**BÁO CÁO THỰC HÀNH ATHT**

**BÀI 06**

**MSSV: B1809365**

**Họ Tên: Phạm Thị Hồng Linh**

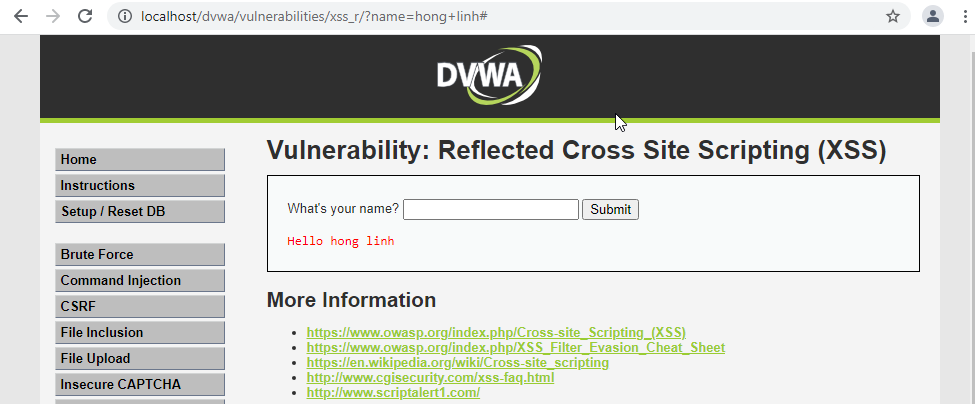
**PHẦN I: TỰ TẠO MỘT WEBSITE VÀ THỬ NGHIỆM:**

* Website có sẵn

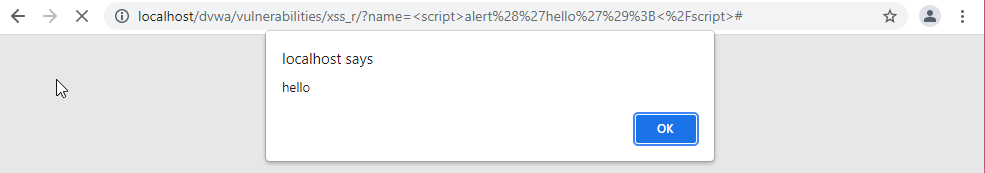
**Một số lỗi từ website khi chọn mức “low”**

1. **XSS (Reflected)**

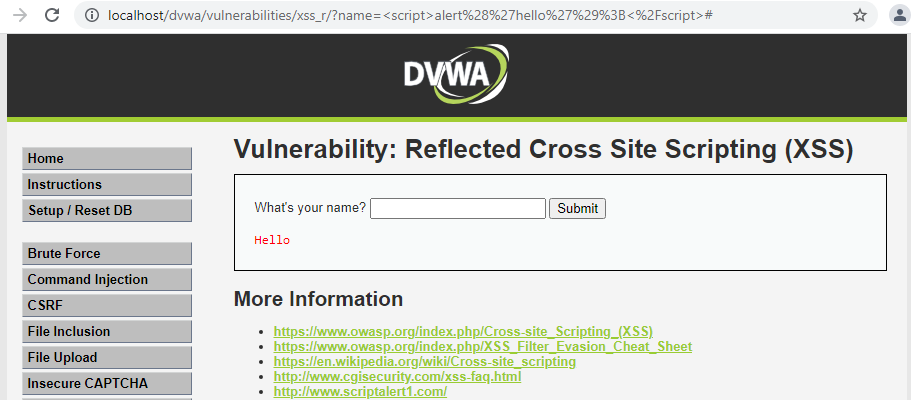
* Khi nhập tên là chuỗi bình thường sẽ không xảy ra lỗi và hiển thị như bên dưới



* Khi cố tình nhập 1 chuỗi có chứa các kí tự javascript. Lúc này website sẽ thực thi câu lệnh javascript

