ nhà sản xuất. Chúng thường ngắn, không phức tạp, hoặc là các từ thông dụng như "password", "123456", hoặc "admin". Mật khẩu ngầm định, thường giống nhau trên nhiều thiết bị hoặc hệ thống, dễ bị tấn công bởi hacker vì chúng thường được biết đến rộng rãi và ít khi được người dùng thay đổi sau khi cài đặt. Để tăng cường bảo mật, người dùng nên tạo mật khẩu mạnh, độc đáo cho mỗi tài khoản và thay đổi mật khẩu ngầm định ngay sau khi thiết lập thiết bị hoặc tài khoản.

**Thực hiện:**

Thêm logic validate password khi đổi mật khẩu và đăng ký tài khoản, mật khẩu phải lớn hơn 8 ký tự, có ít nhất 1 ký tự chữ thường, chữ hoa và ký tự đặc biệt

**A screenshot of a registration form

Description automatically generated**

* 1. **Lỗi chèn mã SQL Injection** 
     1. **Khái quát:**

Tấn công chèn mã SQL (SQL Injection) là một kỹ thuật cho phép kẻ tấn công chèn mã SQL vào dữ liệu gửi đến máy chủ và cuối cùng được thực hiện trên máy chủ cơ sở dữ liệu. Tùy vào mức độ tinh vi, tấn công chèn mã SQL có thể cho phép kẻ tấn công (1) vượt qua các khâu xác thực người dùng, (2) chèn, sửa đổi, hoặc xóa dữ liệu, (3) đánh cắp các thông tin trong cơ sở dữ liệu và (4) chiếm quyền điều khiển hệ thống máy chủ cơ sở dữ liệu. Tấn công chèn mã SQL là dạng tấn công thường gặp ở các ứng dụng web, các trang web có kết nối đến cơ sở dữ liệu.

* + 1. **Phòng chống:**

- Sử dụng Prepared Statements: Tránh nối chuỗi trong câu truy vấn SQL.

- Kiểm tra đầu vào: Hạn chế và kiểm tra định dạng của dữ liệu đầu vào.

- Hạn chế quyền truy cập cơ sở dữ liệu: Chỉ cấp quyền cần thiết cho tài khoản cơ sở dữ liệu.

- Cập nhật hệ thống: Đảm bảo cơ sở dữ liệu và ứng dụng web luôn được cập nhật.

**1.2.3 Thực hiện:**

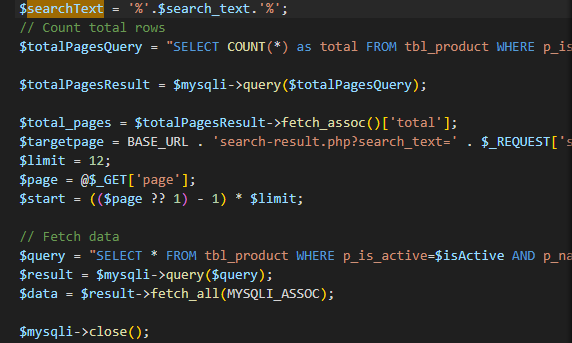
Khi search với ' OR '1'='1, nó đã hiện hết sản phẩm trong database ra:  
A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

**Hình ảnh đầu tiên hiển thị mã PHP nơi biến $searchText được bao gồm trực tiếp trong truy vấn SQL. Đây là một trường hợp dễ bị lỗi SQL injection vì đầu vào không được làm sạch hoặc sử dụng tham số:**

****

**Trong mã này, nếu đầu vào người dùng cho $\_REQUEST['search\_text'] bao gồm mã SQL (như ' OR '1'='1), nó sẽ được thực thi bởi máy chủ SQL, có thể dẫn đến việc tiết lộ hoặc thao tác dữ liệu không được phép.**

**' OR '1'='1 làm cho truy vấn luôn đúng vì '1'='1' là một điều kiện luôn đúng. Điều này dẫn đến việc truy vấn sẽ chọn tất cả các sản phẩm từ cơ sở dữ liệu, bất kể giá trị product\_name.**

