Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin
Khoa mạng máy tính và truyền thông
Bộ môn An toàn thông tin

6

Lab

Luyện tập cuối kì

Thực hành môn Lập trình ứng dụng Web

Tháng 5/2025

Lưu hành nội bộ

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

A. TỔNG QUAN

1. Mục tiêu

- Áp dụng kiến thức đã học về lập trình ứng dụng web để phân tích và khai thác các lỗ hổng thường gặp trong ứng dụng web.
- Rèn luyện kỹ năng viết báo cáo (writeup) để ghi lại quá trình khai thác.

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.

3. Liên quan

- Sinh viên cần nắm các kiến thức nền tảng Cấu trúc website: HTML, HTTP request/response, cookies, sessions.
- Tìm hiểu các lỗ hổng bảo mật web phổ biến như: SQL Injection (SQLi), Cross-site Scripting (XSS), File Inclusion, Web misconfigurations,…
- Tham khảo: OWASP Top Ten

B. THỰC HÀNH

1. Giới thiệu

CTF (Capture The Flag) là cuộc thi về an ninh mạng và người chơi phải khai thác các lỗ hổng để tìm ra "flag" – một chuỗi ký tự đại diện cho thành công trong việc khai thác.

Trong lab này, chúng ta sẽ chơi CTF về Web tại trang Cyber talents:
https://cybertalents.com/challenges/web
(Lưu ý: để tham gia các challenges, các bạn cần phải tạo tài khoản trên website)

Yêu cầu bài tập: Sinh viên chọn **10** web challenges bất kì phù hợp với trình độ tại link trên, giải quyết từng challenge bằng cách phân tích, khai thác và tìm được flag. Viết **writeup** (báo cáo) cho từng challenge theo mẫu dưới và nộp lại file .pdf.
Đánh giá dựa trên: mức độ hoàn thành và chất lượng writeup.

 # 1. Thông tin chung
###Tên challengle
###Mức độ (easy, medium, hard)
 # 2. Phân tích ban đầu (Initial Analysis)
###Mô tả cấu trúc trang web, chức năng các trang chính.
###Kiểm tra source HTML, JS, headers, cookies, ... có gì bất thường
###Công cụ sử dụng: DevTools / Burp Suite / curl / ...
###Giả thuyết về loại lỗ hổng bảo mật:
 # 3. Quá trình khai thác (Exploitation Steps)
###Các bước thực thực hiện và minh chứng (ảnh chụp màn hình,…)
1. Bước 1
2. Bước 2
3. Bước 3

###Tài liệu tham khảo:

 # 4. Mức độ ảnh hưởng: lỗ hổng bị khai thác sẽ ảnh hưởng đến những tài sản gì và có tác động bảo mật như thế nào?
 # 5. Cách khắc phục

2. Công cụ hỗ trợ và tài liệu tham khảo cho CTF Web Challenges

- Burp Suite
  - https://portswigger.net/burp/communitydownload
  - Proxy để chặn và chỉnh sửa request, phân tích request/response, tự động dò lỗi,…
- CyberChef
  - https://gchq.github.io/CyberChef/
  - Dùng để giải mã, encode/decode, chuyển đổi định dạng, regex...
- de4js
  - https://lelinhtinh.github.io/de4js/
  - Trình deobfuscation và unpack mã nguồn JavaScript
- dirsearch
  - https://github.com/maurosoria/dirsearch
  - Là CLI dùng để dò tìm các thư mục và tệp ẩn (directory and file brute-forcing) trên máy chủ web
- PayloadsAllTheThings
  - https://github.com/swisskyrepo/PayloadsAllTheThings
  - Kho payload dùng cho SQLi, XSS, LFI, SSTI...
- HackTricks
  - https://book.hacktricks.wiki/en/pentesting-web/web-vulnerabilities-methodology.html
  - Tập hợp kỹ thuật khai thác nhiều dạng lỗi bảo mật

C. 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 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_NhomY.
  - Ví dụ: [NT208.P12.ANTT.1]-Lab1_Nhom1.
  - 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, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!