

**TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN**



**TIỂU LUẬN GIỮA KỲ
MÔN LẬP TRÌNH WEB VÀ ỨNG DỤNG
HỌC KỲ 1 NĂM HỌC 2021 - 2022**

WEBSITE SECURITY

Người thực hiện: **NGUYỄN THỊ HƯƠNG GIANG – MSSV: C1900103**
PHẠM MINH TRÍ – MSSV: 52000724

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021

**TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN**



**TIỂU LUẬN GIỮA KỲ
MÔN LẬP TRÌNH WEB VÀ ỨNG DỤNG
HỌC KỲ 1 NĂM HỌC 2021-2022**

WEBSITE SECURITY

Người thực hiện: **NGUYỄN THỊ HƯƠNG GIANG – MSSV: C1900103**
PHẠM MINH TRÍ – MSSV: 52000724

THÀNH PHỐ HỒ CHÍ MINH, NĂM 2021

LỜI CẢM ƠN

Trong thời gian học tập tại trường học kì 1 năm học 2021-2022, chúng tôi được sự dẫn dắt tận tình trong quá trình học tập tài trường của Thầy Mai Văn Mạnh và Thầy Nguyễn Thái Duy, chúng tôi xin chân thành cảm ơn các quý thầy đã tận tình giảng dạy để hôm nay chúng tôi có được thêm kiến thức môn học cũng như kinh nghiệm trong việc viết báo cáo. Do kiến thức còn hạn hẹp nên không tránh khỏi những thiếu sót trong cách hiểu, lỗi trình bày. Chúng tôi rất mong nhận được sự đóng góp ý kiến của quý thầy để bài tiểu luận có được kết quả tốt nhất.

Chúng tôi xin chân thành cảm ơn.

TP. Hồ Chí Minh, ngày 12 tháng 12 năm 2021

Tác giả

(Ký tên và ghi rõ họ tên)



Nguyễn Thị Hương Giang



Phạm Minh Trí

BÀI TIỂU LUẬN ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

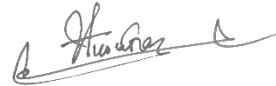
Tôi xin cam đoan đây là sản phẩm tiểu luận riêng của chúng tôi và được sự hướng dẫn của Thầy Mai Văn Mạnh, Thầy Nguyễn Thái Duy. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đề án của mình. Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

TP. Hồ Chí Minh, ngày 12 tháng 12 năm 2021

Tác giả

(ký tên và ghi rõ họ tên)



Nguyễn Thị Hương Giang



Phạm Minh Trí

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

Phần xác nhận của GV hướng dẫn

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

Phần đánh giá của GV chấm bài

Tp. Hồ Chí Minh, ngày tháng năm
(kí và ghi họ tên)

TÓM TẮT

Đề tài này tìm hiểu về những lỗ hổng bảo mật thường gặp đối với một website, cách mà các hacker tấn công các trang web hoặc đánh cắp thông tin người dùng qua những lỗ hổng này và một số phương án khắc phục/ biện pháp phòng tránh và những lời khuyên khi phát triển một website. Các nội dung tìm hiểu về Giao thức HTTPS, SQL Injection, Cross-site Scripting, Directory Traversal sẽ được chúng tôi trình bày chi tiết ở phía dưới và video demo về các lỗ hổng bảo mật.

MỤC LỤC

LỜI CẢM ƠN	i
PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN	iii
TÓM TẮT	iv
MỤC LỤC.....	1
DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ	4
CHƯƠNG 1: MỞ ĐẦU	5
1.1 Giới thiệu đề tài.....	5
1.2 Các nội dung tìm hiểu:	5
CHƯƠNG 2 – GIAO THỨC HTTPS – SQL INJECTION – CROSS-SITE SCRIPTING - DIRECTORY TRAVERSAL	6
1. Tìm hiểu về giao thức HTTPS:	6
1.1 Giao thức HTTP là gì?	6
1.2 Giao thức HTTPS là gì?.....	6
2. SQL Injection	9
2.1 SQL Injection là gì?	9
2.3 Cách giảm thiểu và phòng ngừa SQL Injection:	10
3. Cross-Site Scripting (XSS)	12
3.1 Tấn công Cross-Site Scripting là gì?	12
3.2 Tấn công XSS thực hiện như thế nào?	12
3.3 Một số hình thức phổ biến của tấn công XSS	13
3.3.1 Reflected XSS	13
3.3.2 Stored XSS	14
3.3.3 DOM Based XSS.....	14
3.4 Cách để ngăn chặn sự tấn công của XSS	15
4 DIRECTORY TRAVERSAL	16
4.1 Directory traversal gì?.....	16