**Kết Quả: Vì truy vấn luôn đúng, nó trả về tất cả các sản phẩm trong cơ sở dữ liệu của bạn, không phụ thuộc vào điều kiện tìm kiếm ban đầu**

* Sau khi bảo mật lỗi này:

A computer screen with text

Description automatically generated

**Hình ảnh này cho thấy mã PHP được cải thiện sử dụng câu lệnh chuẩn bị với các vị trí giữ chỗ, đây là cách đúng để ngăn chặn SQL injection:**

**A computer screen shot of text

Description automatically generated**

**Trong mã cải thiện này, đầu vào người dùng được gửi như một tham số cho câu lệnh chuẩn bị, đảm bảo rằng nó được xử lý như một giá trị chuỗi thay vì một phần của truy vấn SQL. Điều này ngăn chặn bất kỳ mã SQL nào được nhúng trong đầu vào từ việc được thực thi.**

**Lỗ hổng được sửa chữa bằng cách tránh việc bao gồm đầu vào người dùng trực tiếp trong câu lệnh SQL. Thay vào đó, sử dụng câu lệnh chuẩn bị với các tham số liên kết giúp đảm bảo rằng đầu vào người dùng không thể can thiệp vào cấu trúc truy vấn.**

**.**

A screenshot of a computer

Description automatically generated

* 1. **Đặc quyền quá mức cho người dùng hoặc nhóm người dùng:**

Hệ thống đang chia thành các role

******

***Super Admin:***

* Quyền cao nhất trong hệ thống.
* Có thể thực hiện mọi thao tác trên hệ thống, bao gồm cả quản lý Admin và Customer.
* Có quyền truy cập vào tất cả các phần của hệ thống.
* Có thể thay đổi quyền hạn của Admin và Customer.
* Thêm, xóa, sửa mọi thông tin quản lý sản phẩm.
* Thống kê doanh thu theo tháng hoặc năm.
* Tổng hợp các vấn đề thế mạnh thế, thế yếu của cửa hàng.

***Admin*:**

* Có quyền quản lý và thực hiện các thao tác quản lý cơ bản trên hệ thống.
* Không có quyền thay đổi quyền hạn của Super Admin.
* Có thể thêm, sửa, và xóa các tài khoản Customer.
* Quản lý các chức năng và dữ liệu cụ thể mà Customer không thể truy cập.
* Thống kê doanh thu và gửi báo cáo.
* Quản lý và tư vấn các vấn đề của khách hàng.

***Customer*:**

* Có quyền truy cập vào các chức năng và dữ liệu liên quan đến cá nhân hóa và sử dụng dịch vụ của họ (thêm, xóa giỏ hàng).
* Không có quyền thay đổi quyền hạn của Admin hoặc Super Admin.
* Có thể xem và cập nhật thông tin cá nhân của mình (trang cá nhân).
* Thực hiện các thao tác liên quan đến dịch vụ hoặc sản phẩm mà họ đã mua (giao dịch, đánh giá, chia sẽ ).

***Guest***:

* Đăng nhập, Đăng ký
* Xem danh sách sản phẩm
* Thêm sản phẩm vào giỏ hàng
* Tìm kiếm sản phẩm
* Sử dụng chức năng quên mật khẩu
  1. **Cho phép các tính năng không sử dụng DBSM**

Chỉ tạo user connect vào DB với 1 số quyền nhất định, không có quá nhiều quyền như tạo db, xoá db, sửa db,… mà chỉ có các quyền select, insert, update, delete record trên db

CREATE USER 'username'@'localhost' IDENTIFIED BY 'password';

GRANT SELECT, INSERT, UPDATE, DELETE ON database\_name.\* TO 'username'@'localhost';

Sau đó sử dụng user này để connect tới DB

A screen shot of a computer program

Description automatically generated

* 1. **Dữ liệu không được mã hóa:**
     1. **Khái quát:**

-Dữ liệu không được mã hóa là thông tin được lưu trữ hoặc truyền tải mà không có bất kỳ biện pháp bảo mật nào như mã hóa. Điều này có nghĩa là dữ liệu có thể được đọc một cách dễ dàng mà không cần bất kỳ khóa hoặc thuật toán nào để giải mã. Trong trạng thái này, dữ liệu dễ bị truy cập và sử dụng không phù hợp bởi những người không có quyền, gây ra rủi ro bảo mật lớn.

