**BÁO CÁO**

**ĐÁNH GIÁ AN NINH THÔNG TIN ỨNG DỤNG**

**XXX**

**Đơn vị thực hiện: Bộ phận An ninh Thông tin**

TP Hồ Chí Minh, xx/xx/xxxx

Lưu hành nội bộ

**MỤC LỤC**

[**I.** **Tổng quan** 2](#_Toc175909952)

[1. Thông tin chung 2](#_Toc175909953)

[2. Thành phần kiểm tra đánh giá 2](#_Toc175909954)

[3. Phân loại cấp độ lỗ hổng 2](#_Toc175909955)

[4. Phạm vi thực hiện kiểm tra đánh giá 3](#_Toc175909956)

[5. Tóm tắt quá trình kiểm tra đánh giá 3](#_Toc175909957)

[**II.** **Chi tiết kiểm tra đánh giá** 5](#_Toc175909958)

[1. Bảng tóm tắt và biểu đồ lỗ hổng tìm được 5](#_Toc175909959)

[2. Danh sách lỗ hổng 5](#_Toc175909960)

[3. Chi tiết các lỗ hổng 5](#_Toc175909961)

[**III.** **Kết quả thực hiện** 6](#_Toc175909966)

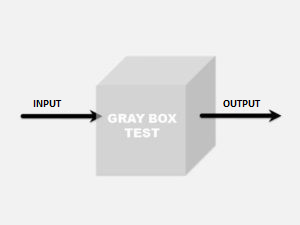
# **Tổng quan**

## Thông tin chung

|  |  |
| --- | --- |
| Tên hệ thống(\*) |  |
| Link truy cập |  |
| Đầu mối phát triển |  |
| Ngày thực hiện kiểm tra |  |
| Đơn vị thực hiện | Bộ phận An ninh Thông tin |
| Lý do đánh giá: | Đánh giá trước khi đưa vào sử dụng |

## Thành phần kiểm tra đánh giá

Thực hiện kiểm tra đánh giá theo hình thức Gray Box: Với phương pháp này cấu trúc bên trong ứng dụng được biết một phần (Thông thường là tài khoản nội bộ/test). Là phương pháp được thực hiện sau khi Bp. ANTT được cung cấp tài khoản ứng dụng, lập trình nội bộ. Dựa trên thông tin được cung cấp, Bp. ANTT có thể tiến hành kiểm tra đánh giá ứng dụng



## Phân loại cấp độ lỗ hổng

|  |  |
| --- | --- |
| **Mức độ** | **Mô tả** |
| **Nghiêm Trọng** | Các lỗi nghiêm trọng có thể khai thác để: Lấy thông tin tài khoản người dùng; Thực thi lệnh từ xa trên máy chủ; Làm gián đoạn hệ thống; ... |
| **Cao** | Hacker có thể khai thác lỗ hổng để lấy những nội dung nhạy cảm hoặc ảnh hưởng đến người dùng khác của các ứng dụng web. Ví dụ như một số loại cross-site scripting và các cuộc tấn công SQL injection, ... |
| **Trung Bình** | Các lỗ hổng ở mức độ này thường tiết lộ những thông tin bảo mật liên quan rò rỉ mã nguồn; thông tin xác thực qua các kênh không mã hóa; chưa cập nhật các bản vá lỗi, … |
| **Thấp** | Các lỗ hổng mức độ thấp có rất ít tác động đến hoạt động kinh doanh của tổ chức. Việc khai thác các lỗ hổng này thường yêu cầu quyền truy cập hệ thống cục bộ hoặc hệ thống vật lý, ... |

## Phạm vi thực hiện kiểm tra đánh giá

|  |  |
| --- | --- |
| **Thực hiện kiểm tra đánh giá** | **Nội dung** |
| Hình thức đánh giá | Graybox |
| Tài khoản được cung cấp | Username :  Password : |

