**Câu 1:**

**Tấn công SQL Injection**

**SQL Injection** là một kỹ thuật tấn công phổ biến, cho phép kẻ tấn công tiêm trực tiếp các đoạn mã SQL vào các trường nhập liệu của website để thao túng cơ sở dữ liệu. Điều này có thể dẫn đến nhiều hậu quả nghiêm trọng như:

* **Truy cập trái phép:** Kẻ tấn công có thể truy cập, xem hoặc sửa đổi dữ liệu nhạy cảm.
* **Tiết lộ thông tin:** Thông tin cá nhân, mật khẩu của người dùng có thể bị đánh cắp.
* **Phủ định dịch vụ:** Tấn công có thể làm quá tải máy chủ hoặc làm hỏng cơ sở dữ liệu.
* **Tiến hành các cuộc tấn công khác:** SQL Injection có thể được sử dụng như một bước đệm để thực hiện các cuộc tấn công phức tạp hơn.

**Cách thức hoạt động:**

1. **Nhập liệu:** Kẻ tấn công nhập vào các đoạn mã SQL độc hại vào các trường nhập liệu (ví dụ: username, password).
2. **Truy vấn:** Ứng dụng web sử dụng trực tiếp dữ liệu nhập vào để xây dựng câu truy vấn SQL, mà không kiểm tra hoặc lọc dữ liệu.
3. **Thực thi:** Câu truy vấn SQL độc hại được gửi đến cơ sở dữ liệu và được thực thi, dẫn đến các hậu quả đã nêu trên.

**Tấn công XSS (Cross-Site Scripting)**

**XSS** là một kỹ thuật tấn công cho phép kẻ tấn công chèn các đoạn mã độc (thường là JavaScript) vào các trang web, khiến cho các đoạn mã này được thực thi trong trình duyệt của người dùng khi họ truy cập vào trang web đó.

**Cách thức hoạt động:**

1. **Tiêm mã:** Kẻ tấn công tiêm các đoạn mã độc vào các trường nhập liệu của website hoặc lợi dụng các lỗ hổng khác trong ứng dụng.
2. **Lưu trữ:** Mã độc được lưu trữ trên máy chủ và được gửi đến trình duyệt của người dùng khi họ truy cập trang web.
3. **Thực thi:** Trình duyệt của người dùng sẽ thực thi mã độc, cho phép kẻ tấn công thực hiện các hành động như:
   * **Trộm cắp cookie:** Lấy cắp thông tin đăng nhập của người dùng.
   * **Thay đổi nội dung trang web:** Thay đổi giao diện hoặc nội dung của trang web.
   * **Chuyển hướng người dùng:** Chuyển hướng người dùng đến các trang web độc hại.

**Biện pháp phòng tránh**

**Đối với SQL Injection:**

* **Sử dụng các câu lệnh chuẩn bị (prepared statements):** Cách này giúp ngăn chặn việc trực tiếp chèn dữ liệu vào câu truy vấn, mà thay vào đó, dữ liệu sẽ được truyền dưới dạng tham số.
* **Lọc và kiểm tra dữ liệu đầu vào:** Kiểm tra và lọc tất cả các dữ liệu đầu vào từ người dùng để loại bỏ các ký tự đặc biệt và các đoạn mã SQL độc hại.
* **Sử dụng các thư viện ORM (Object-Relational Mapping):** ORM giúp tự động hóa việc tạo các câu truy vấn SQL, giảm thiểu nguy cơ viết sai câu lệnh.
* **Cập nhật thường xuyên các hệ thống:** Cập nhật các hệ thống, framework và thư viện để vá các lỗ hổng bảo mật.

**Đối với XSS:**

* **Mã hóa đầu ra:** Mã hóa các dữ liệu đầu ra trước khi hiển thị trên trang web để ngăn chặn việc thực thi các đoạn mã độc.
* **Sử dụng các hàm lọc:** Sử dụng các hàm lọc để loại bỏ các thẻ HTML và các ký tự đặc biệt.
* **Sử dụng Content Security Policy (CSP):** CSP giúp hạn chế các nguồn mà trình duyệt có thể tải script từ đó.
* **Kiểm tra và lọc dữ liệu đầu vào:** Tương tự như SQL Injection, cần kiểm tra và lọc tất cả các dữ liệu đầu vào từ người dùng.