**1.5.2 Phòng chống:**

-Mã hóa dữ liệu: Sử dụng các phương pháp quản lý khóa mã hóa an toàn để đảm bảo chỉ những người cần thiết mới có thể giải mã dữ liệu.

-Quản lý khóa mã hóa: Bảo vệ và quản lý khóa mã hóa một cách an toàn.

-Chính sách truy cập nghiêm ngặt: Hạn chế truy cập dữ liệu chỉ cho những người cần thiết.

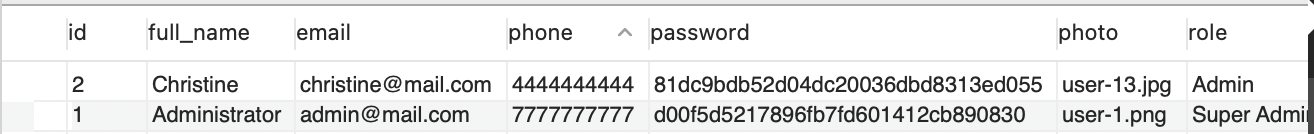
**1.5.3 Thực hiện:**

Mã hoá mật khẩu trong db để người dùng ko thể thấy được

* Trước khi mã hoá

******

* Sau khi mã hoá



A screen shot of a computer program

Description automatically generated

Mã hóa mật khẩu md5

* 1. **Tấn công từ chối dịch vụ DDOS**

**Khái quát:**

Tấn công từ chối dịch vụ phân tán (DDoS) là một loại tấn công mạng nơi nhiều hệ thống máy tính được sử dụng để gửi lưu lượng truy cập lớn đến một máy chủ hoặc mạng cụ thể, với mục đích làm quá tải và ngăn cản hoạt động bình thường của nó. Trong một tấn công DDoS, máy chủ hoặc mạng bị tấn công không thể xử lý lượng truy cập lớn đột ngột và không còn khả năng phục vụ người dùng hợp pháp.

Mục tiêu của tấn công DDoS thường là các trang web hoặc dịch vụ trực tuyến, với mục đích gây gián đoạn hoạt động, gây tổn thất về mặt tài chính hoặc uy tín. Tấn công này thường được thực hiện bởi mạng lưới các máy tính bị nhiễm malware (gọi là botnet), cho phép kẻ tấn công kiểm soát từ xa và sử dụng chúng để phát động tấn công mạng.

Để bảo vệ chống lại tấn công DDoS, các tổ chức thường sử dụng biện pháp như cân bằng tải, tường lửa,captcha, và các dịch vụ chống DDoS chuyên nghiệp, cũng như các chiến lược phân tán nguồn lực và mạng lưới để giảm thiểu tác động của các cuộc tấn công.

Thêm captcha vào những request post lên hệ thống như đăng ký, đăng nhập

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**CHƯƠNG 2. PHÒNG CHỐNG TẤN CÔNG ỨNG DỤNG WEB**

**2.1 Chèn mã HTML và XSS**

**2.1.1. Khái quát:**

Tấn công Cross-Site Scriting (XSS – Mã script liên site, liên miền) là một trong các dạng tấn công phổ biến nhất vào các ứng dụng web. XSS xuất hiện từ khi trình duyệt bắt đầu hỗ trợ ngôn ngữ JavaScript (ban đầu được gọi là LiveScript – trên trình duyệt Netscape). Mã tấn công XSS được nhúng trong trang web chạy trong lòng trình duyệt với quyền truy nhập của người dùng, có thể truy nhập các thông tin nhạy cảm của người dụng lưu trong trình duyệt. Do mã XSS chạy trong lòng trình duyệt nên nó miễn nhiễm với các trình quét các phần mềm độc hại và các công cụ bảo vệ hệ thống.