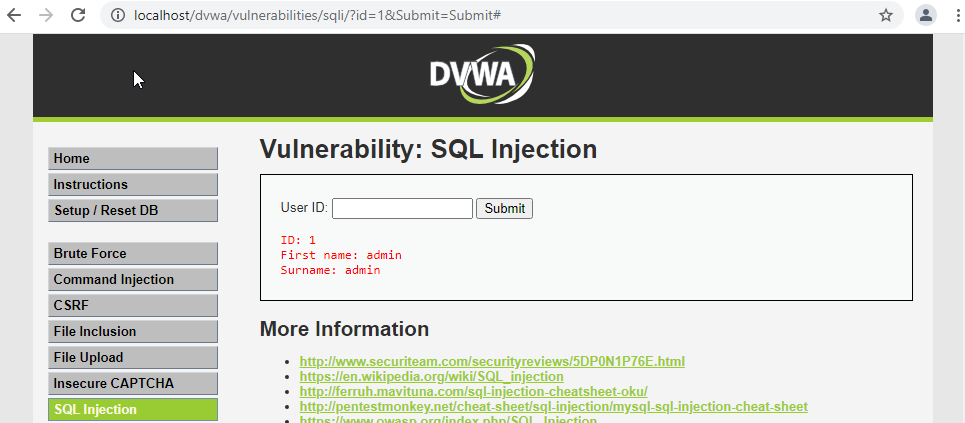


* Kết quả chỉ in ra câu “hello”



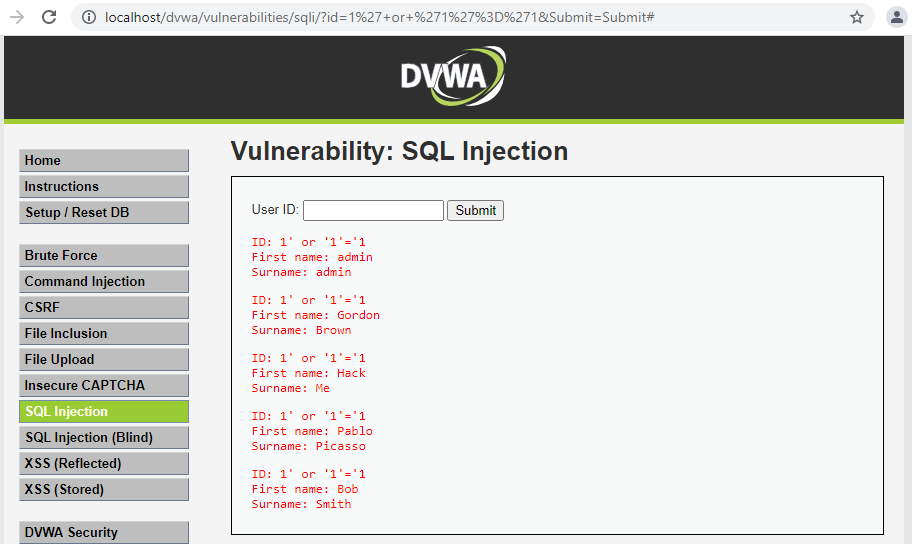
1. **SQL Injection:**

❖ Trường hợp nhập đúng



❖ Khi người dùng cố tình nhập sai để có thể tìm các thông tin liên quan đến cơ sở dữ liệu

