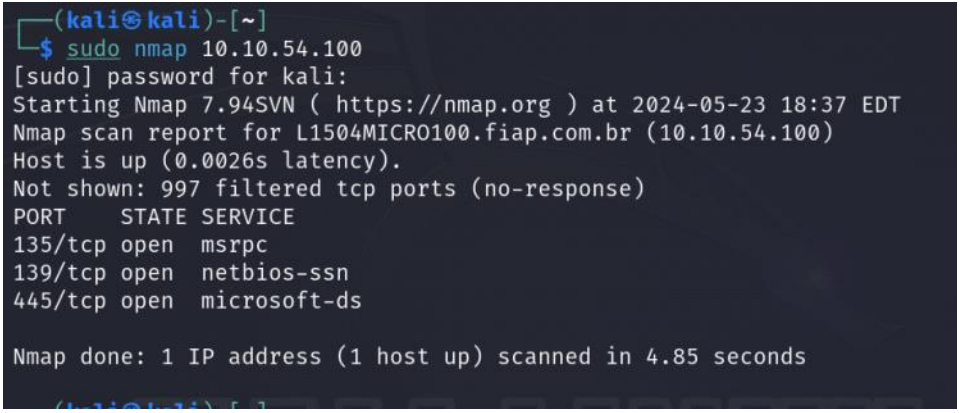
CP 03 - Hacker mindset

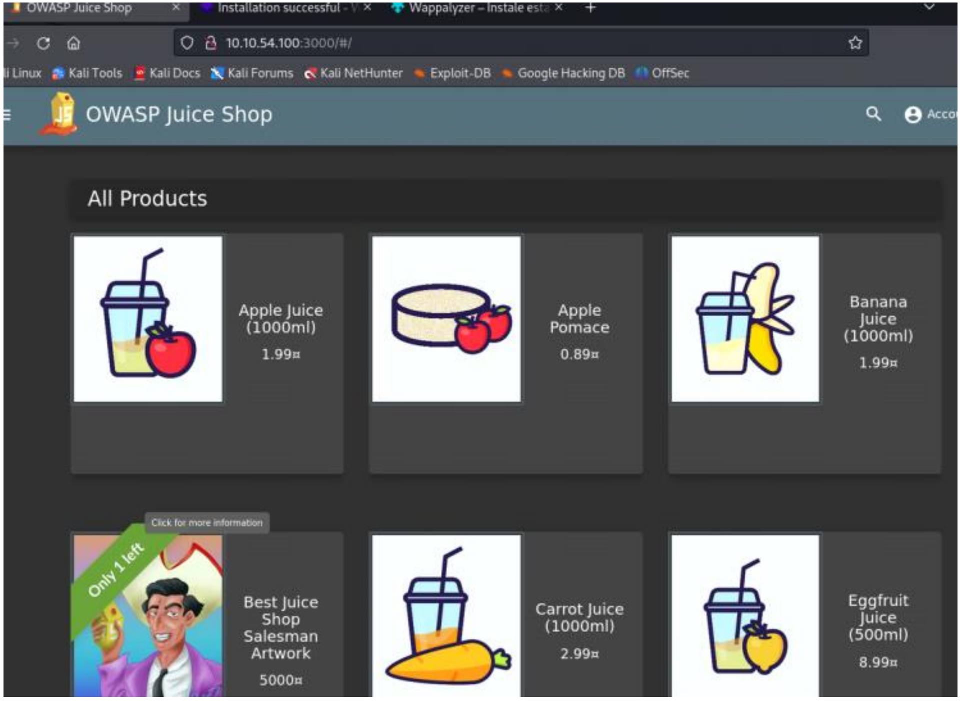
Thursday, May 23, 2024 7:27 PM

Checar portas abertas
Sudo nmap 10.10.54.100
Encontramos as seguintes portas ativas:
135/tcp
139/tcp
445/tcp
3000/tcp -



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 10.10.54.100
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 18:37 EDT
Nmap scan report for L1504MICRO100.fiap.com.br (10.10.54.100)
Host is up (0.0026s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds
```

Porta 3000 apresenta interface web:



All Products

Apple Juice (1000ml) 1.99¤