XSS có thể được xem là một dạng của chèn mã HTML (HTML Injection). Trên thực tế, có thể thực hiện tấn công bằng chèn mã HTML mà không cần mã JavaScript và cũng không cần liên site hoặc liên miền. Kẻ tấn công khai thác các lỗ hổng bảo mật để chèn mã XSS vào trang web, trong đó dữ liệu web (như trên và địa chỉ email) và mx (cú pháp và các phần tử như <script>) của XSS được trộn lẫn vào mã gốc của trang web.

Tấn công XSS thường xuất hiện khi trang web cho phép người dùng nhập dữ liệu và su dó hiển thị dữ liệu lên trang. Kẻ tấn công có thể khéo léo chèn mã script vào trang và mã script của kẻ tấn công được thực thiện khi người dùng khác thăm lại trang web đó. Tùy theo mục đích và mức độ tinh vi, XSS có thể cho phép kẻ tấn công thực hiện các thao tác sau trên hệ thống nạn nhân:

* Đánh cắp thông tin nhạy cảm của người dùng lưu trong Cookie của trình duyệt
* Giả mạo hộp đối thoại đăng nhập để đánh cắp mật khẩu
* Bắt phím gõ từ người dùng để đánh cắp thông tin về tài khoản ngân hàng, email và thông tin đăng nhập các dịch vụ trả tiền,…
* Sử dụng trình duyệt để quét các dịch vụ trong mạng LAN
* Lén lút cấu hình lại bộ định tuyến nội bộ để bỏ qua tường lửa của mạng nội bộ
* Tự động thêm người dùng ngẫu nhiên và tài khoản mạng xã hội
* Tạo môi trường cho tấn công CSRF

Nhìn chung, mã tấn công HTML/XSS có thể được chèn vào mọi vị trí trong địa chỉ (URL) và nội dung trang web. Các vị trí cụ thể có thể chèn mã:

* Các thành phần của URL (URL Components)
* Các trường nhập liệu (Form Fields) – HTTP Request Header & Cookie
* JavaScript Object Notation (JSON)
* Các thuộc tính của DOM (Document Object Model)
* CSS (Cascade Style Sheet)
* Các nội dung do người dùng tạo ra

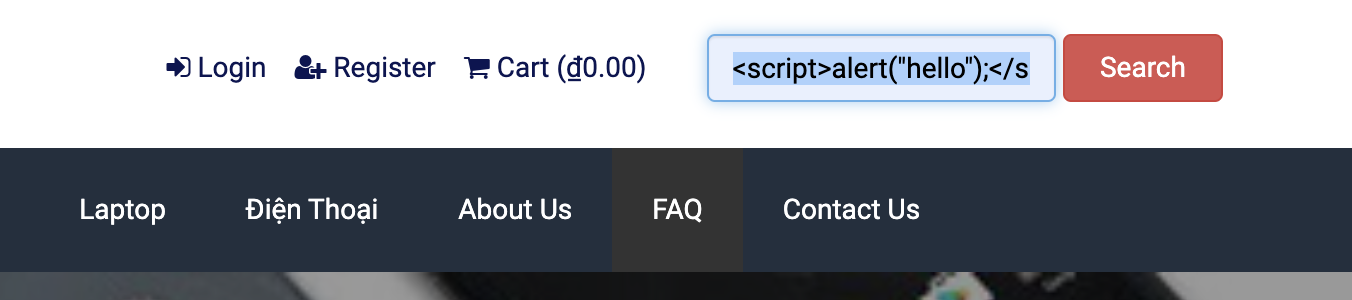
Có thể chia tấn công XSS thành 3 loại chính: Stored XSS (XSS lưu trữ), Reflected XSS (XSS phản chiếu) và DOM-based/Local XSS (XSS dựa trên DOM hoặc cục bộ).