* Liệt kê tất cả các tài khoản có trong cơ sở dữ liệu



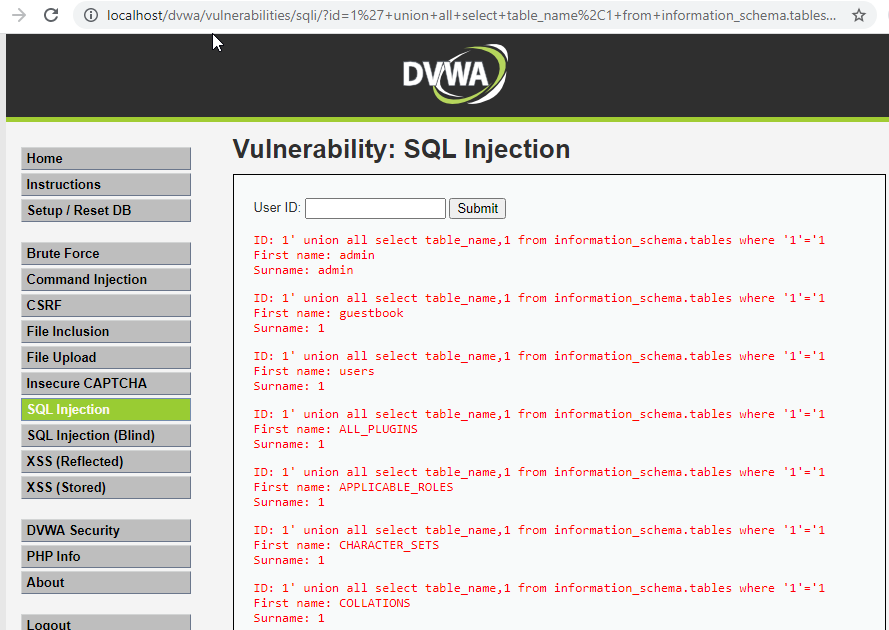
* Trong cơ sở dữ liệu có 5 tài khoản với họ tên như bên trên
* Lấy thông tin về phiên bản của cơ sở dữ liệu, ta nhập :

*1' union all select @@version, '1*



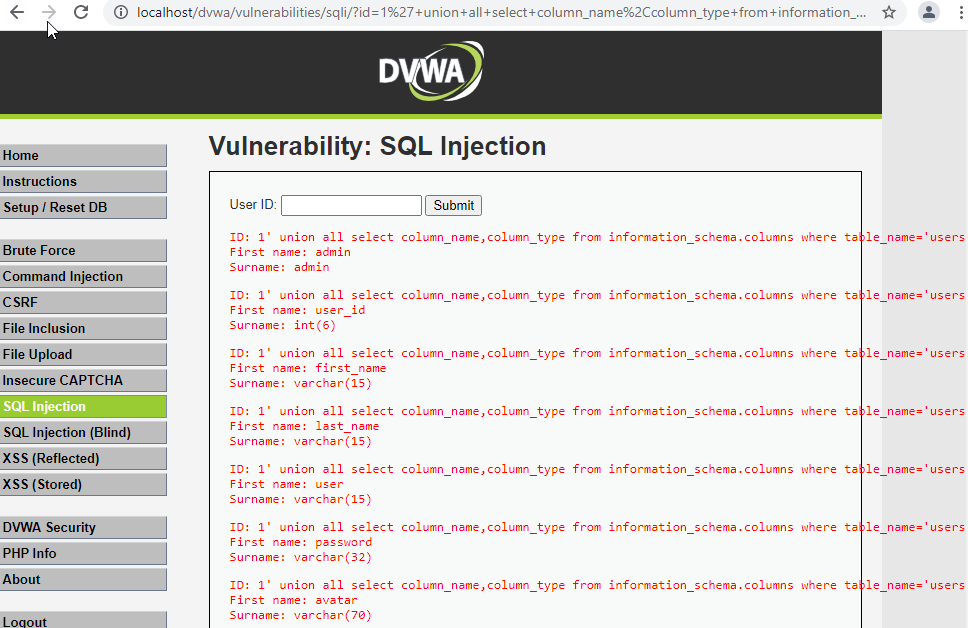
* Phiên bản của cơ sở dữ liệu là : 10.1.13-MariaDB
* Dò các bảng có trong cơ sở dữ liệu

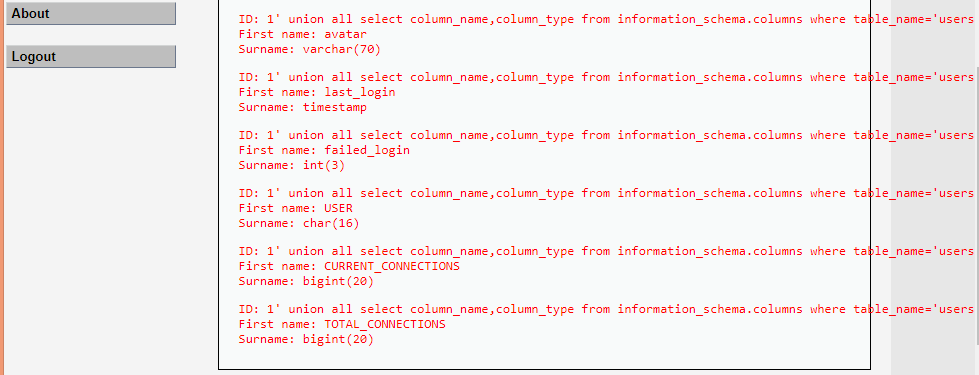
*1' union all select table\_name,1 from information\_schema.tables where '1'='1*