4.2 Cách thức hoạt động Directory traversal.....	16
4.3 Ngăn chặn tấn công Directory traversal.....	16
CHƯƠNG 3 – NHỮNG ĐIỀU CẦN LÀM VÀ NÊN TRÁNH KHI PHÁT TRIỂN MỘT TRANG WEB.....	18
1 Những điều cần làm.....	18
1.1 Xác định mục đích thiết kế website.....	18
1.2. Đặt tiêu chí khi thiết kế website.....	18
1.3 Thiết kế website: những việc phải làm quan trọng.....	19
2. Những điều nên tránh.....	19
Tài liệu tham khảo.....	21

DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

CÁC CHỮ VIẾT TẮT

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

SSL: Secure Sockets Layer

www: World Wide Web

SQL: Structured Query Language

TLS: Transport Layer Secure

DB: DataBase

URL: Uniform Resource Locators

DOM: Document Object Model

HTML: Hypertext Markup Language

DHTML: Dynamic Hypertext Markup Language

CSDL: Cơ Sở Dữ Liệu

PR: public relations

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

DANH MỤC HÌNH

Hình 1: dấu hiệu nhận biết một website được bảo mật bằng giao thức https.....8

Hình 2: Ví dụ về form đăng nhập.....9

CHƯƠNG 1: MỞ ĐẦU

1.1 Giới thiệu đề tài

- Bài báo cáo này sẽ trình bày về những lỗ hổng bảo mật thường gặp đối với một website, cách mà các hacker tấn công các trang web hoặc đánh cắp thông tin người dùng qua những lỗ hổng này và một số phương án khắc phục/ biện pháp phòng tránh và những lời khuyên khi phát triển một website.

1.2 Các nội dung tìm hiểu:

- Giao thức HTTPS
- SQL Injection
- Cross-site Scripting
- Directory Traversal
- Những điều cần làm và không nên làm để phát triển một trang web.

CHƯƠNG 2 – GIAO THỨC HTTPS – SQL INJECTION – CROSS-SITE SCRIPTING - DIRECTORY TRAVERSAL

1. Tìm hiểu về giao thức HTTPS:

1.1 Giao thức HTTP là gì?

- HTTP (Hypertext Transfer Protocol) là giao thức truyền tải siêu văn bản. Đây là giao thức tiêu chuẩn cho World Wide Web (www) để truyền tải dữ liệu dưới dạng văn bản, âm thanh, hình ảnh, video từ Web Server tới trình duyệt web của người dùng và ngược lại.

1.2 Giao thức HTTPS là gì?

- HTTPS (Hypertext Transfer Protocol Secure) là giao thức giúp truyền tải siêu văn bản an toàn. HTTPS là một phiên bản của HTTP nhưng được tích hợp thêm chứng chỉ bảo mật SSL (Secure Sockets Layer) hoặc TLS (Transport Layer Secure) giúp HTTPS có tính bảo mật và an toàn cao hơn HTTP. Cho đến nay, SSL và TLS là hai tiêu chuẩn bảo mật hàng đầu cho các website trên thế giới, nó được dùng để mã hóa các thông tin giao tiếp.
- HTTPS là giao thức giúp đảm bảo các yếu tố cơ bản của thông tin, cụ thể:
 - Confidentiality: Sử dụng phương thức mã hóa để đảm bảo các thông điệp trao đổi giữa client và server không bị kẻ thứ 3 đọc được.
 - Integrity: Sử dụng phương thức hashing để cả người dùng và máy chủ đều có thể tin tưởng rằng các thông điệp chuyển giao qua lại là toàn diện và không qua bất kỳ chỉnh sửa nào.
 - Authenticity: Sử dụng chứng chỉ số (digital certificate) để giúp client có thể tin tưởng rằng server/website mà họ đang truy cập thực sự là an toàn.

