ISP CLUB

CHƯƠNG TRÌNH ĐÀO TẠO
MẢNG WEB SECURITY
Tuần 5: SQL Injection

Thời gian: 1 tuần

1. YÊU CẦU

Yêu cầu lý thuyết:

- Tìm hiểu lý thuyết tại *https://portswigger.net/web-security/sql-injection* để viết docx trình bày các nội dung sau:
  - SQL Injection là gì?
  - Các loại SQLi, cách nhận biết, khai thác với từng loại?
  - Phòng chống?
  - Cách lập trình an toàn để không bị SQLi trong lập trình PHP?
- Cài đặt IDE để dev.

Làm Lab:

- Thực hành tất cả bài lab được mô tả tại *https://portswigger.net/web-security/all-labs#sql-injection* .
- Viết write up.

Đánh giá các ứng dụng đã code:

- Thực hiện tìm và khai thác lỗ hổng SQLi trong các bài đã code, gồm:

STT	Tên bài	Link web	Source code(git)
1	NamNG	*week4 (000webhostapp.com)*	*GitHub - giangnamG/week4update*
2	NamDN	*your tasks (000webhostapp.com)*	*GitHub - dnamgithub33/test2*
3	HuyNQ	*Login (000webhostapp.com)*	*GitHub - thewantedx/my_first_web*

- Format báo cáo phần này gồm 2 mục như sau:
  - Mục 1: Bảng gồm danh sách các lỗ hổng:

STT	Tên bài bị lỗi	Tên, vị trí lỗi

- Mục 2: Mô tả chi tiết từng lỗi, mỗi lỗi gồm các thông tin:
  - Vị trí lỗi.
  - Ảnh demo khai thác (dump db,…)

Làm CTF:

- Luyện tập 1 số bài CTF liên quan đến SQLi trên rootme (*Challenges/Web - Server [Root Me : Hacking and Information Security learning platform] (root-me.org)*)
- Viết writeup.

2. BÁO CÁO

File docx/pdf bao gồm:

- Trả lời phần lý thuyết.
- Báo cáo lỗ hổng tìm được trong bài code code PHP.
- Writeup các Lab trên portswigger.
- Writeup CTF.

3. TÀI LIỆU THAM KHẢO:

- *All labs | Web Security Academy (portswigger.net)*
- *What is SQL Injection? Tutorial & Examples | Web Security Academy (portswigger.net)*
- *Learn to Hack (hacksplaining.com)*
- *Challenges/Web - Server [Root Me : Hacking and Information Security learning platform] (root-me.org)*