* Trong cơ sở dữ liệu có 2 bảng là: **guestbook** và **users**
* Hiển thị các cột và kiểu dữ liệu của từng cột trong một bảng

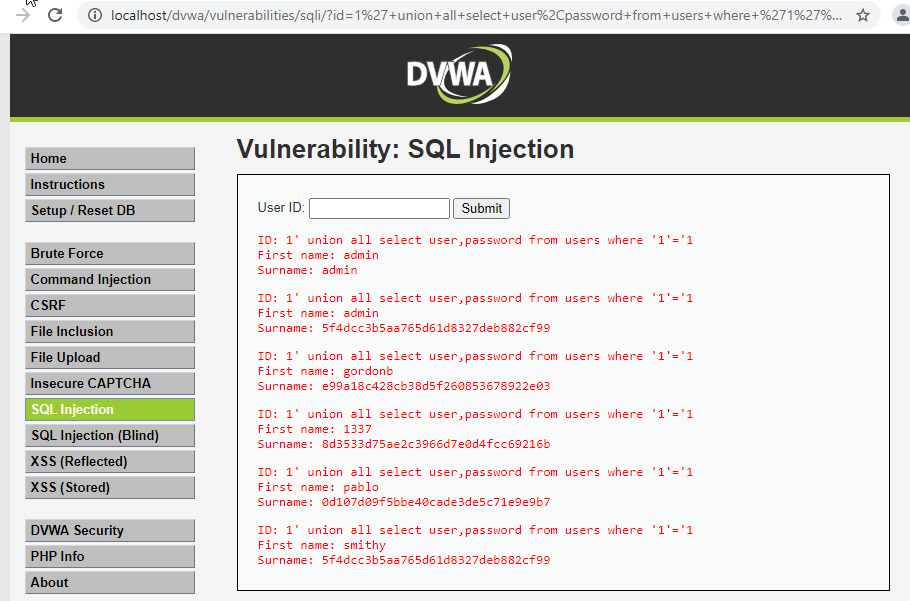
*1' union all select column\_name,column\_type from information\_schema.columns where table\_name='users*