## Tóm tắt quá trình kiểm tra đánh giá

Chi tiết công việc thực hiện kiểm tra đánh giá như sau:

| **STT** | **Nội dung** | **Mô tả** | **Nội dung thực hiện** | **Tình trạng** | **Retest** |
| --- | --- | --- | --- | --- | --- |
| 1 | Thu thập và khảo sát thông tin | Thực hiện tìm kiếm thông tin về ứng dụng phục vụ cho quá trình đánh giá | Phân tích các trình web spider, robots và Crawlers | **PASS** |  |
| Sử dụng công cụ tìm kiếm | **PASS** |  |
| Xác định các điểm vào của ứng dụng | **PASS** |  |
| Nhận diện Web Server | **PASS** |  |
| Dò tìm thông tin ứng dụng | **PASS** |  |
| Phân tích các trang báo lỗi | **PASS** |  |
| 2 | Kiểm tra cấu hình | Việc phân tích cơ sở hạ tầng và kiến trúc của website có thể giúp xác định rất nhiều yếu tố về một ứng dụng web như: Một số thông tin về mã nguồn, các phương pháp xử lý mà HTTP cho phép, chức năng, phương pháp xác thực, và cấu hình cơ sở… | Kiểm tra giao thức SSL/TLS | **PASS** |  |
| Dò tìm CSDL | **PASS** |  |
| Kiểm tra cấu hình máy chủ web | **PASS** |  |
| Kiểm tra cấu hình ứng dụng web | **PASS** |  |
| Phân tích cách thức ứng dụng xử lý tên tập tin | **PASS** |  |
| Tìm các tập tin cũ, lưu trữ và không được tham chiếu | **PASS** |  |
| Kiểm tra giao diện quản trị | **PASS** |  |
| Kiểm tra phương pháp HTTP và XST | **PASS** |  |
| 3 | Kiểm tra phần xác thực | Xác thực là cơ chế xác định chủ thể khi đăng nhập vào hệ thống. Cơ chế này chính là phần đăng nhập log-on vào ứng dụng trực tuyến. Kiểm tra cơ chế xác thực dựa trên các phân tích cơ chế hoạt động của module log-on trong ứng dụng Web để tìm ra các điểm yếu. | Kiểm tra phương thức truyền dữ liệu thông qua kênh liên lạc an toàn | **PASS** |  |
| Kiểm tra liệt kê người dùng | **PASS** |  |
| Tìm các tài khoản mặc định hoặc dễ đoán | **PASS** |  |
| Tấn công Brute Force | **PASS** |  |
| Tìm cách vượt qua tầng xác thực | **PASS** |  |
| Kiểm tra CAPTCHA | **PASS** |  |
| Tấn công cơ chế “nhớ mật khẩu” và cơ chế tạo lại mật khẩu | **PASS** |  |
| Cơ chế thoát và kiểm tra phần quản lý cache trên trình duyệt | **PASS** |  |
| Kiểm tra xác thực đa nhân tố | **PASS** |  |
| 4 | Kiểm tra quản lý phiên giao dịch | Kiểm tra xem cookie và các security token có được tạo ra một cách an toàn hoặc có thể đoán trước đựơc hay không. Một attacker nếu chiếm hoặc giả mạo được cookie có thể dễ dàng chiếm phiên của người khác | Phân tích cơ chế quản lý phiên giao dịch | **PASS** |  |
| Kiểm tra thuộc tính cookie | **PASS** |  |
| Kiểm tra lỗi Session Fixation | **PASS** |  |
| Kiểm tra việc bảo vệ các biến trong phiên | **PASS** |  |
| Kiểm tra lỗi CSRF | **PASS** |  |
| 5 | Kiểm tra quá trình cấp quyền | Trong phần này, chúng tôi sẽ tìm hiểu quá trình authorization làm việc, thử phá vỡ cơ chế authorization | Kiểm tra path traversal | **PASS** |  |
| Kiểm tra vượt qua cơ chế cấp quyền | **PASS** |  |
| Kiểm tra leo thang đặc quyền | **PASS** |  |
| 6 | Kiểm tra phê chuẩn đầu vào dữ liệu | Đa phần điểm yếu trong ứng dụng web tập trung vào khâu đánh giá đầu vào đến từ người dùng. Điểm yếu này dẫn đến hầu hết lỗ hổng trong ứng dụng web như: SQL injection, XSS...Dữ liệu từ các thành phần bên ngoài và người dùng không bao giờ được tin cậy, vì nó có thể bị can thiệp, sửa đổi bởi kẻ tấn công. Trong phần này tập trung vào Data Validation testing, trong đó, xem xét cách mà ứng dụng web xử lý đầu vào trước khi sử dụng | Kiểm tra Reflected XSS | **PASS** |  |
| Kiểm tra Stored XSS | **PASS** |  |
| Kiểm tra DOM XSS | **PASS** |  |
| Kiểm tra Cross Site Flashing | **PASS** |  |
| Kiểm tra SQL Injection | **PASS** |  |
| Kiểm tra ORM Injection | **PASS** |  |
| Kiểm tra LDAP Injection | **PASS** |  |
| Kiểm tra XML Injection | **PASS** |  |
| Kiểm tra XPath Injection | **PASS** |  |
| Kiểm tra IMAP/SMTP Injection | **PASS** |  |
| Kiểm tra Code Injection | **PASS** |  |
| Kiểm tra OS Commanding | **PASS** |  |
| Kiểm tra Buffer overflow | **PASS** |  |
| Kiểm tra lỗ hổng tiềm tàng | **PASS** |  |
| Kiểm tra lỗi HTTP Splitting/Smuggling | **PASS** |  |
| 7 | Đánh giá Web Services | Đánh giá lỗi của các thành phần WebServices | Thu thập thông tin WSDL (Web Services Description Language) | **PASS** |  |
| Kiểm tra WSDL (Web Services Description Language) | **PASS** |  |
| Kiểm tra kiến trúc XML | **PASS** |  |
| Kiểm tra nội dung của XML | **PASS** |  |
| Kiểm tra HTTP GET parameters/ REST | **PASS** |  |
| Kiểm tra SOAP | **PASS** |  |
| Replay Testing | **PASS** |  |
| 8 | Đánh giá AJAX | Đánh giá lỗi của các thành phần AJAX | Đánh giá AJAX | **PASS** |  |