**Câu 2:**

**Khi website bị lỗi giao diện: Nguyên nhân và cách giải quyết**

**Hiểu rõ về lỗi giao diện**

Khi một website không hiển thị đúng trên các thiết bị khác nhau (điện thoại, máy tính bảng, máy tính để bàn), điều đó thường được gọi là lỗi giao diện hoặc lỗi responsive design. Lỗi này khiến trải nghiệm người dùng trở nên kém đi, ảnh hưởng đến hiệu quả của website.

**Nguyên nhân gây ra lỗi giao diện:**

* **CSS không tương thích:** Các thuộc tính CSS được sử dụng có thể không hoạt động đúng trên các trình duyệt hoặc kích thước màn hình khác nhau.
* **Media query không chính xác:** Các media query dùng để điều chỉnh giao diện cho các thiết bị khác nhau có thể bị viết sai hoặc không đầy đủ.
* **HTML cấu trúc kém:** Cấu trúc HTML không hợp lý, thiếu các thẻ cần thiết hoặc sử dụng sai các thẻ có thể gây ra lỗi hiển thị.
* **JavaScript lỗi:** Các đoạn mã JavaScript có thể gây xung đột hoặc không tương thích với các trình duyệt khác nhau.
* **Ảnh hưởng của plugin hoặc theme:** Các plugin hoặc theme được cài đặt có thể gây ra xung đột với các file CSS hoặc JavaScript khác.

**Cách giải quyết lỗi giao diện:**

1. **Kiểm tra giao diện trên nhiều thiết bị và trình duyệt:**
   * Sử dụng các công cụ phát triển của trình duyệt (Chrome DevTools, Firefox Developer Tools) để kiểm tra mã nguồn và giao diện trên các thiết bị khác nhau.
   * Sử dụng các công cụ mô phỏng thiết bị (emulator) để kiểm tra giao diện trên nhiều kích thước màn hình khác nhau.
   * Sử dụng các dịch vụ kiểm tra responsive online.
2. **Sử dụng các công cụ kiểm tra lỗi:**
   * **Validator W3C:** Kiểm tra xem HTML và CSS có tuân thủ các tiêu chuẩn W3C không.
   * **Linter:** Kiểm tra lỗi cú pháp trong CSS và JavaScript.
3. **Sửa lỗi CSS:**
   * **Kiểm tra các thuộc tính CSS:** Đảm bảo các thuộc tính như width, height, margin, padding được sử dụng đúng và tương thích với các thiết bị khác nhau.
   * **Sử dụng các đơn vị đo tương đối:** Sử dụng các đơn vị đo như em, rem, % thay vì px để giao diện tự động điều chỉnh theo kích thước màn hình.
   * **Kiểm tra các media query:** Đảm bảo các media query được viết đúng và bao phủ tất cả các kích thước màn hình cần thiết.
4. **Sửa lỗi HTML:**
   * **Kiểm tra cấu trúc HTML:** Đảm bảo cấu trúc HTML rõ ràng, sử dụng các thẻ đúng cách và không có lỗi cú pháp.
   * **Sử dụng các thẻ semantic:** Sử dụng các thẻ semantic như header, nav, section, article để giúp trình duyệt hiểu rõ hơn về cấu trúc của trang web.
5. **Sửa lỗi JavaScript:**
   * **Kiểm tra các đoạn mã JavaScript:** Đảm bảo các đoạn mã JavaScript không gây xung đột với các file CSS hoặc các đoạn mã JavaScript khác.
   * **Sử dụng các thư viện JavaScript:** Sử dụng các thư viện JavaScript như jQuery để đơn giản hóa việc viết mã và xử lý các sự kiện.
6. **Kiểm tra plugin và theme:**
   * **Tắt các plugin không cần thiết:** Tắt tạm thời các plugin để xem liệu chúng có gây ra lỗi không.
   * **Cập nhật plugin và theme:** Cập nhật các plugin và theme lên phiên bản mới nhất để khắc phục các lỗi đã biết.

**Câu 3:**

**Nguyên nhân dẫn đến lỗi 404 hoặc 500 trên trang chủ**

Lỗi 404 và 500 là hai lỗi thường gặp khi truy cập website, đặc biệt là trang chủ. Chúng thường xuất hiện do một số nguyên nhân sau đây:

**Lỗi 404 Not Found (Không tìm thấy trang)**

* **Đường dẫn sai:** URL của trang chủ đã bị thay đổi hoặc gõ sai.
* **Tệp tin bị xóa:** Tệp tin HTML của trang chủ đã bị xóa hoặc di chuyển.
* **Cấu hình máy chủ sai:** Máy chủ không thể tìm thấy tệp tin trang chủ do cấu hình sai.
* **Vấn đề với .htaccess:** Tệp .htaccess có thể bị cấu hình sai hoặc gây xung đột với các quy tắc khác.