* Hiển thị nội dung của 2 cột user và password trong bảng users

*1' union all select user,password from users where '1'='1*

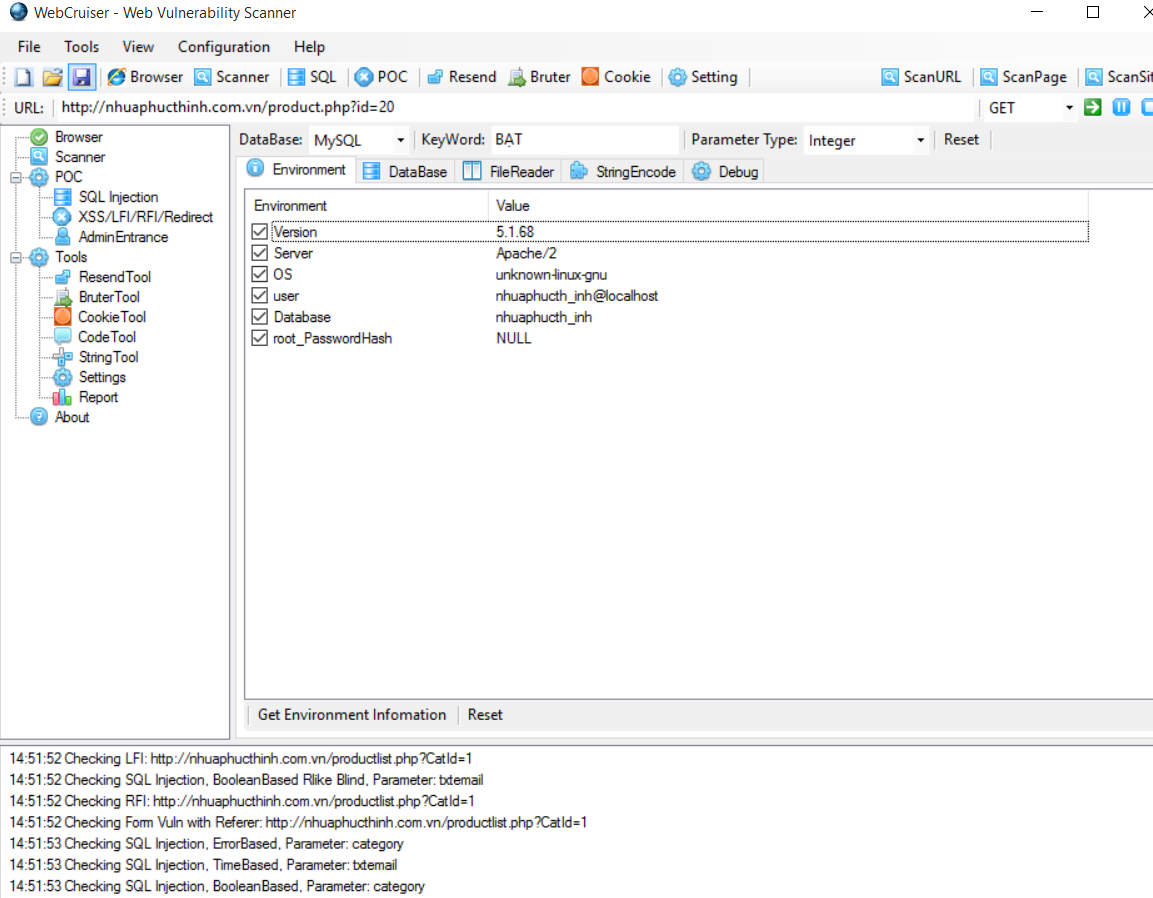


**PHẦN II: THỬ NGHIỆM VỚI WEBSITE BÊN NGOÀI:**

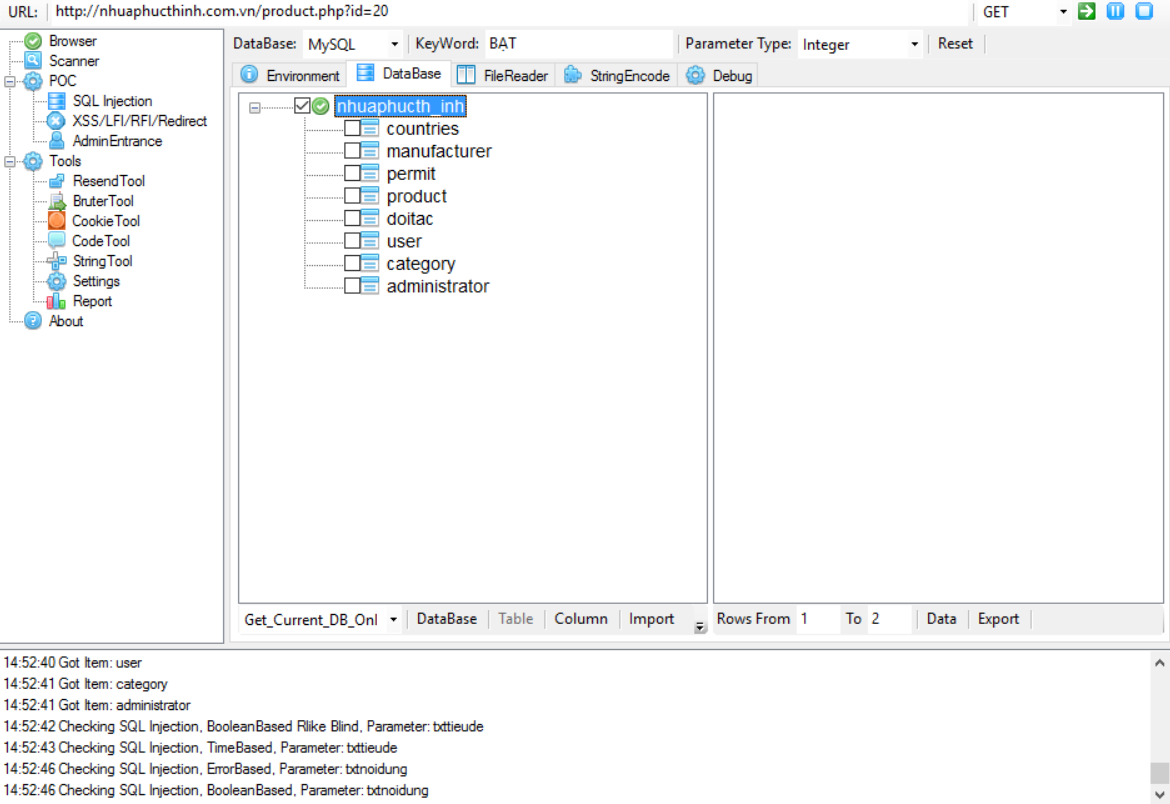
* Đường link đến website thử nghiệm: <http://nhuaphucthinh.com.vn/product.php?id=20>
* Khi đã quét và phát hiện lỗi, phải chuột vào lỗi -> chọn SQL INJECTION POC

