**PHỤ LỤC 09**

**BIÊN BẢN XÁC NHẬN**

**KẾT QUẢ KIỂM THỬ BẢO MẬT**

*Tên phần mềm* Hệ thống X

*Phiên bản*: X

*Môi trường:* Test

*Công việc*: Kiểm thử bảo mật chức năng Y

*Người thực hiện*: Nguyễn Văn A

*Ngày thực hiện*: 24/12/2018 – 26/12/2018

*Mô tả kết quả*: Kết quả được mô tả trong bảng dưới đây

# mô tẢ Ứng dỤng

Ứng dụng được triển khai trên môi trường Test.

Chi tiết:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Địa chỉ ứng dụng** | **Tên ứng dụng** | **Nền tảng** | **Phiên bản** |
| 1 |  |  |  |  |

# cách thỨc tiẾp cẬn & phương pháp luẬn

## Các loại kiểm thử

|  |  |
| --- | --- |
| **Loại kiểm thử** | **Thực hiện** |
| Kiểm thử quản lý cấu hình và triển khai | Checked |
| Kiểm thử quản lý định danh | Checked |
| Kiểm thử xác thực | Checked |
| Kiểm thử phân quyền | Checked |
| Kiểm thử quản lý phiên | Checked |
| Kiểm thử xử lý dữ liệu đầu vào | Checked |
| Kiểm thử mật mã | Checked |
| Kiểm thử các lỗi logic | Checked |
| Kiểm thử web service | Checked |
| Kiểm thử phía client | Checked |
| Kiểm thử tấn công từ chối dịch vụ | Checked |

## Mô tả điểm yếu

Đưa ra, mô tả các loại điểm yếu kỹ thuật và cung cấp chi tiết thông tin về điểm yếu được phát hiện ra trong quá trình kiểm thử bảo mật.

|  |  |
| --- | --- |
| **Tên điểm yếu** | |
| **Mức độ** |  |
| **Thuộc danh mục OWASP** |  |
| **Sơ lược về điểm yếu** |  |
| **Khả năng khai thác** |  |
| **Khả năng tác động** |  |
| **Khuyến cáo** |  |
| **Bằng chứng** |  |
| **URL bị tác động** |  |
| **Ghi chú** |  |
| **Tham khảo** |  |
| **CWE** |  |
| **CWSS Score** |  |

* **Tên điểm yếu**: Mộ mô tả ngắn gọn về điểm yếu.

Tên điểm yếu sẽ được bôi mầu khác nhau để xác định mức độ rủi ro của điểm yếu, quy ước có 03 mã mầu như sau:

|  |  |
| --- | --- |
| **Mức độ rủi ro** | **Mô tả** |
| **Cao** | Điểm yếu có mức độ rủi ro **Cao** có thể bị khai thác bởi một kẻ tấn công lấy được quyền quản trị truy cập cao nhất vào ứng dụng hoặc hệ điều hành bên dưới. |
| **Trung bình** | Điểm yếu có mức độ rủi ro **Trung bình** để lộ những thông tin về ứng dụng và thông tin về kiến trúc bên dưới, nó có thẻ được sử dụng để kẻ tấn công khai thác những điểm yếu khác nhằm lấy được quyền quản trị của ứng dụng hoặc hệ điều hành bên dưới. |
| **Thấp** | Điểm yếu có mức độ rủi ro **Thấp** có thể liệt kê ra những thông tin trợ giúp quan trọng hoặc về ứng dụng hoặc về hệ điều hành bên dưới. |

* **Thuộc danh mục OWASP:** Điểm yếu có thuộc 10 điểm yếu bảo mật chúy ý của năm không.
* **Sơ lược về điểm yếu:** Mô tả về luồng hoặc bugs gây ra điểm yếu.
* **Khả năng khai thác:** Cung cấp mức độ yêu cầu kỹ năng để khai thác điểm yếu, gồm có:

|  |  |
| --- | --- |
| **Thước đo** | **Yêu cầu kỹ năng** |
| Dễ | Người sử dụng có mức độ hiểu biết bình thường. |
| Trung bình | Đòi hỏi phải tính toán, có kiến thức. |
| Khó | Phải là một hacker thực sự. |

* **Khả năng tác động:** Mô tả khả năng tác động nghiệp vụ nếu điểm yếu được khai thác thành công.
* **Khuyến cáo:** Cung cấp giải pháp hoặc cách giải quyết giảm thiểu rủi ro từ điểm yếu kỹ thuật.
* **Bằng chứng:** Đưa ra các bằng chứng của điểm yếu như vị trí tồn tại, form, màn hình…
* **URL bị tác động:** Đưa ra URLs và những tham số bị tác động bởi điểm yếu.
* **Ghi chú:** Một mô tả ngắn gọn là điểm yếu bị khai khai thác như thế nào bởi kẻ tấn công bên trong hoặc bên ngoài.
* **Tham khảo:** Cung cấp các tham chiếu từ các nguồn như OWASP, SANS,…
* **CWE:** Cung cấp các mã của điểm yếu hoặc các mã của các điểm yếu liên quan.
* **CWSS Score:** Cung cấp điểm của điểm yếu.

# thông tin chung vỀ ĐIỂM YẾU

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Mức độ rủi ro** | **Số lượng** | | Cao | 0 | | Trung bình | 2 | | Thấp | 1 | | Tổng số | 3 | |  |

Bảng danh sách điểm yếu:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Điểm yếu** | **Mức độ rủi ro** | **Bắt buộc xử lý** | **Trạng thái** |
| 1 | Password Brute Forcing | Trung bình | x | Open |
| 2 |  |  |  |  |
| 3 |  |  |  |  |

# chi tiẾT nhỮng điỂm yẾU đã đưỢc phát hiỆN

Trong quá trình kiểm thử nhóm phát hiện ra x điểm yếu có độ rủi ro trung bình và z điểm yếu có độ rủi ro thấp.

|  |  |
| --- | --- |
| Password Brute Forcing | |
| **Mức độ rủi ro** |  |
| **Thuộc danh mục OWASP** |  |
| **Sơ lược về điểm yếu** |  |
| **Khả năng khai thác** |  |
| **Khả năng tác động** |  |
| **Khuyến cáo** |  |
| **Bằng chứng** |  |
| **URL bị tác động** |  |
| **Ghi chú** |  |
| **Tham khảo** |  |
| **CWE** |  |
| **CWSS Score** |  |

# kẾT luẬn

|  |  |
| --- | --- |
| Hà Nội, Ngày 20 tháng 09 năm 2017 | |
| CÁN BỘ THỰC HIỆN | triển khai sauiển khai đượcTRƯỞNG ĐƠN VỊ ATBM |
| Đặng Long Hải | Nguyễn Phương Quân |