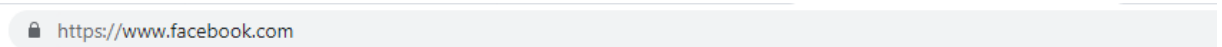
1.3 Vì sao nên sử dụng HTTPS cho website của bạn ?

- HTTPS bảo mật thông tin người dùng:

- Giao thức Https áp dụng phương thức mã hóa để bảo toàn các thông điệp trao đổi giữa máy khách và máy chủ không bị hacker đọc được.
 - Nếu truy cập một trang web không sử dụng giao thức Https người dùng có nguy cơ cao bị hacker chen ngang vào đường kết nối giữa máy chủ và máy khách và đánh cắp thông tin mà người dùng gửi đi (password, văn bản email, thông tin thẻ...) hoặc các thông tin có sẵn từ website.
 - Với Https, người dùng và máy chủ có thể hoàn toàn yên tâm tin tưởng độ bảo mật truyền tải thông điệp đi luôn trong trạng thái nguyên vẹn, không có bất kì sự chỉnh sửa, hay sai lệch nào so với dữ liệu đầu vào.
- Tránh lừa đảo bằng website giả mạo:
- Thực tế cho thấy, bất cứ server nào cũng có thể vào server của bạn để lấy cắp thông tin của người dùng. Nếu bạn dùng giao thức Https thì trình duyệt trên máy khách sẽ được yêu cầu kiểm tra chứng chỉ SSL từ máy chủ trước khi các dữ liệu giữa máy chủ và máy khách được mã hóa để trao đổi. Bên cạnh đó, chứng chỉ TLS/SSL sẽ giúp website bạn được xác minh là chính chủ.
- Giao thức Https tăng uy tín website đối với người dùng:
- Những trình duyệt web hiện nay như Mozilla Firefox, Google Chrome, Apple Safari hay Microsoft Edge sẽ có những cảnh báo đến người dùng về những trang web không được bảo mật.
 - Việc này giúp thông tin của người dùng được bảo vệ khi lướt web, trong đó bao gồm các thông tin từ thẻ ngân hàng, thông tin cá nhân hay những dữ liệu quan trọng khác.
 - Một website không thể hoạt động nếu thiếu người dùng. Vậy nên việc bảo vệ người dùng chính là bảo vệ trang web của bạn. Nếu người dùng cảm thấy

thiếu an toàn khi sử dụng trang web thì bạn sẽ bị mất một lượng lớn user sẵn có của mình.

1.4 Cách nhận biết một website có sử dụng giao thức **Https:** Đối với các website có sử dụng giao thức Https, khi truy cập bạn sẽ thấy ở đầu khung địa chỉ web xuất hiện chiếc ổ khóa cùng dòng Https. Đây được xem là dấu hiệu cho thấy website được bảo mật và chứng thực.



Hình 1.1: dấu hiệu nhận biết một website được bảo mật bằng giao thức https

2. SQL Injection

2.1 SQL Injection là gì?

- SQL injection – còn được gọi là SQLi – sử dụng những lỗ hổng trong các kênh đầu vào (input) của website để nhắm mục tiêu vào cơ sở dữ liệu nằm trong phần phụ trợ của ứng dụng web, nơi lưu giữ những thông tin nhạy cảm và có giá trị nhất. Chúng có thể được kẻ tấn công sử dụng để ăn cắp hoặc xáo trộn dữ liệu, cản trở sự hoạt động của các ứng dụng, và, trong trường hợp xấu nhất, nó có thể chiếm được quyền truy cập quản trị vào máy chủ cơ sở dữ liệu.