**2.1.2: Kịch bản tấn công:**

Reflected Cross-site scripting:

Tiến hành tiêm các đoạn mã vào ô tìm kiếm của ứng dụng.

Chèn <script>alert("hello");</script> vào thanh tìm kiếm và xem kết quả



* Kết quả là nó đã chạy script mình vừa chèn ở thanh tìm kiếm và hiển thị ra ngoài  
  A white surface with a white background

  Description automatically generated

A computer screen shot of text

Description automatically generated

**Trong đoạn trên, biến $search\_text, được lấy từ $\_REQUEST['search\_text'], được echo trực tiếp ra trang web mà không qua bất kỳ hình thức làm sạch hay mã hóa nào. Điều này có thể tạo ra lỗ hổng XSS nếu người dùng nhập script độc hại vào hộp tìm kiếm và script đó được thực thi trên trình duyệt của người dùng khác.**

**Không có Sự Làm Sạch (Sanitization) Đầu vào: Trong đoạn code này, đầu vào từ người dùng (trong trường hợp này là mã JavaScript) được lấy trực tiếp từ biến $\_REQUEST['search\_text'] và sau đó được in ra (echo) trên trang web mà không qua bất kỳ bước làm sạch hoặc mã hóa nào. Điều này cho phép mã JavaScript được thực thi.**

**Thực Thi Mã Script: Khi trình duyệt tải trang web, nó sẽ phân tích và thực thi tất cả mã JavaScript mà nó gặp. Do đó, mã <script>alert("hello");</script> được thực thi, gây ra hiển thị thông báo "hello".**

**2.1.3. Phòng chống:**

- Để chặn lỗi này cần validate input của người dùng nhập, ta có thể sử dùng hàm htmlspecialchars, hàm này dùng để mã hoá các ký tự html nên nó sẽ ko dính lỗi này nữa

* echo '<div>' . htmlspecialchars($\_GET[searchText]) . '</div>';

A screenshot of a computer

Description automatically generated

**2.2 SQL Injection**

Tấn công chèn mã SQL (SQL Injection) là một kỹ thuật cho phép kẻ tấn công chèn mã SQL vào dữ liệu gửi đến máy chủ và cuối cùng được thực hiện trên máy chủ cơ sở dữ liệu. Tùy vào mức độ tinh vi, tấn công chèn mã SQL có thể cho phép kẻ tấn công (1) vượt qua các khâu xác thực người dùng, (2) chèn, sửa đổi, hoặc xóa dữ liệu, (3) đánh cắp các thông tin trong cơ sở dữ liệu và (4) chiếm quyền điều khiển hệ thống máy chủ cơ sở dữ liệu. Tấn công chèn mã SQL là dạng tấn công thường gặp ở các ứng dụng web, các trang web có kết nối đến cơ sở dữ liệu.

Có 2 nguyên nhân của lỗ hổng trong ứng dụng cho phép thực hiện tấn công chèn mã SQL:

