CHƯƠNG TRÌNH ĐÀO TẠO PENTEST

BÀI 3: LỖI WEB CƠ BẢN - Authentication & Access Control

Thời gian	1 tuần

Yêu cầu:

Lý thuyết (4đ)

- Authentication:
  - Tìm hiểu các cơ chế xác thực sau: HTTP basic authentication, HTTP digest authentication. Hai cơ chế xác thực trên có vấn đề gì về security?
  - Liệt kê một số kĩ thuật (lỗ hổng) bypass authentication khi ứng dụng sử dụng Oauth2.
  - Liệt kê một số kĩ thuật (lỗ hổng) bypass 2FA.
- Access Control:
  - Phân biệt Vertical Access Control và Horizontal Access Control.
  - IDOR là gì? Làm thế nào để kiểm tra một chức năng có bị IDOR không?

Thực hành (6đ)

- Giải các bài lab trong phần authentication & access control trên: https://labs.matesctf.org/
- Kiểm tra các website challenge 1a có lỗi IDOR không? Nếu website có lỗi chỉ cần nêu ra một lỗi duy nhất để minh họa, không cần tìm tất cả.

Output:

- File báo cáo lý thuyết: challenge03.docx
- File writeups mô tả ngắn gọn cách giải các bài lab

- File report mô tả lỗi IDOR tìm được (nếu website không có lỗi nào thì ghi không bị lỗi, nếu website có nhiều lỗi chỉ cần mô tả một lỗi, thông tin mô tả gồm: chức năng bị lỗi, url, tham số, impact): report.docx

Tài liệu tham khảo:

- https://portswigger.net/web-security/authentication
- https://portswigger.net/web-security/access-control