2.2 Cách thức website bị tấn công SQL Injection

- Các cuộc tấn công SQL Injection được thực hiện bằng cách gửi lệnh SQL độc hại đến các máy chủ cơ sở dữ liệu thông qua các yêu cầu của người dùng mà website cho phép. Bất kỳ kênh input nào cũng có thể được sử dụng để gửi các lệnh độc hại, bao gồm các thẻ<input>, chuỗi truy vấn (query strings), cookie và tệp tin.
- Ví dụ về tấn công SQL Injection:
 - Giả sử bạn có 1 form đăng nhập như sau:

User Login

Username

Password

☐ Remember login

Invalid username or password

Login

Forgot password? [Click here](#)

Hình 2. Ví dụ về form đăng nhập

- Và đoạn code server xử lý của bạn:

```
if(isset($_POST['username']) && isset($_POST['password'])){
    $sql = "SELECT * FROM tbl_user WHERE username='".
$_POST['username'] . "' AND password = '" . $_POST['password'] . "'";
}
```

- Nếu như người dùng nhập username hoặc password thêm một dấu ‘ hoặc “ thì dòng code sẽ bị lỗi ngay. Hoặc họ có thể sửa thành một câu truy vấn đúng như sau:

```
$sql = "SELECT * FROM tbl_user WHERE username = ' ' OR '1' = '1' and
password = ' ' OR '1' = '1'";
```

2.3 Cách giảm thiểu và phòng ngừa SQL Injection:

- Sử dụng Parameterized Statements (tham số hóa các câu lệnh):

- Ví dụ:

```
$sql = "select * from student where pass == ?";
$stmt = $conn->prepare($sql);
$stmt->bind_param("s",$pw);
```

- Không bao giờ được tin tưởng những input người dùng nhập vào: Dữ liệu luôn phải được xác thực trước khi sử dụng trong các câu lệnh SQL.
- Không cộng chuỗi để tạo SQL: Sử dụng parameter thay vì cộng chuỗi. Nếu dữ liệu truyền vào không hợp pháp, SQL Engine sẽ tự động báo lỗi, ta không cần dùng code để check.
- Mã hóa, kiểm tra dữ liệu nhập vào để tránh trường hợp gây hại cho câu lệnh sql.
- Không hiển thị exception, message lỗi: Hacker dựa vào message lỗi để tìm ra cấu trúc database. Khi có lỗi, ta chỉ hiện thông báo lỗi chứ đừng hiển thị đầy đủ thông tin về lỗi, tránh hacker lợi dụng.

- Phân quyền rõ ràng trong DB: Nếu chỉ truy cập dữ liệu từ một số bảng, hãy tạo một account trong DB, gán quyền truy cập cho account đó chứ đừng dùng account root hay sa. Lúc này, dù hacker có inject được sql cũng không thể đọc dữ liệu từ các bảng chính, sửa hay xóa dữ liệu.

3. Cross-Site Scripting (XSS)

3.1 Tấn công Cross-Site Scripting là gì?

- Tấn công Cross-Site Scripting hay còn được viết tắt XSS là là một kỹ thuật tấn công bằng cách chèn vào các website động (ASP, PHP, CGI, JSP ...) những thẻ HTML hay những đoạn mã script nguy hiểm có khả năng đánh cắp hay thiết lập được những thông tin quan trọng như cookies, mật khẩu, username.... Trong đó, những đoạn mã nguy hiểm được chèn vào hầu hết được viết bằng các Client-Site Script như JavaScript, JScript, DHTML và cũng có thể là cả các thẻ HTML.
- Phương pháp này không nhằm vào máy chủ hệ thống mà chủ yếu tấn công trên chính máy người sử dụng. Hacker sẽ lợi dụng sự kiểm tra lỏng lẻo từ ứng dụng và hiểu biết hạn chế của người dùng cũng như biết đánh vào sự tò mò của họ dẫn đến người dùng bị mất thông tin một cách dễ dàng.
- Thông thường hacker lợi dụng địa chỉ URL để đưa ra những liên kết là tác nhân kích hoạt những đoạn chương trình được viết bằng ngôn ngữ máy khách như VBScript, JavaScript...được thực thi trên chính trình duyệt của nạn nhân.

