BÁO CÁO BÀI TẬP

**Môn học: Bảo mật Web và Ứng dụng**

**Kỳ báo cáo: Buổi 05 (Session 05)**

**Tên chủ đề: Ôn tập**

*GV: Nghi Hoàng Khoa*

*Ngày báo cáo: 24/5 /2023*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.N21.ANTN

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Võ Anh Kiệt | 20520605 | 20520605@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** | **Người đóng góp** |
| 1 | Kịch bản 01 | 100% |  |
| 2 | Kịch bản 02 | 100% |  |
| 3 | Kịch bản 03 | 100% |  |
| 4 | Kịch bản 04 | 100% |  |
| 5 | Kịch bản 05 | 100% |  |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

## Kịch bản 01

**Tên**: Lỗi curl\_exec khi thực hiện gửi câu truy vấn vào box của web

**Mô tả:** thực hiện truyền câu truy vấn gọi các file trong khung truyền giá trị để gọi các file lên

**Các bước thực hiện:**

Đầu tiên ta thực hiện vào trang và quan sát

A screenshot of a computer

Description automatically generated

Tiếp tục ta thực hiện thử truyền câu truy vấn

A screenshot of a computer

Description automatically generated

Thì sau khi truyền xong ta có dự đoán rằng trang có thể bị vul liên quan đến curl\_exec

<https://www.acunetix.com/vulnerabilities/web/php-curl_exec-url-is-controlled-by-user/>

Vậy ta sẽ thử thực hiện gửi câu truy vấn để xem thông tin /etc/passwd

A screenshot of a computer

Description automatically generated

Kết quả sau khi thực hiện truy vấn

A screenshot of a computer

Description automatically generated

Ta cũng có thể coi thông tin của một số file trong đó

A screenshot of a computer

Description automatically generated

Kết quả sau khi thực hiện truy vấn

A screenshot of a computer

Description automatically generated

**Mức độ: Cao**

**Khuyến cáo:**

Thực hiện lọc đầu vào khi trước khi thực hiện truy vấn, cập nhật phiên bản mới nhất của curl bản 7.87.0

## Kịch bản 02

**Tên:** Lỗi để các đường dẫn trực tiếp ngay trong file code và các api được lưu trực tiếp trong database

**Mô tả:** Thực hiện truy vấn vào trang database và tìm các api để thực hiện truy cập

**Các bước thực hiện:**

Đầu tiên ta thực hiện đọc code thì ta thấy thông tin về trang /graphql

A screenshot of a computer

Description automatically generated

Tiếp tục vào trang grapql, ở đây ta sẽ thực hiện xem toàn bộ các user và một số thông tin đi cùng

A screenshot of a computer

Description automatically generated

Ở đây ta thấy thông tin là ở johndoe đang có uuid là 1 khi thực hiện xem thông tin của toàn user

Tiếp tục ta sẽ xem thông tin của johndoe với uuid là 1

A screenshot of a computer

Description automatically generated

Ở đây ta thấy được thông tin của apiKey như hình, ta sẽ thực hiện sử dụng apiKey này để thực hiện đăng nhập.

Ở đây ta thực hiện truyền apiKey vào thẻ application

A screenshot of a computer

Description automatically generated

Thực hiện reload lại trang thì ta vào được trang của user của johndoe

A screenshot of a computer

Description automatically generated

**Mức độ: Cao**

**Khuyến cáo:** Thực hiện chặn các trang không được phép truy cập, thực hiện phân quyền truy cập, thực hiện lưu trữ apiKey an toàn hơn

## Kịch bản 03

**Tên:** Thực hiện kiểm tra và phát hiện các thư viện đang sử dụng có lỗ hỏng của domain www.rmit.edu.vn

**Mô tả:** Thực hiện sử dụng tool nuclei để tìm kiếm và phân tích các thư viện có chứa các lỗ hỏng

**Các bước thực hiện:**

Đầu tiên thực hiện tải tool nuclei bằng go: go install -v [github.com/projectdiscovery/nuclei/v2/cmd/nuclei@latest](mailto:github.com/projectdiscovery/nuclei/v2/cmd/nuclei@latest)

Tham khảo: <https://github.com/projectdiscovery/nuclei>

A screenshot of a computer

Description automatically generated

Tiếp theo thực hiện scanning

A picture containing text, screenshot, display, software

Description automatically generated

Ở đây ta thấy có lỗ hỏng XSS liên quan để jQuery, thực hiện lên mạng để kiểm tra

A screenshot of a computer

Description automatically generated

Ngoài ra ta cũng thấy các lỗi liên quan đến http-missing-security-headers

A screen shot of a computer program

Description automatically generated with low confidence

**Mức độ: cao**

**Khuyến cáo:** Thực hiện cập nhật các phiên bản mới nhất của các thư viện đang sử dụng, ngoài ra có thể thực hiện chặn việc scanning từ bên ngoài

## Kịch bản 04

**Tên:** Để lộ thông tin đăng nhập trực tiếp trên code

**Mô tả:** Thực hiện tìm kiếm code từ dịch ngược ra từ file apk thành java và tìm thấy thông tin đăng nhập

**Các bước thực hiện:**

Đầu tiên ta thực hiện dịch ngược, sau đó sử dụng ide vscode và tìm kiếm các thông tin thì ta thấy được thông tin đăng nhập được để trực tiếp trong code

A picture containing text, screenshot, software, multimedia software

Description automatically generated



Ta sẽ thực hiện đăng nhập thử

A screenshot of a computer

Description automatically generated with medium confidence

Thì ta đã đăng nhập thành công

**Mức độ: Cao**

**Khuyến cáo:** Thực hiện mã hoá và lưu thông tin đăng nhập của user vào database chứ không thực hiện ghi trực tiếp vào code

## Kịch bản 05

**Tên:** Thực hiện ghi log các thông tin đăng nhập

**Mô tả:** Thực hiện kiểm tra code và thông tin trong log để xem các thông tin đăng nhập

**Các bước thực hiện:**

Đầu tiên ta thực hiện lấy thông tin đăng nhập như yêu cầu 4

Tiếp theo thực hiện kiểm tra code java, ở đây ta thấy thông tin được ghi lại trực tiếp trong log

A picture containing text, screenshot, software, multimedia software

Description automatically generated

Để kiểm tra ta có thể vào đăng nhập vào app và kiểm tra log

A screenshot of a computer

Description automatically generated



Thì ta thấy được thông tin đăng nhập có trong log

**Mức độ: Cao**

**Khuyến cáo:** Thực hiện không ghi log lại các thông tin nhạy cảm như thông tin đăng nhập, các thông tin liên quan đến tài khoản payment

---

***Sinh viên đọc kỹ yêu cầu trình bày bên dưới trang này***

# **YÊU CẦU CHUNG**

* Sinh viên tìm hiểu và thực hành theo hướng dẫn.
* Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
* Sinh viên báo cáo kết quả thực hiện và nộp bài.

**Báo cáo:**

* File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
* Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
* Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành/Tên Cá nhân đã đăng ký với GV).

*Ví dụ: [*NT101.K11.ANTT*]-Session1\_Group3.*

* Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
* Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm.
* Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

**Đánh giá**: Sinh viên hiểu và tự thực hiện. Khuyến khích:

* Chuẩn bị tốt.
* Có nội dung mở rộng, ứng dụng trong kịch bản/câu hỏi phức tạp hơn, có đóng góp xây dựng.

*Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)