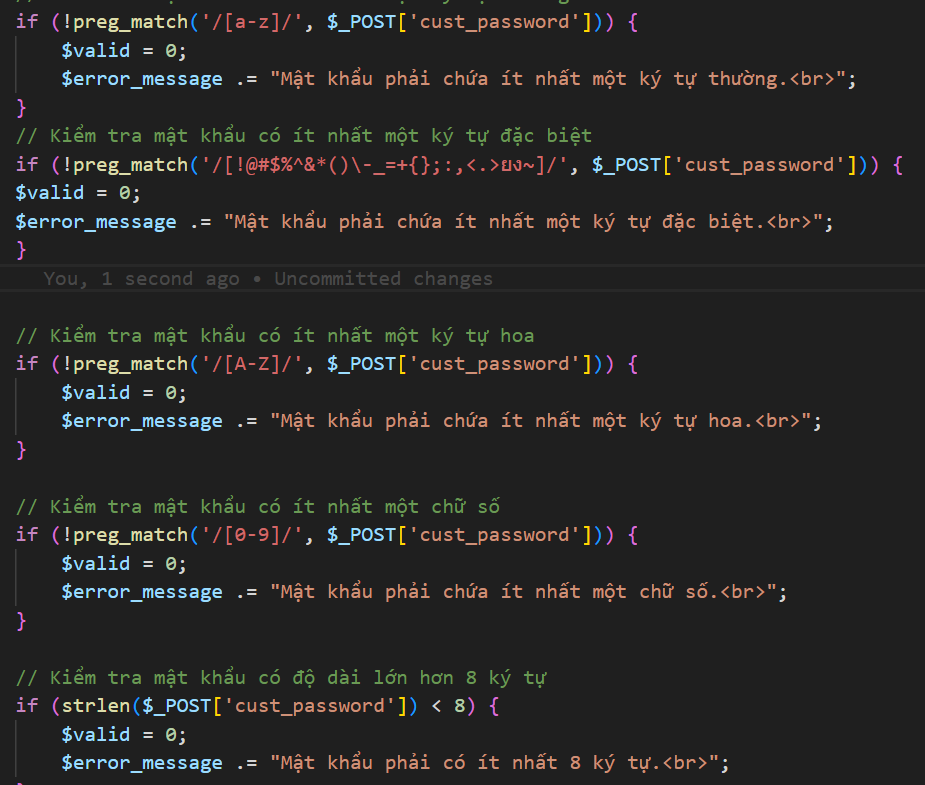
- Dữ liệu đầu vào từ người dùng hoặc từ các nguồn khác không được kiểm tra hoặc kiểm tra không kỹ lưỡng;

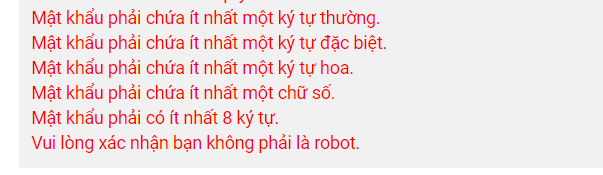
- Sử dụng các câu lệnh SQL động trong ứng dụng, trong đó có thao tác nối dữ liệu người dùng với mã lệnh SQL gốc.

Như mục 1, lỗi chèn mã SQL

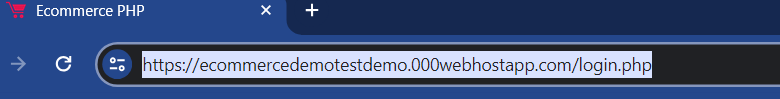
**2.3 Tấn công vào cơ chế xác thực**

* Brute Force Attack (Tấn công Brute Force): Kẻ tấn công thử tất cả các khả năng mật khẩu có thể để đăng nhập bằng cách liên tục thử các mật khẩu khác nhau. Đối với cơ chế xác thực, đây có thể là tấn công vào tài khoản người dùng bằng cách thử mật khẩu đến khi tìm ra một mật khẩu đúng -> Sử dụng mật khẩu mạnh mẽ hơn





* Man-in-the-Middle Attack (Tấn công Man-in-the-Middle): Kẻ tấn công đưa mình vào giữa truyền tải dữ liệu giữa người dùng và hệ thống xác thực, có thể theo dõi và thậm chí sửa đổi thông tin xác thực -> Sử dụng HTTPS để mã hoá thông tin gửi qua lại từ server đến trình duyệt web



**2.4 Tấn công lợi dụng các khiếm khuyết thiết kế**

* Hệ thống hiện tại đã validate các input được nhập từ người dùng, bao gồm những input có chứa mã độc, input có chữa script, hoặc các lỗi như sql injection