3.2 Tấn công XSS thực hiện như thế nào?

- Mục đích chính của cuộc tấn công này là ăn cắp dữ liệu nhận dạng của người dùng như: cookies, session tokens và các thông tin khác.
- Các hacker tấn công XSS thông qua việc gửi, chèn các lệnh, script độc hại gây nguy hiểm và những mã độc này thường được viết dưới dạng ngôn ngữ lập trình như là HTML, Javascript, Flash..., Cách tấn công XSS có thể được thực hiện theo nhiều cách khác nhau và nó phụ thuộc vào các loại tấn công của XSS. Theo đó, những mã độc có thể được phản chiếu trên các trình duyệt hệ thống hoặc được lưu trữ ở các CSDL. Mã độc này sẽ được chạy khi người dùng gọi các chức năng thích hợp. Nguyên nhân chính xảy ra các loại tấn công này chính là xác thực đầu vào của người dùng không phù hợp, các dữ liệu độc hại sẽ bắt đầu có thể xâm nhập. Các mã độc có thể nhận 1 script đồng thời chèn vào các mã nguồn của website. Khi đó,

trình duyệt thiết bị của người dùng sẽ không thể nào biết được mã thực thi có phải mã độc hay không. Cũng chính vì vậy mà mã độc trong sự tấn công của XSS có thể được thực thi ngay trên trình duyệt hoặc bất kỳ hình thức giả nào hiển thị lên mà người dùng không biết.

– Một số hình thức phổ biến của tấn công XSS:

- XSS có thể xảy ra trên tập lệnh độc hại được thực hiện ở phía client.
- Trang web hoặc form giả mạo được hiển thị cho người dùng (nơi nạn nhân nhập thông tin đăng nhập hoặc nhấp vào liên kết độc hại).
- Trên các trang web có quảng cáo được hiển thị.
- Email độc hại được gửi đến nạn nhân. Tấn công xảy ra khi tin tặc tìm kiếm những lỗ hổng trên website và gửi nó làm đầu vào độc hại. Tập lệnh độc hại được thêm vào mã lệnh và sau đó được gửi dưới dạng đầu ra cho người dùng cuối cùng.

3.3 Một số hình thức phổ biến của tấn công XSS

Hiện nay, XSS có 3 loại tấn công phổ biến nhất đó là Reflected XSS, Stored XSS và DOM Based XSS.

3.3.1 Reflected XSS: Đây là một trong những cách được sử dụng phổ biến nhất để chiếm session của người dùng. Chi tiết về quá trình tấn công này bao gồm:

- Người dùng sẽ tiến hành đăng nhập vào trang web và giả sử như nó đã được gán session.
- Bằng một cách nào đó, các hacker sẽ gửi đến cho người dùng một url nhất định
- Tiếp đó người dùng sẽ truy cập vào url đã nhận được và server sẽ phản hồi về cho người dùng kèm theo các dữ liệu có trong đoạn javascript của hacker.

- Trình duyệt của người dùng sẽ nhận phản hồi, đồng thời thực thi các đoạn javascript. Các dòng lệnh trên bản chất thực hiện request đến site của các hacker cùng với tham số chính là cookies của người dùng.
- Cuối cùng, từ phía site của mình, các hacker sẽ có thể nắm bắt được các nội dung mà mình request được trên, xem như các session của người dùng đã bị chiếm. Và lúc này hacker có thể giả mạo với tư cách là người dùng, thực hiện các quyền truy cập vào website mà người dùng đang có.

3.3.2 Stored XSS: Loại tấn công này sẽ hướng tới nhiều người dùng. Lỗi này sẽ xảy ra trong trường hợp ứng dụng web không được kiểm tra kỹ lưỡng các dữ liệu đầu vào trước khi thực hiện lưu vào cơ sở dữ liệu. Ví dụ như đối với các form góp ý hay các comment... có trên website thì với kỹ thuật này, các hacker có thể không khai thác được trực tiếp mã sẽ cần ít nhất 2 bước sau:

- Bước 1: các hacker sẽ thông qua điểm đầu vào như là input, form hay textarea,.. không được kiểm tra kỹ để thực hiện chèn vào các cơ sở dữ liệu những đoạn mã nguy hiểm, độc hại.
- Bước 2: Khi người dùng thực hiện truy cập vào các ứng dụng web, thực hiện các thao tác có liên quan đến cơ sở dữ liệu được lưu này, các đoạn mã của hacker sẽ được thực thi trên trình duyệt của người dùng đang sử dụng.