Apple Pomace 0.89¤

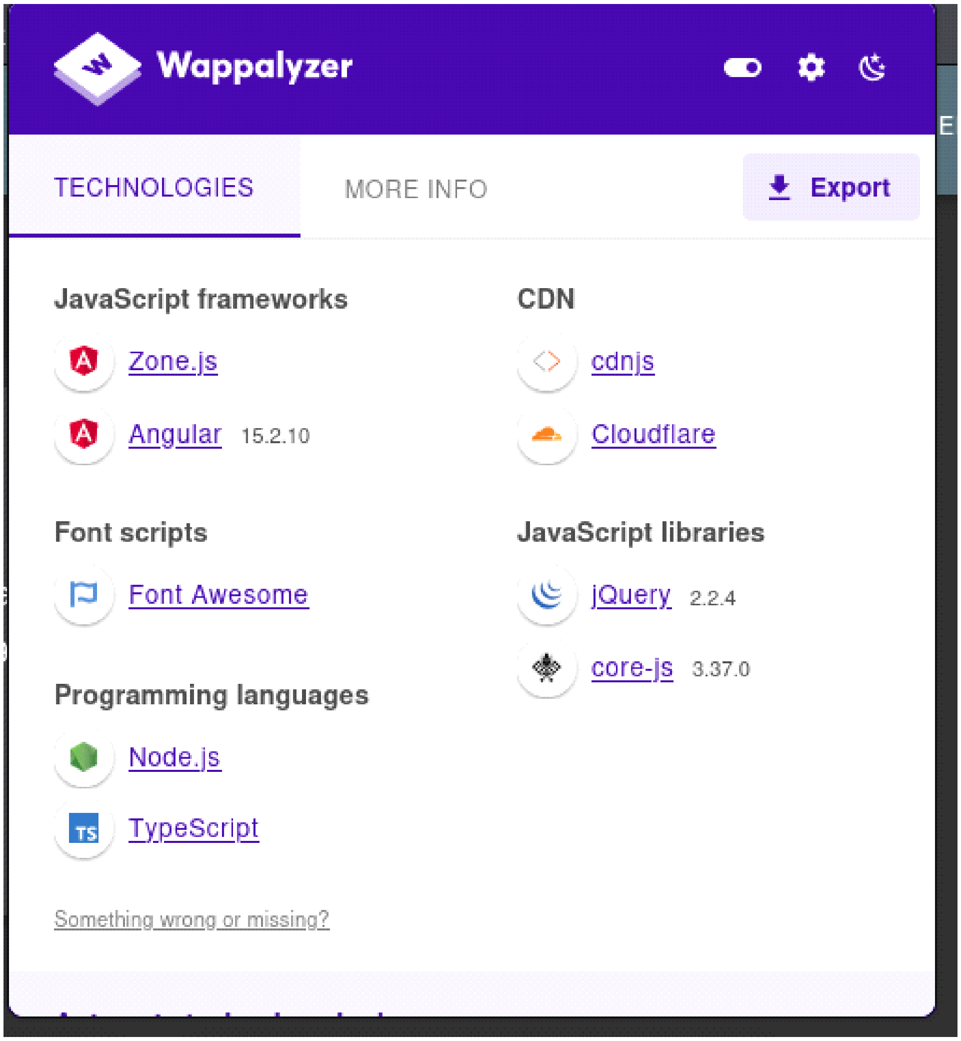
Banana Juice (1000ml) 1.99¤

Best Juice Shop Salesman Artwork 5000¤

Carrot Juice (1000ml) 2.99¤

Eggfruit Juice (500ml) 8.99¤

Ao ultilizar o Wappalyzer nós identificamos as seguintes ferramentas:



Wappalyzer

TECHNOLOGIES | MORE INFO | Export

JavaScript frameworks

- Zone.js
- Angular 15.2.10

CDN

- cdnjs
- Cloudflare

Font scripts

- Font Awesome

JavaScript libraries

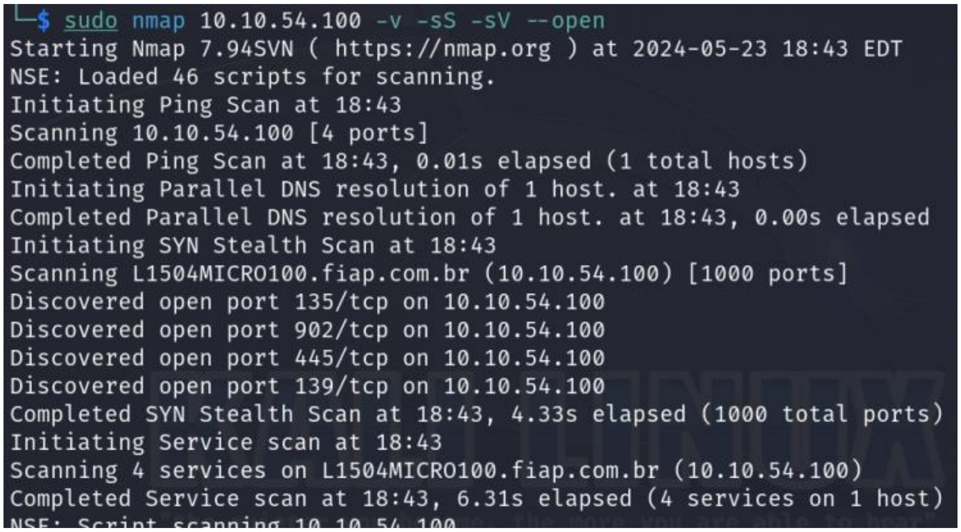
- jQuery 2.2.4
- core-js 3.37.0

Programming languages

- Node.js
- TypeScript

Something wrong or missing?