**Lỗi 500 Internal Server Error (Lỗi máy chủ nội bộ)**

* **Lỗi mã nguồn:** Có lỗi trong mã PHP, Python hoặc các ngôn ngữ lập trình khác sử dụng để xây dựng trang web.
* **Vấn đề với cơ sở dữ liệu:** Lỗi kết nối cơ sở dữ liệu, lỗi truy vấn hoặc bảng bị hỏng.
* **Giới hạn tài nguyên:** Máy chủ hết dung lượng đĩa, bộ nhớ hoặc các tài nguyên khác.
* **Xung đột plugin/theme:** Plugin hoặc theme của WordPress hoặc các hệ thống quản trị nội dung khác gây xung đột.
* **Cấu hình máy chủ sai:** Cấu hình PHP, Apache hoặc Nginx có vấn đề.

**Câu 4:**

**Dedicated server**

*Ưu điểm:*

* Bên thuê khá linh động chọn các phần cứng server.
* Khả năng lưu trữ lớn, do dùng được toàn bộ đĩa cứng.
* Tốc độ xử lý nhanh, và an toàn do không chia sẻ tài nguyên server với ai.
* Bên thuê có toàn quyền quản trị server như cài đặt hệ điều hành, các phần mềm..

*Nhược điểm:*

* Chi phí cao do thuê riêng server.
* Cần phải có người có kỹ năng quản trị và bảo trì server.
* Tự chịu trách nhiệm các dữ liệu của mình (backup, restore…)
* Thay đổi tài nguyên (CPU, RAM, đĩa…): không linh động, không thể thực hiện chỉ bằng click chuột, phải dừng server và thực hiện thủ công.

**VPS Hosting**

*Ưu điểm:*

* Tiết kiệm tiền đầu tư phần cứng, tiền điện vận hành máy chủ, không gian lắp đặt…Vì nhiều VPS cùng chạy trên 1 máy vật lý.
* Thay đổi tài nguyên máy chủ rất linh động, dễ dàng bằng cách click chuột. Ví dụ tăng giảm CPU, tăng giảm RAM, tăng giảm đĩa cứng …
* Do nhiều VPS nằm trong 1 máy chủ nên việc kiểm tra,

vận hành, quản trị, dễ dàng hơn.

*Nhược điểm:*

* Hoạt động của VPS bị phụ thuộc bởi hoạt động và độ ổn định của máy chủ vật lý.
* Việc sử dụng chung máy chủ vật lý khiến các VPS bị phụ thuộc, ảnh hưởng lẫn nhau.
* Tài nguyên (RAM, CPU, HDD) có thể thay đổi dễ dàng nhưng bị giới hạn bởi khả năng server vật lý.
* Tốc độ thực thi, năng suất hoạt động của VPS không đạt hiệu quả như dedicated server.

**Colocation**

*Ưu điểm:*

* Bên thuê tự chủ hoàn toàn việc chọn phần cứng server theo khả

năng tài chính và nhu cầu của mình.

* Bên thuê không cần đầu tư hạ tầng như tủ rack, máy lạnh, hệ thống điện, chống sét, người bảo vệ server 24/7.
* Bên thuê được tự chủ hoàn toàn quyền quản trị và bảo trì server.
* Tốc độ thực thi cao do không chia sẻ tài nguyên.

Server được đặt nơi an toàn, tốc độ mạng cao.