# **Chi tiết kiểm tra đánh giá**

## Bảng tóm tắt và biểu đồ lỗ hổng tìm được

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Phân loại** | **Số lượng** | | | |
| **Mục tiêu** |  | | | |
| **Tổng số lỗi tìm được** | **0** | | | |
| **NGHIÊM TRỌNG/CAO / TRUNG BÌNH / THẤP** | **0** | **0** | **0** | **0** |

## Danh sách lỗ hổng

|  |  |  |
| --- | --- | --- |
| **Rủi ro** | **Lỗ hổng** | **Phạm vi ảnh hưởng** |
|  |  |  |

## Chi tiết các lỗ hổng

|  |  |  |
| --- | --- | --- |
| **MỨC ĐỘ** | | **NGHIÊM TRỌNG** |
| **ĐỘ KHÓ KHAI THÁC** | | CAO |
| **VỊ TRÍ ẢNH HƯỞNG** | |  |
| **MÔ TẢ** | |  |
| **ẢNH HƯỞNG** | |  |
| **CHI TIẾT KIỂM TRA** | | |
| **GỢI Ý KHẮC PHỤC** |  | |
| **THAM KHẢO** |  | |



# **Kết quả thực hiện**

- Hiện tại, phát hiện được lỗi bảo mật NGHIÊM TRỌNG tại thời điểm kiểm tra lần 1. Cần khắc phục các lỗ hổng mức độ TRUNG BÌNH trở lên đã tìm được trước khi golive.

- Những lỗ hổng mức THẤP có thể thực hiện xử lý sau khi golive.

* **Lưu ý:** Báo cáo chỉ có hiệu lực trong vòng 30 ngày kể từ ngày gửi Báo cáo

|  |  |
| --- | --- |
| TP HCM, ngày … tháng … năm …  **PHỤ TRÁCH ANTT** | TP HCM, ngày … tháng … năm …  **NHÂN SỰ KIỂM TRA** |
|  |  |

|  |
| --- |
| **PHÊ DUYỆT CỦA BAN GIÁM ĐỐC KHỐI CNNH** |