Hồ Minh Thiện HTTT2311010

**Bảng Báo Cáo Đánh Giá Lỗ Hổng**

| STT | Điểm yếu bảo mật | Mô tả ngắn gọn | Mức độ nghiêm trọng | Công cụ sử dụng |
| --- | --- | --- | --- | --- |
| 1 | SQL Injection | Chèn lệnh SQL độc hại để truy xuất/sửa đổi/xóa dữ liệu CSDL, hoặc kiểm soát máy chủ CSDL. | Critical | SQLMap, OWASP ZAP, Burp Suite, Acunetix, Nessus |
| 2 | Local File Inclusion (LFI)/Path Traversal | Đọc các tệp nhạy cảm trên hệ thống hoặc thực thi mã độc bằng cách thao túng đường dẫn tệp. | High | OWASP ZAP, Burp Suite, Acunetix, Nessus |
| 3 | Server Side Request Forgery (SSRF) | Khiến máy chủ gửi yêu cầu đến tài nguyên nội bộ hoặc bên ngoài, dẫn đến tiết lộ thông tin. | High | OWASP ZAP, Burp Suite, Acunetix, Netsparker/Invicti |
| 4 | Default/Weak Credentials | Sử dụng thông tin đăng nhập mặc định hoặc mật khẩu yếu/dễ đoán để truy cập trái phép. | High | Nmap, Hydra, Metasploit, Nessus, OpenVAS |
| 5 | Insecure Direct Object References (IDOR) | Thay đổi tham chiếu ID để truy cập hoặc thao tác dữ liệu của người dùng khác. | High | OWASP ZAP, Burp Suite, Acunetix |
| 6 | Missing Security Headers | Thiếu các HTTP Security Headers thiết yếu, tăng rủi ro XSS, Clickjacking, tấn công hạ cấp kết nối. | Medium | OWASP ZAP, Burp Suite, SecurityHeaders.com, Nessus, Acunetix |
| 7 | Cross-Site Scripting (XSS) (Reflected) | Chèn mã độc vào trang web, được thực thi trong trình duyệt người dùng, có thể đánh cắp cookie/chiếm quyền phiên. | Medium | OWASP ZAP, Burp Suite, Acunetix, Netsparker/Invicti |
| 8 | Unsecured / Open Ports | Các cổng dịch vụ mở không cần thiết, tạo điểm vào tiềm năng cho kẻ tấn công. | Medium | Nmap, Fping, Shodan |
| 9 | Lộ thông tin máy chủ | Tiết lộ thông tin cấu hình máy chủ/phần mềm, giúp kẻ tấn công xác định lỗ hổng. | Low | Nmap, Whatweb, BuiltWith, HTTP Headers, Google Dorks |
| 10 | Information Disclosure in Error Messages | Hiển thị thông báo lỗi chi tiết, tiết lộ cấu trúc nội bộ hoặc phiên bản phần mềm. | Low | OWASP ZAP, Burp Suite |

**Tổng kết lỗ hổng:**

* **Critical:** 1
* **High:** 4
* **Medium:** 3
* **Low:** 2
* **Tổng số lỗ hổng:** 10

Lab4













