**BẢN BÁO CÁO VỀ LỖ HỔNG TỒN TẠI TRÊN WEBSITE**

1. Các lỗ hổng:
   1. SQLi In-band:

* Chức năng search của website
  1. Stored XSS:
* Chức năng đăng bài viết của website
  1. Reflected XSS:
* Chức năng search của website
  1. Vertical access controls:
* Chức năng sửa xóa người dùng dành cho admin
  1. Horizontal access controls:
* Chức năng xóa bài đăng của người dùng khác
  1. CSRF:
* Chức năng đổi email của người dùng

1. Nguyên nhân (root-cause):
   1. SQLi In-band:

* Cho phép người dùng nhập truy xuất dữ liệu và xử lí câu truy vấn trực tiếp. Điều này cho phép các truy vấn độc hại có thể được thực thi trong quá trình truy vấn dữ liệu.
  1. Stored XSS:
* Trang web lưu trữ trực tiếp dữ liệu từ nguồn không đáng tin cậy và phản hồi lại một cách không an toàn khi truy xuất lại dữ liệu
  1. Reflected XSS:
* Trang web không xử lí kĩ tham số truyền vào và trả về phản hồi ngay lập tức
  1. Access controls:
* Trang web không có biện pháp bảo vệ các chức năng đặc biệt
* Không kiểm soát các chức năng truy cập
  1. CSRF:
* Không có CSRF token để xác thực người dùng
* Không có referrer để kiểm tra HTTP được gửi đến trang web đến từ đâu

1. Tác động (impact):
   1. SQLi In-band:

* Hacker có thể truy xuất những dữ liệu và thông tin cá nhân
* Sửa xóa dữ liệu
  1. XSS:
* Có thể bị đánh cắp thông tin
* Hacker có thể có toàn quyền kiểm soát nếu nạn nhân có đặc quyền cao trong ứng dụng web
* Khi nạn nhân click vào đường link được gửi, trình duyệt sẽ phản hồi trang web và thực thi các đoạn script kèm theo, sau đó gửi về cho hacker những thông tin của nạn nhân.
  1. Access controls:
* Hacker có thể có quyền can thiệp vào nhiều chức năng như sửa xóa người dùng, lấy cắp thông tin,…
  1. CSRF:
* Nạn nhân có thể bị lừa để hacker thực hiện những thủ đoạn không mong muốn

1. Cách khắc phục(fix, patch) lỗ hổng:
   1. SQLi In-band:

* Tham số hóa các câu truy vấn (prepare\_statement)
* Lọc những kí tự đặc biệt
  1. XSS:
* Lọc những kí tự đặc biệt khi người dùng nhập vào
* Mã hóa dữ liệu đầu ra khi phản hồi lại cho người dùng khác
* Chỉ chấp nhận những dữ liệu hợp lệ
* Không nhận những dữ liệu hỏng bên ngoài
* Tạo ra danh sách thẻ HTML được sử dụng
* Lọc dấu nháy đơn và nháy kép
* Xóa hoặc encode cho các kí tự “<” hay “>”
  1. Access controls:
* Không che giấu để hạn chế việc truy cập trái phép
* Mặc định từ chối truy cập
  1. CSRF:
* Sử dụng csrf\_token
* Sử dụng HTTP referer để xác định địa chỉ của web liên kết với trang được yêu cầu có hợp lệ hay không
* Theo dõi session của người dùng