BÁO CÁO KIỂM THỬ BẢO MẬT ỨNG DỤNG WEB

Bản dịch tiếng Việt từ tài liệu "Blaze – Sample Web Application Penetration Testing Report" (phát hành 21/11/2022, 45 trang).

Khách hàng: ACME Ltd.

Đơn vị thực hiện: Blaze Information Security

1. Kiểm soát tài liệu

Phiên bản: 1.2 – Ngày phát hành 21/11/2022

Mức độ bảo mật: Lưu hành nội bộ của ACME Ltd. và Blaze Information Security.

Liên hệ: security@blazeinfosec.com

2. Giới thiệu

Báo cáo này trình bày toàn bộ kết quả của đợt kiểm thử xâm nhập (penetration test) đối với ứng dụng web của ACME Ltd. Mục tiêu là phát hiện, khai thác và đánh giá các lỗ hổng bảo mật, đồng thời đề xuất biện pháp khắc phục nhằm giảm thiểu rủi ro.

3. Phạm vi đánh giá

Thành phần	URL / IP
Cổng người dùng	https://web.acme.ltd (5.6.7.8)
Trang quản trị	https://admin.acme.ltd (1.3.3.7)
API	https://api.acme.ltd (4.3.2.1)

4. Tóm tắt đợt đánh giá

Thời gian: 11 – 22/04/2022 (10 ngày công).

Đội ngũ: 2 chuyên gia bảo mật cấp Senior.

Môi trường: staging, truy cập từ xa.

Phương pháp: kết hợp quét tự động và đánh giá thủ công chuyên sâu.

5. Phương pháp luận

Quy trình dựa trên OWASP Testing Guide và OSSTMM gồm 5 giai đoạn: 1) Thu thập thông tin; 2) Lập bản đồ ứng dụng; 3) Kiểm thử theo OWASP Top 10; 4) Khai thác & kiểm chứng; 5) Báo cáo & xác minh lại.

6. Tóm tắt điều hành

9 lỗ hổng được xác định: 1 Nghiêm trọng, 4 Cao, 2 Trung bình, 2 Thấp. Các lỗ hổng nghiêm trọng có thể dẫn tới chiếm đoạt tài khoản, rò rỉ cơ sở dữ liệu và phá hoại dữ liệu đơn hàng.

7. Bảng lỗ hổng

#	Lỗ hổng	CWE	Mức độ
1	IDOR đổi email → chiếm tài khoản	CWE-285	Nghiêm trọng
2	XSS lưu trữ	CWE-79	Cao
3	Blind SQL Injection	CWE-89	Cao
4	IDOR xoá đơn hàng	CWE-284	Cao
5	Host header poisoning (reset mật khẩu)	CWE-20	Cao
6	SSRF chưa xác thực	CWE-918	Trung bình
7	Truyền hash bcrypt qua GET	CWE-294	Trung bình
8	Cookie thiếu cờ Secure	CWE-614	Thấp
9	Tính năng quên mật khẩu dễ bị flood	CWE-799	Thấp

8. Chi tiết lỗ hổng

Lỗ hổng 1: IDOR đổi email → chiếm tài khoản

Mô tả: Điều khiển truy cập không đúng (IDOR) trong API chỉnh sửa người dùng cho phép kẻ tấn công thay đổi email của bất kỳ tài khoản nào, sau đó sử dụng chức năng "Quên mật khẩu" để chiếm đoạt tài khoản.

Tác động: Kẻ tấn công có thể chiếm quyền hàng loạt tài khoản người dùng hợp lệ.

Khuyến nghị: Áp dụng kiểm tra quyền sở hữu tại API, xác thực token phiên và userID.

Lỗ hổng 2: XSS lưu trữ

Mô tả: Trường nhập "Họ tên" trên trang hồ sơ không lọc ký tự HTML, cho phép chèn JavaScript (XSS lưu trữ).

Tác động: Thực thi mã tùy ý trong trình duyệt nạn nhân, đánh cắp cookie phiên.

Khuyến nghị: Triển khai lọc/encode đầu vào theo OWASP XSS Prevention Cheat Sheet.

Lỗ hổng 3: Blind SQL Injection

Mô tả: Tham số "columnName" trong endpoint /ar/ajax/tableaction dễ bị chèn SQL mù (Blind SQLi).

Tác động: Truy xuất toàn bộ CSDL, bao gồm dữ liệu cá nhân và thông tin đăng nhập đã hash.

Khuyến nghị: Sử dụng truy vấn có tham số (prepared statements) và cấp quyền DB tối thiểu.

Lỗ hổng 4: IDOR xoá đơn hàng

Mô tả: API xoá đơn hàng thiếu xác thực đối tượng, cho phép xoá đơn của người khác bằng cách thay đổi acmeOrderID.

Tác động: Kẻ tấn công gây mất mát dữ liệu giao dịch và gián đoạn dịch vụ.

Khuyến nghị: Kiểm tra quyền sở hữu đơn hàng trước khi thực hiện thao tác.

Lỗ hổng 5: Host header poisoning (reset mật khẩu)

Mô tả: Ứng dụng tin vào header Host khi tạo liên kết đặt lại mật khẩu, dẫn tới "Host Header Poisoning".

Tác động: Liên kết đặt lại được gửi tới domain do kẻ tấn công kiểm soát, đánh cắp token đặt lại.

Khuyến nghị: Xác thực giá trị Host header hoặc tạo URL tuyệt đối dựa trên cấu hình máy chủ.

Lỗ hổng 6: SSRF chưa xác thực

Mô tả: Endpoint "/fetch?url=" cho phép máy chủ truy cập địa chỉ tùy ý mà không giới hạn – dẫn tới SSRF.

Tác động: Truy cập dịch vụ nội bộ, quét cổng mạng doanh nghiệp.

Khuyến nghị: Hạn chế domain đích, dùng danh sách trắng, chặn IP cục bộ/metadata.

Lỗ hổng 7: Truyền hash bcrypt qua GET

Mô tả: Hash mật khẩu (bcrypt) bị truyền qua phương thức GET, dễ bị ghi log.

Tác động: Lộ hash dẫn tới tấn công offline brute-force.

Khuyến nghị: Gửi hash qua POST body, áp dụng HTTPS và xóa log nhạy cảm.

Lỗ hổng 8: Cookie thiếu cờ Secure

Mô tả: Cookie phiên thiếu cờ Secure, có thể bị tiết lộ trên kết nối HTTP.

Tác động: Tấn công Man-in-the-Middle đánh cắp cookie.

Khuyến nghị: Thêm thuộc tính Secure và HttpOnly cho cookie phiên.

Lỗ hổng 9: Tính năng quên mật khẩu dễ bị flood

Mô tả: Không giới hạn số lần gửi email quên mật khẩu, cho phép spam.

Tác động: Tấn công từ chối dịch vụ đối với máy chủ email và người dùng.

Khuyến nghị: Áp dụng rate limiting và CAPTCHA.

9. Kết luận

ACME Ltd. cần ưu tiên khắc phục các lỗ hổng truy cập ngang và injection, đồng thời triển khai quy trình kiểm thử bảo mật định kỳ để ngăn ngừa tái phát.