**CHƯƠNG 3. CÁC BIỆN PHÁP BẢO MẬT MÁY CHỦ VÀ TRÌNH DUYỆT WEB**

**3.1 Xác thực người dùng và phân quyền truy cập**

Hiện tại hệ thống đã có trang login cho khách hàng và cho admin  
- Trang login cho khách hàng  
A screenshot of a login form

Description automatically generated

* Trang login cho admin

**3.2 Bảo mật phiên làm việc**

* Xác thực (Authentication): Đảm bảo rằng quá trình xác thực người dùng được thực hiện một cách an toàn, sử dụng các phương tiện như mã thông tin, xác thực hai yếu tố, hoặc các phương pháp xác thực mạnh mẽ khác.
* Quản lý Phiên (Session Management): Điều này bao gồm việc tạo, duy trì và hủy phiên làm việc một cách an toàn. Các biện pháp bảo vệ bao gồm sử dụng mã hóa phiên, cơ chế đổi khóa, và cập nhật định kỳ.
* Bảo vệ chống Cross-Site Scripting (XSS): Ngăn chặn tấn công XSS bằng cách kiểm tra và lọc dữ liệu đầu vào, sử dụng mã hóa để ngăn chặn việc chèn mã độc hại vào trang web.
* Bảo vệ chống Cross-Site Request Forgery (CSRF): Sử dụng mã thông tin chống CSRF để đảm bảo rằng các yêu cầu được gửi từ người dùng đến máy chủ là hợp lệ.
* Sử dụng HTTPS: Bảo vệ dữ liệu truyền qua mạng bằng cách sử dụng kết nối an toàn HTTPS thay vì HTTP.
* Quản lý Cookie an toàn: Đảm bảo rằng thông tin trên cookie được mã hóa và chỉ được gửi qua kết nối an toàn.
* Thời gian chờ phiên làm việc (Session Timeout): Đặt thời gian chờ cho phiên làm việc để đảm bảo rằng nếu người dùng không hoạt động trong một khoảng thời gian dài, phiên của họ sẽ tự động kết thúc**.**

**3.3 Bảo mật máy chủ web**

* Cập Nhật Hệ Điều Hành và Phần Mềm Máy Chủ: Đảm bảo rằng hệ điều hành và tất cả các phần mềm máy chủ đều được cập nhật đến phiên bản mới nhất để bảo vệ chống lại các lỗ hổng bảo mật đã được vá.
* Cấu hình An Toàn: Thiết lập cấu hình máy chủ và ứng dụng web để đảm bảo sự an toàn và tối thiểu hóa rủi ro. Điều này bao gồm việc vô hiệu hóa các tính năng không cần thiết, giảm đặc quyền, và thực hiện các biện pháp an toàn khác.
* Bảo mật Kết Nối (SSL/TLS): Sử dụng giao thức HTTPS (SSL/TLS) để mã hóa dữ liệu truyền tải giữa máy khách và máy chủ, đảm bảo tính riêng tư và ngăn chặn tấn công gián điệp.
* Firewall: Sử dụng tường lửa để kiểm soát lưu lượng mạng đến và từ máy chủ, ngăn chặn các kết nối không mong muốn và giảm rủi ro từ các tấn công mạng.
* Phát Hiện Xâm Nhập (Intrusion Detection System - IDS) và Phòng Chống Xâm Nhập (Intrusion Prevention System - IPS): Cài đặt các hệ thống này để phát hiện và ngăn chặn các hành vi đáng ngờ hoặc tấn công từ bên ngoài.
* Quản lý Phiên Làm Việc: Đảm bảo quản lý phiên làm việc một cách an toàn để ngăn chặn tấn công như đánh cắp phiên.
* Quản lý Log và Giám Sát Hệ Thống: Ghi lại các sự kiện hệ thống và theo dõi log một cách chặt chẽ để phát hiện bất kỳ hoạt động không bình thường nào.
* Bảo vệ chống Tấn Công DDoS: Thực hiện biện pháp để ngăn chặn và giảm thiểu ảnh hưởng của các tấn công từ chối dịch vụ (DDoS).
* Sao Lưu và Phục Hồi Dữ Liệu: \*\*Thiết lập hệ thống sao lưu định kỳ để có khả năng phục hồi dữ liệu sau một sự cố bảo mật hoặc mất dữ liệu.

