AN NINH MÁY TÍNH

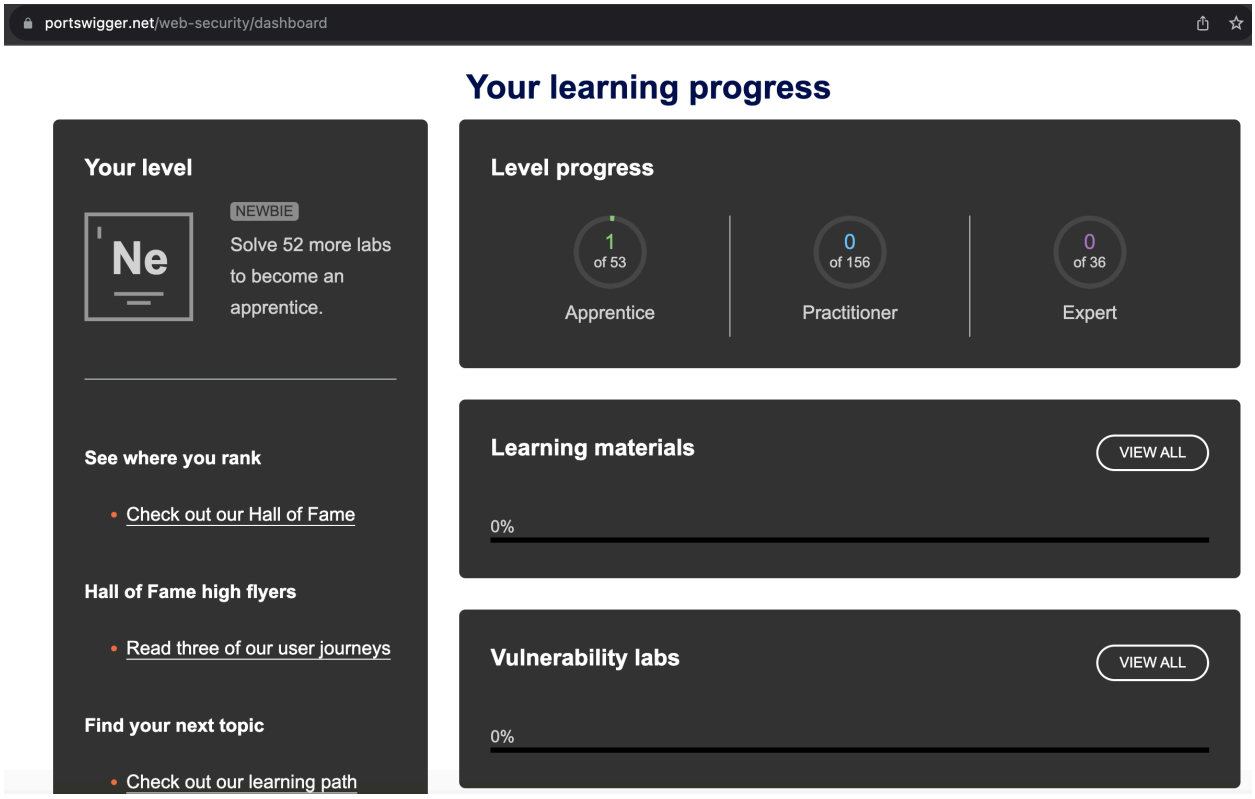
ĐỒ ÁN 2

QUI ĐỊNH

- Đồ án nhóm 2 sinh viên.
- Nhóm sinh viên thực hiện đồ án theo yêu cầu bên dưới, phân công đều để tất cả các thành viên trong nhóm đều tham gia thực hiện đồ án.
- Viết báo cáo trình bày rõ các nội dung sau:
    - Thông tin các thành viên trong nhóm (họ tên, mssv, email), phân công thực hiện
    - Ghi rõ các nội dung đã thực hiện, chụp màn hình minh chứng
    - Giải thích ngắn gọn, súc tích các vấn đề đã thực hiện được theo các yêu cầu của đề bài.
- 1 sinh viên đại diện nhóm nộp file MSSV1_MSSV2.zip/rar là bài nộp của nhóm lên link nộp bài ở website môn học.

