**Lời nói đầu**

Áp dụng tiêu chuẩn OWASP về Web Application Security Testing (4) mục (4.5) Authentication Testing, ([4.5.8) Testing for Weak security question/answer (OTG-AUTHN-008)](https://www.owasp.org/index.php/Testing_for_Weak_security_question/answer_(OTG-AUTHN-008)); mục (4.6) Authorization Testing, ([4.6.1) Testing Directory traversal/file include (OTG-AUTHZ-001)](https://www.owasp.org/index.php/Testing_for_Path_Traversal_(OTG-AUTHZ-001)); mục (4.8) Input Validation Testing, (4.8.1) [Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)](https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)); ([4.8.5) Testing for SQL Injection (OTG-INPVAL-005)](https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)). Sử dụng công cụ Burp Suite để đánh giá.

1. Testing for Weak security question/answer

* Thường được gọi là câu hỏi và câu trả lời "bí mật", câu hỏi và câu trả lời bảo mật thường được sử dụng để khôi phục mật khẩu hoặc bảo mật bổ sung trên mật khẩu.

1. [Testing Directory traversal/file include (OTG-AUTHZ-001)](https://www.owasp.org/index.php/Testing_for_Path_Traversal_(OTG-AUTHZ-001))

* Nhiều ứng dụng web sử dụng và quản lý các tệp như một phần của hoạt động hàng ngày của chúng. Sử dụng các phương thức xác thực đầu vào chưa được thiết kế hoặc triển khai tốt, kẻ xâm nhập có thể khai thác hệ thống để đọc hoặc ghi các tệp không được phép truy cập. Trong các tình huống cụ thể, có thể thực thi các lệnh hệ thống hoặc mã tùy ý.

1. Testing for Reflected Cross Site Scripting (OTG-INPVAL-001)

* Reflected Cross Site Scripting (XSS) xảy ra khi kẻ tấn công tiêm mã thực thi của trình duyệt trong một phản hồi HTTP. Những kẻ tấn công thường tận dụng các lỗ hổng này để cài đặt bộ ghi nhật ký khóa, đánh cắp cookie nạn nhân hoặc thay đổi nội dung của trang. Thông thường mã của kẻ tấn công được viết bằng ngôn ngữ Javascript

1. Testing for SQL Injection (OTG-INPVAL-005)

* Một cuộc tấn công [tiêm SQL](https://www.owasp.org/index.php/SQL_injection) bao gồm chèn hoặc "tiêm" một truy vấn SQL một phần hoặc toàn bộ thông qua đầu vào dữ liệu hoặc được truyền từ máy khách (trình duyệt) đến ứng dụng web. Một cuộc tấn công SQL thành công có thể đọc dữ liệu nhạy cảm từ cơ sở dữ liệu, sửa đổi cơ sở dữ liệu (chèn/cập nhật/xóa), thực thi các thao tác quản trị trên cơ sở dữ liệu, …

1. Burp Suite

- Là một công cụ đồ họa để kiểm tra bảo mật ứng dụng Web

|  |  |  |
| --- | --- | --- |
| **STT** | **Đánh giá** | **Kịch bản** |
| 1 | OTG-AUTHN-008 | B1: Người dùng nhập nội dung vào thẻ <input>  B2: Sử dụng Burp Suite Tool để xem các request  B4: Sử dụng Intruder trong Burp Suite tất công để xem các username  B5: Sử dụng một user để khôi phục password bằng các câu hỏi bí mật  B6: Tiếp tục sử dụng Intruder tấn công để tìm ra câu trả lời cho câu hỏi bí mật  B7: Lấy lại mật khẩu |
| 2 | OTG-AUTHZ-001 | B1: Gửi 1 request có kèm theo giá trị đường dẫn file  B2: Sử dụng Burp Suite để xem request  B4: Sử dụng Proxy để chặn request  B5: Thay đổi nội dung request dẫn tới file khác  B6: Kiểm tra nội dung file |
| 3 | OTG-INPVAL-001 | B1: Người dùng nhập nội dung vào thẻ <input>  B2: Sử dụng Burp Suite Tool để xem các request  B3: Kiểm tra request đã reflected trong response từ server  B4: Sử dụng tính năng Intruder trong Burp Suite để tấn công  B5: Lấy cookie |
| 4 | OTG-INPVAL-005 | B1: Sử dụng Burp Suite để scan và tìm lỗ hổng SQL injection  B2: Sử dụng tính năng Intruder trong Burp Suite để tấn công |