| **Hạng mục** | **Triệu chứng (dấu hiệu lỗ hổng)** | **Payload ví dụ** | **Kết quả mong đợi (mục tiêu test)** | **Khuyến nghị khắc phục** |
| --- | --- | --- | --- | --- |
| **A01:2023 - Broken Access Control** | Người dùng thường có thể truy cập dữ liệu/tính năng không thuộc quyền | GET /admin/deleteUser?id=5 (dùng user thường) | Truy cập **không hợp lệ bị chặn** (HTTP 403) | Áp dụng **RBAC**, kiểm tra quyền ở backend, dùng middleware auth |
| **A02:2023 - Cryptographic Failures** | Thông tin nhạy cảm (password, token) lưu/trao đổi dưới dạng plaintext | Chặn traffic: thấy mật khẩu trong HTTP | Mật khẩu **không hiển thị** (dùng TLS + hashing) | Bật **HTTPS**, dùng **bcrypt/argon2** để hash mật khẩu |
| **A03:2023 - Injection** | Có chèn được code SQL/OS command vào input | ' OR '1'='1 (SQLi), ; ls (OS command) | Ứng dụng **từ chối** payload, không rò dữ liệu | Dùng **prepared statements**, lọc input, ORM |
| **A04:2023 - Insecure Design** | Chức năng app cho phép bypass logic (ví dụ reset mật khẩu không xác thực email) | Gửi request reset mật khẩu với email bất kỳ | Ứng dụng yêu cầu **multi-step verification** | Áp dụng **secure SDLC**, threat modeling, kiểm tra business logic |
| **A05:2023 - Security Misconfiguration** | Header bảo mật thiếu, bật debug mode | Kiểm tra response header không có Content-Security-Policy | Response **có đầy đủ** security headers | Tắt debug, cấu hình **CSP, HSTS, X-Frame-Options** |
| **A06:2023 - Vulnerable & Outdated Components** | Dùng framework version cũ có CVE | Kiểm tra banner: X-Powered-By: Express/4.15.0 | Phiên bản **cập nhật, không có CVE known** | Quản lý patch, SCA tools (OWASP Dependency-Check) |
| **A07:2023 - Identification & Authentication Failures** | Cho phép brute-force login hoặc session ID đoán được | Dùng Hydra: hydra -l admin -P rockyou.txt target.com | Login bị **rate-limit**, session ID random | Áp dụng **MFA, rate-limiting, session timeout** |
| **A08:2023 - Software & Data Integrity Failures** | Ứng dụng tải code/plugin từ nguồn không xác thực | Chèn script vào dependency update | Ứng dụng **verify checksum/signature** | Dùng **code signing, supply chain security** |
| **A09:2023 - Security Logging & Monitoring Failures** | Tấn công nhưng log không ghi lại / SIEM không cảnh báo | SQLi thử nhiều lần nhưng không thấy log | Ứng dụng **ghi log đầy đủ, alert gửi SOC** | Dùng **centralized logging, SIEM (ELK/Wazuh)** |
| **A10:2023 - Server-Side Request Forgery (SSRF)** | Người dùng có thể ép server truy cập URL nội bộ | Payload: http://127.0.0.1:8080/admin trong request | Server **từ chối** truy cập nội bộ | Dùng allowlist URL, chặn private IP range |