**3.4 Bảo mật cơ sở dữ liệu web**

* Xác Thực và Quyền Hạn: Sử dụng hệ thống xác thực mạnh mẽ để đảm bảo rằng chỉ có những người dùng được ủy quyền mới có thể truy cập cơ sở dữ liệu. Thiết lập quyền hạn một cách cẩn thận để giới hạn quyền truy cập của người dùng đến các chức năng cụ thể.
* Mã Hóa Dữ Liệu: Mã hóa dữ liệu trong cơ sở dữ liệu để ngăn chặn việc đọc thông tin quan trọng bởi người không được ủy quyền. Mã hóa cũng giúp bảo vệ dữ liệu khi chúng được truyền giữa máy chủ và ứng dụng web.
* Kiểm Soát Người Dùng: Hạn chế số lượng người dùng có quyền truy cập trực tiếp vào cơ sở dữ liệu. Thay vào đó, sử dụng giao diện ứng dụng để thực hiện các thao tác trên cơ sở dữ liệu.
* Kiểm Tra Dữ Liệu Đầu Vào (Input Validation): Kiểm tra và xác thực dữ liệu đầu vào để ngăn chặn các cuộc tấn công như SQL injection. Sử dụng các câu lệnh thực thi thủ công hoặc thư viện chống SQL injection.
* Log và Giám Sát Hoạt Động: Bật chế độ ghi log chi tiết và giám sát nhật ký để theo dõi hoạt động của cơ sở dữ liệu. Điều này có thể giúp phát hiện sớm các hành vi bất thường.
* Sao Lưu Định Kỳ: Thực hiện quy trình sao lưu định kỳ để đảm bảo khả năng phục hồi nhanh chóng sau sự cố, chẳng hạn như mất dữ liệu hoặc tấn công.

**3.5 Bảo mật hệ thống file**

* Quyền Truy Cập (Access Control): Thiết lập quyền truy cập chính xác để đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập, sửa đổi, hoặc xóa dữ liệu trong hệ thống file.
* Mã Hóa Dữ Liệu: Mã hóa tệp tin và dữ liệu để đảm bảo tính bí mật khi chúng đang chuyển hoặc lưu trữ.
* Backup và Phục Hồi: Thực hiện quá trình sao lưu định kỳ để đảm bảo khả năng phục hồi nhanh chóng sau sự cố như mất dữ liệu hoặc tấn công malware.
* Quản lý Phiên Làm Việc: Đảm bảo rằng quản lý phiên làm việc được thiết lập chặt chẽ để ngăn chặn truy cập trái phép vào tệp tin và dữ liệu.
* Log và Giám Sát Hoạt Động: Bật và giám sát log hệ thống để theo dõi các sự kiện quan trọng và phát hiện các hoạt động đáng ngờ.
* Kiểm Soát Người Dùng: Hạn chế số lượng người dùng có quyền cao cấp (như quản trị viên hệ thống) và sử dụng nguyên tắc của tối thiểu quyền để giảm thiểu rủi ro.
* Cấu Hình Firewall: Sử dụng tường lửa để kiểm soát lưu lượng mạng đến và từ hệ thống file.

# TÀI LIỆU THAM KHẢO

[1] Bộ bài giảng môn An toàn Ứng dụng Web và CSDL của ThS Phan Nghĩa Hiệp

[2] Bộ bài giảng môn Lập trình Ứng dụng Web của ThS Nguyễn Trung Hiếu

[3] Hoàng Xuân Dậu, “*Bài giản An toàn Ứng dụng Web và CSDL*”, Hà Nội, 2017