*Nhược điểm:*

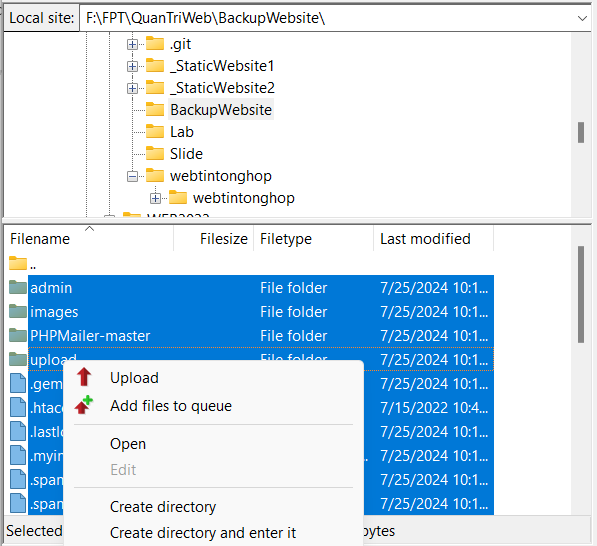
* Bên thuê phải có tài chính để đầu tư server (khá cao)
* Phải có nhân viên đủ trình độ mạng và bảo mật để quản trị server.
* Tự chịu trách nhiệm vụ dữ liệu, bảo mật server.
* Thay đổi tài nguyên máy chủ không được linh động

**Câu 5:**

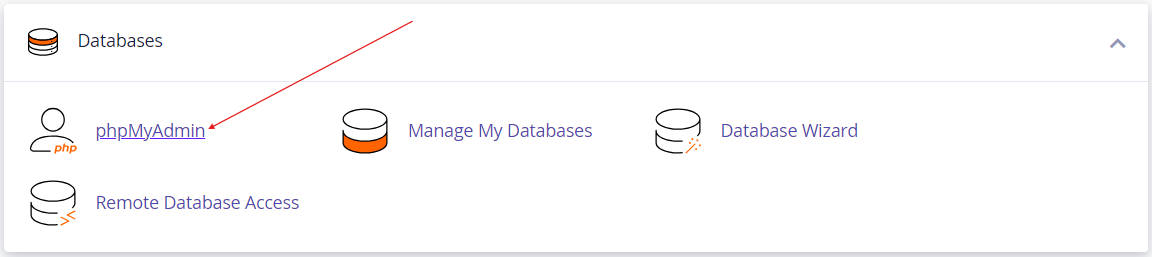
1.Restore file

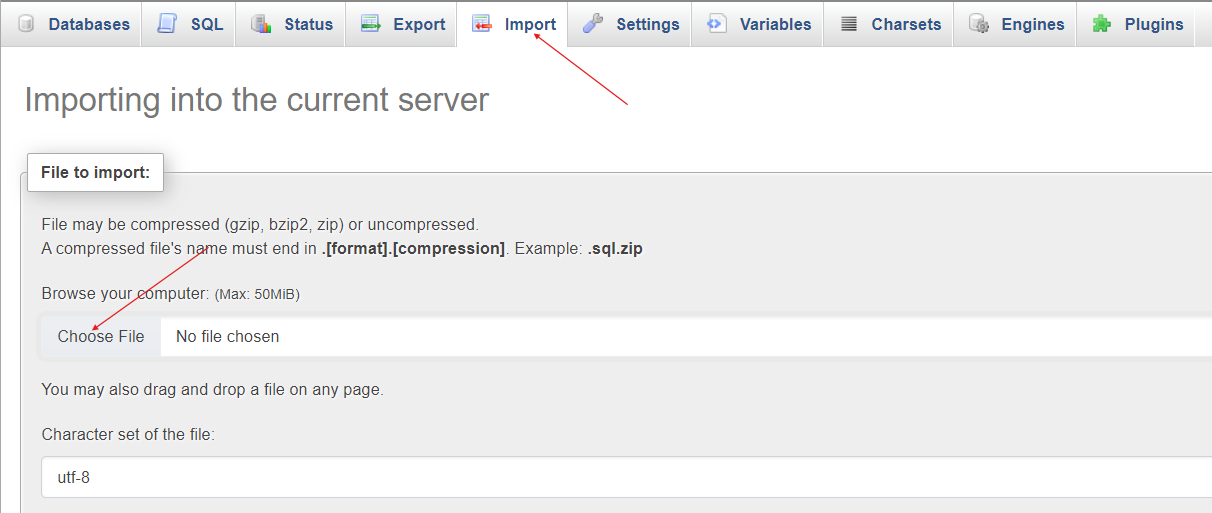
- Bước 1: Mở Filezilla kết nối đến Hosting-> Vào folder public\_html

- Bước 2: Trỏ đến thư mục chứa website Backup-> Upload



2. Restore Database

- Bước 1: Chọn phpMyAdmin

* Bước 2: Import-> Choose file
* Bước 3: Tìm đến folder chứa website Backup -> chọn db đã backup