3.3.3 DOM Based XSS: là kỹ thuật khai thác XSS dựa trên cơ sở thay đổi các cấu trúc DOM của tài liệu mà cụ thể ở đây chính là HTML. Ví dụ như một website có url nhất định để đăng ký và người dùng khi truy cập đến sẽ thấy form rất bình thường, quen thuộc. Chắc chắn khi đó người dùng sẽ không có một chút nghi ngờ gì mà sẽ lựa chọn điền các thông tin theo yêu cầu. Lúc này script sẽ ngay lập tức thực thi và cơ sở dữ liệu, thông tin của hệ thống đã bị hack. Chỉ thông qua việc áp dụng DOM Based XSS, các hacker đã có thể xâm nhập và có được thông tin họ cần.

3.4 Cách để ngăn chặn sự tấn công của XSS

- Quá trình ngăn ngừa sự tấn công xâm nhập của XSS sẽ được thực hiện từ việc xác thực đầu vào. Toàn bộ mọi thứ được nhập bởi người dùng sẽ cần phải đảm bảo xác thực chính xác vì đầu vào sẽ ảnh hưởng đến đầu ra. Việc xác thực dữ liệu này có thể được đặt tên làm cơ sở và đảm bảo về tính bảo mật của hệ thống dữ liệu đó.
- Lọc đầu vào là một cách để ngăn chặn sự tấn công XSS. Tức là sẽ thực hiện tìm kiếm các từ khóa nguy hiểm ở mục nhập của người dùng và sẽ xóa chúng hay thực hiện thao tác thay thế chúng bằng chuỗi trống. Các từ khóa đó có thể sẽ là `<script></script>` hoặc là lệnh javascript, đánh dấu HTML... Một số cách thực hiện lọc đầu vào như:
 - Thực hiện bởi các lập trình viên đã viết mã ở phía server
 - Thông qua thư viện ngôn ngữ lập trình thích hợp mà người dùng đang sử dụng
- Ngoài ra, để phòng ngừa sự tấn công XSS thì cũng có thể sử dụng các ký tự Escape và trong thực tế thì các ký tự này đang được thay đổi bằng các mã đặc biệt.

4 Directory Traversal

4.1 Directory traversal gì?

Directory traversal(hay còn gọi là Path traversal) là một lỗ hổng web cho phép kẻ tấn công đọc các file không mong muốn trên server. Nó dẫn đến việc bị lộ thông tin nhạy cảm của ứng dụng như thông tin đăng nhập , một số file hoặc thư mục của hệ điều hành. Trong một số trường hợp cũng có thể ghi vào các files trên server, cho phép kẻ tấn công có thể thay đổi dữ liệu hay thậm chí là chiếm quyền điều khiển server.

4.2 Cách thức hoạt động Directory traversal

- Một ví dụ về việc lưu trữ ảnh trong hệ thống:
 1. Giả sử những file ảnh được dev lưu trong thư mục `/var/www/html/blog/public/img/`
 2. Khi truy cập file `avatar.jpg` trên thư mục này dev có thể để link là `GET photo/file?name=avata.jpg`. Lúc này webserver sẽ truy cập vào file ở đường dẫn `/var/www/html/blog/public/img/avatar.jpg` và trả về cho người dùng.
 3. Nhưng thay vì việc truyền file name là `avatar.jpg` hacker có thể truyền tên file là `../../../../etc/password`. Lúc này webserver sẽ truy cập và trả về file ở đường dẫn `/var/www/html/blog/public/img/../../../../etc/password`. Đường dẫn này tương đương với `/etc/pasword` nên webserver sẽ trả về file hệ thống cho chúng ta.
 4. Ví dụ như đối với windown server thì chúng ta có thể dùng cả `../` và `..\`

4.3 Cách kiểm tra lỗ hổng Directory traversal: Cách để kiểm tra liệu trang web có tồn tại lỗ hổng directory traversal là sử dụng Webvulnerability web Scanner. Nó sẽ giúp quét toàn bộ trang web và tự động kiểm tra lỗ hổng sau đó báo cáo và chúng ta sẽ dễ dàng để sửa chữa lỗ hổng.

