

5

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

Ôn tập

Thực hành môn Bảo mật web và ứng dụng

Tháng 5/2024

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

- Thực hành ôn tập lại một số lỗ hổng đã biết và viết báo cáo.

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

1. Docker

2. Phần mềm yêu cầu

- Phần mềm Burp Suite được cung cấp hoặc bất kỳ một phần mềm proxy nào mà sinh viên sử dụng quen thuộc.

C. THỰC HÀNH

1. Tìm kiếm lỗi và báo cáo lỗ hổng

a) Lab1

- Môi trường thực hành sử dụng docker được cung cấp

```
docker load -i review1.tar
```

- Chạy môi trường bài thực hành

```
docker run -d -p 8999:80 review-lab/basic
```

- Truy cập trang web thông qua url:

```
http://127.0.0.1:8999
```

Bài tập 1:(2đ) Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

#Tiêu đề: Tiêu đề rõ ràng và ngắn gọn bao gồm loại lỗ hổng và tài sản bị ảnh hưởng.

#Mô tả lỗ hổng: Lỗ hổng này là gì? Trong các bước rõ ràng, làm thế nào để bạn tái tạo nó?

Tóm tắt:

Các bước để thực hiện lại và bằng chứng:

1. bước 1

2. bước 2

3. bước 3

Tài liệu hỗ trợ và tham khảo:

* Liệt kê bất kỳ tài liệu bổ sung nào (ví dụ: ảnh chụp màn hình, nhật ký, v.v.)

#Mức độ ảnh hưởng của lỗ hổng: Tác động bảo mật nào mà kẻ tấn công có thể đạt được?

#Khuyến cáo khắc phục: Làm thế nào để vá lỗ hổng này?

b) Lab2

- Môi trường thực hành sử dụng docker được cung cấp

```
docker load -i review2.tar
```

- Chạy môi trường bài thực hành

```
docker run -ti -p 5000:5000 review/graphql
```

- Truy cập trang web thông qua url:

```
http://127.0.0.1:5000
```

- Mã nguồn được cung cấp kèm theo:

```
app.py
```

Bài tập 2:(2đ) Báo cáo lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

#Tiêu đề: Tiêu đề rõ ràng và ngắn gọn bao gồm loại lỗ hổng và tài sản bị ảnh hưởng.

#Mô tả lỗ hổng: Lỗ hổng này là gì? Trong các bước rõ ràng, làm thế nào để bạn tái tạo nó?

Tóm tắt:

Các bước để thực hiện lại và bằng chứng:

1. bước 1

2. bước 2

3. bước 3

Tài liệu hỗ trợ và tham khảo:

* Liệt kê bất kỳ tài liệu bổ sung nào (ví dụ: ảnh chụp màn hình, nhật ký, v.v.)

#Mức độ ảnh hưởng của lỗ hổng: Tác động bảo mật nào mà kẻ tấn công có thể đạt được?

#Khuyến cáo khắc phục: Làm thế nào để vá lỗ hổng này?

2. Tìm kiếm thông tin website trên internet.

Bài tập 3:(2đ) Tìm kiếm thông tin và hoàn thành các thử thách tại <https://tryhackme.com/r/room/greptrp>. Viết báo cáo giải thích cách có đáp án các câu hỏi.

Task 1 ○ Grep



Welcome to the OSINT challenge, part of TryHackMe's Red Teaming Path. In this task, you will be an ethical hacker aiming to exploit a newly developed web application.

▶ Start Machine

SuperSecure Corp, a fast-paced startup, is currently creating a blogging platform inviting security professionals to assess its security. The challenge involves using OSINT techniques to gather information from publicly accessible sources and exploit potential vulnerabilities in the web application.

Start by deploying the machine; Click on the **Start Machine** button in the upper-right-hand corner of this task to deploy the virtual machine for this room.

Your goal is to identify and exploit vulnerabilities in the application using a combination of recon and OSINT skills. As you progress, you'll look for weak points in the app, find sensitive data, and attempt to gain unauthorized access. You will leverage the skills and knowledge acquired through the Red Team Pathway to devise and execute your attack strategies.

Note: Please allow the machine 3 - 5 minutes to fully boot. Also, no local privilege escalation is necessary to answer the questions.

3. Ứng dụng android.

- Sử dụng ứng dụng android **InsecureShop.apk**. Báo cáo ít nhất 2 lỗ hổng được tìm thấy.

Bài tập 4,5:(4đ) Báo cáo 2 lỗ hổng tìm thấy. Sử dụng format theo mẫu sau:

#Tiêu đề: Tiêu đề rõ ràng và ngắn gọn bao gồm loại lỗ hổng và tài sản bị ảnh hưởng.

#Mô tả lỗ hổng: Lỗ hổng này là gì? Trong các bước rõ ràng, làm thế nào để bạn tái tạo nó?.

Tóm tắt:

Các bước để thực hiện lại và bằng chứng:

1. bước 1

2. bước 2

3. bước 3

Tài liệu hỗ trợ và tham khảo:

* Liệt kê bất kỳ tài liệu bổ sung nào (ví dụ: ảnh chụp màn hình, nhật ký, v.v.)

#Mức độ ảnh hưởng của lỗ hổng: Tác động bảo mật nào mà kẻ tấn công có thể đạt được?

#Khuyến cáo khắc phục: Làm thế nào để vá lỗ hổng này?

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện **theo nhóm đã đăng ký**.
- Nộp báo cáo kết quả gồm **Code, CSDL được export** và chi tiết những việc (**Report**) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).

Báo cáo:

- File **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Đặt tên theo định dạng: **[Mã lớp]-LabX_MSSV1-MSSV2-MSSV3**.
Ví dụ: *[NT213.K11.ANTN.1]-Lab1_1852xxxx-1852yyyy-1852zzzz*.
- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trể, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!