1. **Xem một số thông tin liên quan đến: verion, server, hệ điều hành, tên user, tên database và mật khẩu**

* Check các thông tin cần xem và click chọn “Get Environment information”



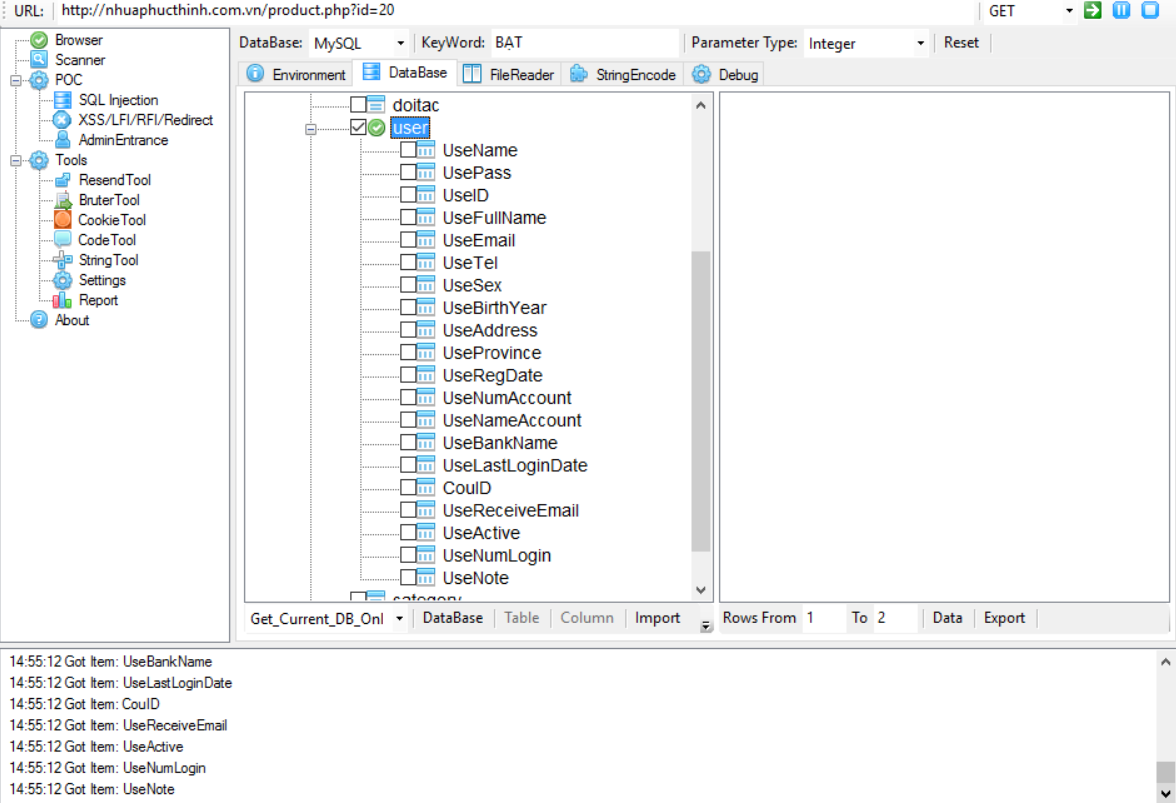
1. **Xem các bảng có trong cơ sở dữ liệu**