4.4 Ngăn chặn tấn công Directory traversal

- Nên validate input của người dùng trước khi xử lý nó

- Sử dụng whitelist cho những giá trị được cho phép
- Tên file nên là những ký tự số hoặc chữ, không nên chứa các ký tự đặc biệt

CHƯƠNG 3 – NHỮNG ĐIỀU CẦN LÀM VÀ NÊN TRÁNH KHI PHÁT TRIỂN MỘT TRANG WEB

1. Những điều cần làm

1.1 Xác định mục đích thiết kế website

Thiết kế website cũng chính là một hoạt động đầu tư tài chính. Website tất nhiên phải đảm bảo sẽ đem lại cho bạn những giá trị nhất định thì bạn mới đầu tư vào nó. Thường thì Website được sử dụng với nhiều mục đích rất linh hoạt như:

Giới thiệu, quảng bá hình ảnh của doanh nghiệp

Quảng bá, PR cho sản phẩm mới

Là kênh kinh doanh sản phẩm chủ đạo của doanh nghiệp

Việc xác định rõ mục đích sẽ giúp bạn khoanh vùng được lượng khách hàng tiềm năng mà bạn nhắm đến là ai. Từ đó, có sự chuẩn bị kỹ càng và đầy đủ nhất để hiện thực hóa ý tưởng của mình.

1.2. Đặt tiêu chí khi thiết kế website

Sự bùng nổ của mạng xã hội khiến việc cạnh tranh giữa các thương hiệu vô cùng khốc liệt, xu hướng kinh doanh online được hầu hết các doanh nghiệp lựa chọn. Vì vậy, việc nghiên cứu những điều cần biết về website đối thủ cạnh tranh và khách hàng tiềm năng để đề ra những tiêu chí mà website phải đạt được. Hãy chi tiết hóa những tiêu chí này một cách cụ thể, ví dụ:

- Giao diện website phải đẹp mắt, ấn tượng, có điểm nhấn, thu hút người truy cập.
- Nội dung phải đầy đủ, hấp dẫn, đúng trọng tâm cần quảng bá
- Web phải đảm bảo khả năng truy xuất cao, ổn định và thân thiện với công cụ tìm kiếm nhưng đảm bảo tính bảo mật cao
- Dễ dàng quản trị, cập nhật nội dung, thuận tiện cho khách hàng tra cứu thông tin và mua sắm...

1.3 Thiết kế website: những việc phải làm quan trọng

- Về giao diện: đưa ra màu sắc chủ đạo gắn liền với thương hiệu (phù hợp với logo và ngành nghề của doanh nghiệp, tương đồng với bộ nhận diện thương hiệu).
- Về nội dung: Nội dung bạn muốn truyền đạt đến khách hàng của mình là gì?
- Soạn thảo tài liệu quảng bá liên quan đến sản phẩm/doanh nghiệp của bạn
- Về hệ thống tính năng của web: Phải đầy đủ tính năng, tiện ích. Bạn nên nhớ nội dung website càng đặc sắc, hệ thống tính năng càng đơn giản, nhiều tiện ích, thực sự mang lại giá trị cho người dùng thì tỷ lệ thành công của web càng cao.
- Lựa chọn đối tác xây dựng website uy tín: Một website hoàn thiện không chỉ phải đạt được các yêu cầu về kỹ thuật, thẩm mỹ mà còn phải thực sự hữu ích, chi phí hợp lý và mang lại giá trị cho doanh nghiệp
- Về bảo mật: Một website cần được bảo mật kỹ để tránh các lỗ hổng dẫn đến việc hacker dễ dàng tấn công và đánh cắp thông tin dữ liệu, điều này rất nguy hiểm cho một trang web.

