Lab-Project 13: Exploiting SQL with Havij and Input Filtering

+ Website sử dụng: <http://testphp.vulnweb.com/>

+ Khai thác SQLi: <http://testphp.vulnweb.com/listproducts.php?cat=1> order by 5 – và thu được

A screenshot of a computer

Description automatically generated

=> Website bị SQLi

+ Tải Havij:

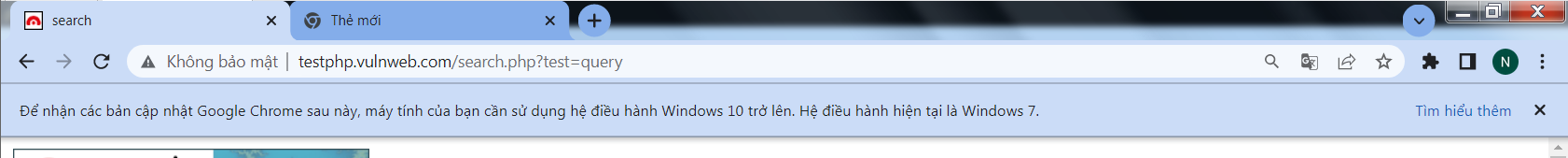
Link: <https://samsclass.info/123/proj14/Havij1.15Free.rar>

+ Sử dụng Havij để lấy dữ liệu:  
 - gõ vào thanh search một từ bất kỳ:

A screenshot of a computer

Description automatically generated

* Nhấn **go** và trên url sẽ hiện:



* Copy đường dẫn này vào thanh Target của Havij

A screenshot of a computer

Description automatically generated

- Nhấn vào nút **Analyze** và thu được kết quả:

A screenshot of a computer

Description automatically generated

=> Thu được database có tên: **acuart**

- Chọn tính năng **Get Tables** và thu được các bảng:

A screenshot of a computer

Description automatically generated

- Tích vào 1 bảng bất kỳ (ở đây tôi tích vào bảng **artists**), chọn **Get Columns** và thu được:

A screenshot of a computer

Description automatically generated

=> Các thuộc tính trong bảng

- Tích vào các cột được tìm thấy, chọn **Get Data** và thu được nội dung của từng cột

A screenshot of a computer

Description automatically generated

**Fixing the Vulnerability with Input Validation:**

Website sử dụng: <http://34.143.189.101/>

Tìm đến thanh tìm kiếm ở cuối trang:

A screenshot of a computer

Description automatically generated

Gõ 1 chữ cái (b) để lấy link truy vấn trên URL:

A screenshot of a computer

Description automatically generated

Copy đường dẫn vào thanh **Target** chọn **Analyze** để tiến hành khai thác SQLi

A screenshot of a computer

Description automatically generated

=> Đường dẫn này không bị SQli