YÊU CẦU

1. Tạo tài khoản trên website https://portswigger.net/
2. Thực hiện ít nhất 30 bài labs các bài "**Vulnerability labs"** tại https://portswigger.net/web-security/dashboard. Lưu ý: Làm tối đa 10 bài ở trình độ APPRENTICE và 10 bài ở trình độ PRACTITIONER



3. Viết báo cáo trình bày kết quả thực hiện bài tập. **Chụp màn hình** minh chứng và **giải thích cách thực hiện** và **kết quả** đạt được. Ví dụ, các hình minh hoạ sau cho biết bài lab đầu tiên đã được hoàn thành:

0a2600c603776e6b80b8300600060097.web-security-academy.net/filter?category=%27+OR+1=1--

Web Security Academy

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

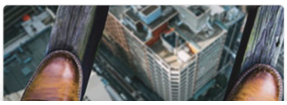
Home

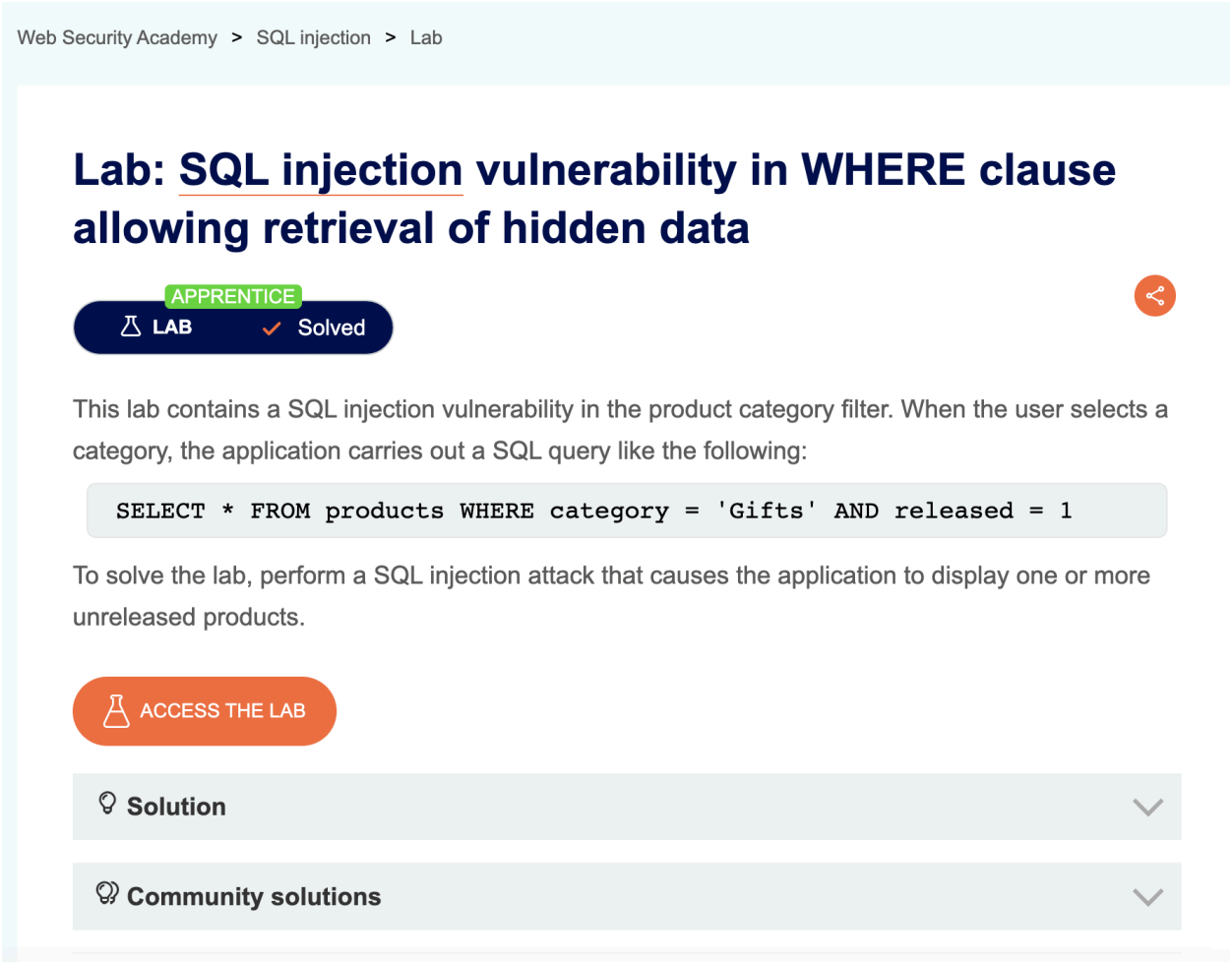
WE LIKE TO SHOP

' OR 1=1--

Refine your search:

All Accessories Food & Drink Gifts Lifestyle



4. Lập danh sách thống kê các labs, đánh dấu các labs đã thực hiện được. Ví dụ:

STT	Loại tấn công	Trình độ	Lab	Hoàn thành
1	SQL Injection	APPRENTICE	Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data	☑
2	Cross-site scripting	PRACTITIONER	Reflected XSS into HTML context with nothing encoded	☑
3		EXPERT		