2. Những điều nên tránh

- Lựa chọn màu không hài hòa, quá rắc rối: Một trang web không nên nhiều hơn 3 màu và chữ trong bài viết nên là màu có tính tương phản cao với
- Thanh navigation rắc rối: Trang web bố trí menu không hiểu quả sẽ không gây được hiệu ứng cho người xem. Nên bố trí menu:
 - Phân dạng menu: khi thiết lập dự án thiết kế web bạn cần phân dạng các menu thông tin theo nhóm tương đồng
 - Vị trí đặt menu: Bên trên, bên trái, bên phải,... Sao cho hài hòa với các thông tin dự án thiết kế web
 - Đồng nhất font : trong thiết kế web quy ước kiểu font, kích cỡ font thông nhất như một cuốn sách xuyên suốt.

- Nổi bật tiêu đề: Tiêu đề nội dung trên trang web bố trí nổi bật hơn về kích cỡ, kiểu,... nhưng mang tính thống nhất
- Font chữ không đồng nhất, mỗi phần 1 kiểu: Việc này để tránh cho người dùng không bị loạn khi theo dõi website, họ sẽ khó định hình và mất nhiều thời gian khi mà chưa tìm được thông tin mình muốn tìm kiếm.
- Nội dung hiển thị quá dài và lộn xộn
- Tốc độ tải trang chậm
- Không có META tag
- Chọn độ phân giải không phù hợp
- Không đầu tư vào hiển thị trên thiết bị di động

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. CyStack (2019), Giao thức HTTP và HTTPS là gì? Tại sao nên sử dụng HTTPS? , access: <https://cystack.net/vi/blog/http-va-https-la-gi>
2. BaoBinhDinh (2021), Bảo vệ an toàn thông tin bằng giao thức https,access: <https://baobinhdinh.vn/viewer.aspx?macm=23&macmp=23&mabb=221253>
3. HelpEx (2017), Path Traversal là gì? Access: <https://helpex.vn/article/path-traversal-la-gi-60c733ad773a21c44f3d2d72>
4. Quantrimang (2021), Kiến thức cơ bản về Cross-Site Scripting (XSS): lỗ hổng thú vị mới của hacker
Access: <https://quantrimang.com/cross-site-scripting-lo-hong-thu-vi-moi-cua-nhung-ke-tan-cong-32105>
5. Quantrimang (2021), SQL Injection là gì? Cách phòng chống tấn công SQL Injection, access: <https://quantrimang.com/tan-cong-kieu-sql-injection-va-cac-phong-chong-trong-asp-net-34905>
6. Phạm Huy Hoàng (2018), Hack cùng Code Đạo - Kỳ 1: SQL Injection, access: <https://www.youtube.com/watch?v=6i1CWIaTH60>
7. Phạm Huy Hoàng (2018), Hack cùng Code Đạo - Kỳ 2: XSS - Cross-Site Scripting, access: https://www.youtube.com/watch?v=3_BfecB1Dqk&t=361s
- 8.NhanHoa.com (2016), SAI LẦM CẦN TRÁNH KHI THIẾT KẾ WEBSITE
<https://nhanhoa.com/tin-tuc/sai-lam-can-tranh-khi-thiet-ke-website.html>
9. Tailieu123.org (2021), Tìm hiểu về tấn công mạng Directory Traversal, access: <https://www.tailieu123.org/tim-hieu-ve-tan-cong-mang-directory-traversal.html>

Tiếng Anh

10. PortSwigger (2021), What is SQL injection? ,access:
<https://portswigger.net/web-security/sql-injection>
11. VERACODE (2021), Directory traversal, access:
<https://www.veracode.com/security/directory-traversal>
12. OWASP (2021), Cross Site Scripting (XSS), access:
<https://owasp.org/www-community/attacks/xss/>
- 13.Hacksplaining (2021), security training for developers, access:
<https://www.hacksplaining.com/>