* Trong cơ sở dữ liệu nhuaphucth\_inh có 8 bảng

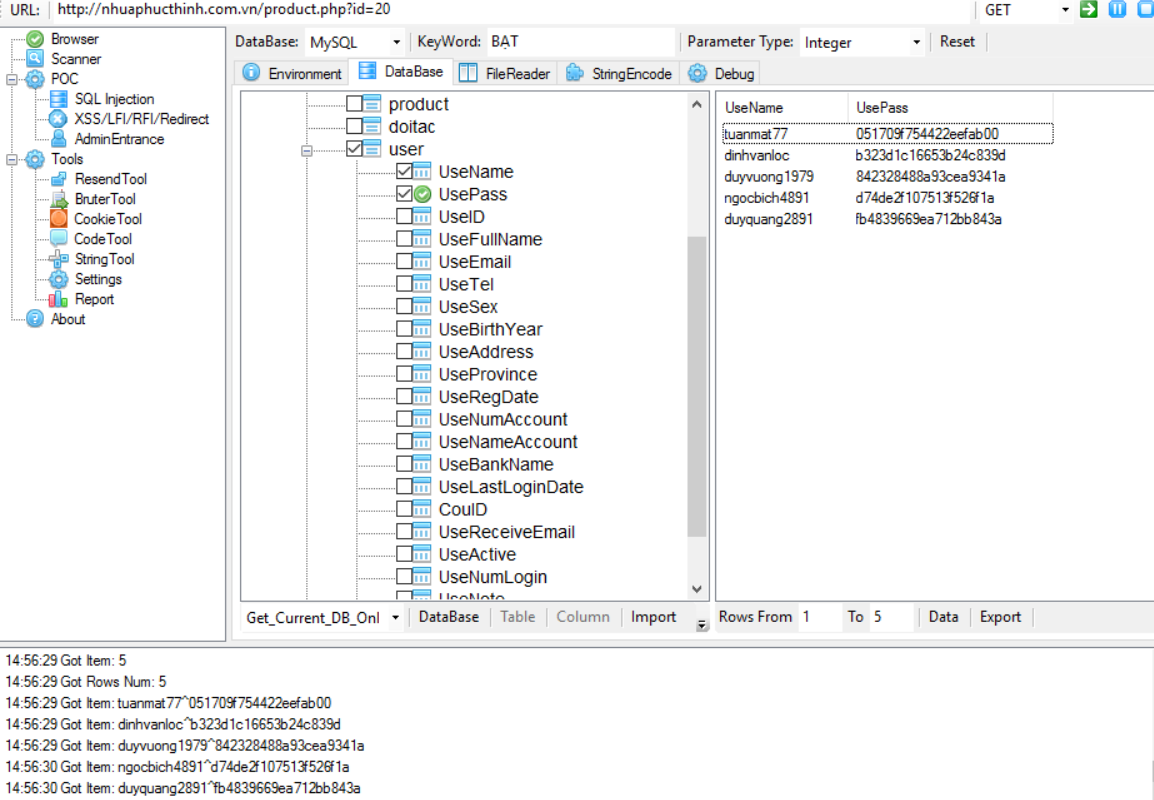
1. **Xem các trường trong bảng**

* Muốn xem bảng ‘user’:



1. **Xem dữ liệu lưu trong 1 số cột của bảng**

* Bảng muốn xem dữ liệu là bảng “user”, cần xem 2 trường là “UsePass” và “UseName”. Chọn số dòng hiển thị là 5 dòng chọn ‘Data’, kết quả như hình



*--Hết--*