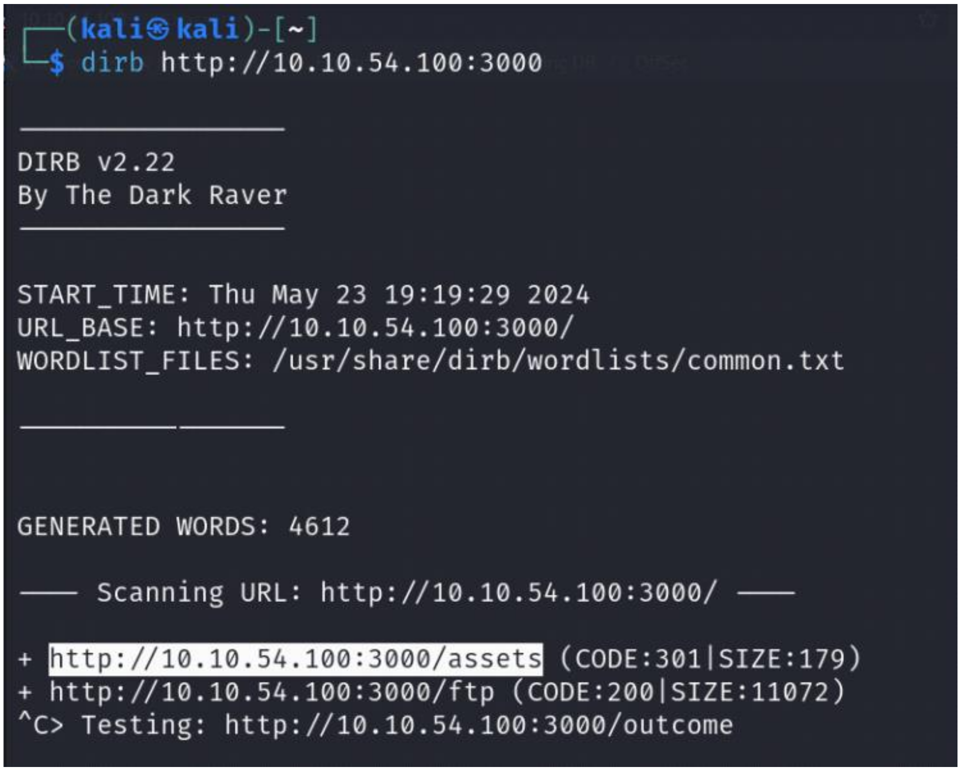
Checar versões:



```
└─$ sudo nmap 10.10.54.100 -v -sS -sV --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 18:43 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 18:43
Scanning 10.10.54.100 [4 ports]
Completed Ping Scan at 18:43, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:43
Completed Parallel DNS resolution of 1 host. at 18:43, 0.00s elapsed
Initiating SYN Stealth Scan at 18:43
Scanning L1504MICRO100.fiap.com.br (10.10.54.100) [1000 ports]
Discovered open port 135/tcp on 10.10.54.100
Discovered open port 902/tcp on 10.10.54.100
Discovered open port 445/tcp on 10.10.54.100
Discovered open port 139/tcp on 10.10.54.100
Completed SYN Stealth Scan at 18:43, 4.33s elapsed (1000 total ports)
Initiating Service scan at 18:43
Scanning 4 services on L1504MICRO100.fiap.com.br (10.10.54.100)
Completed Service scan at 18:43, 6.31s elapsed (4 services on 1 host)
NSE: Script scanning 10.10.54.100
```

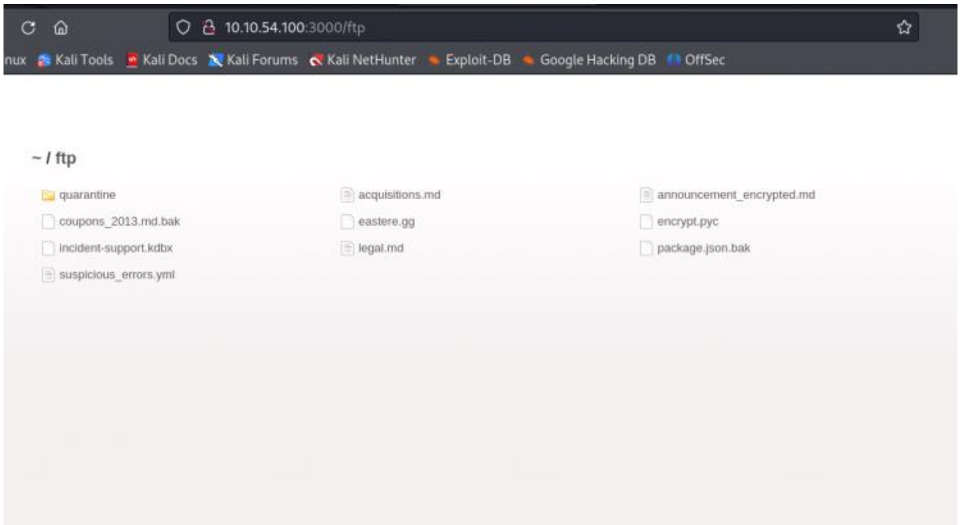
Descobrir paths no alvo usando o comando Dirb:

Encontramos duas URLs ativas:



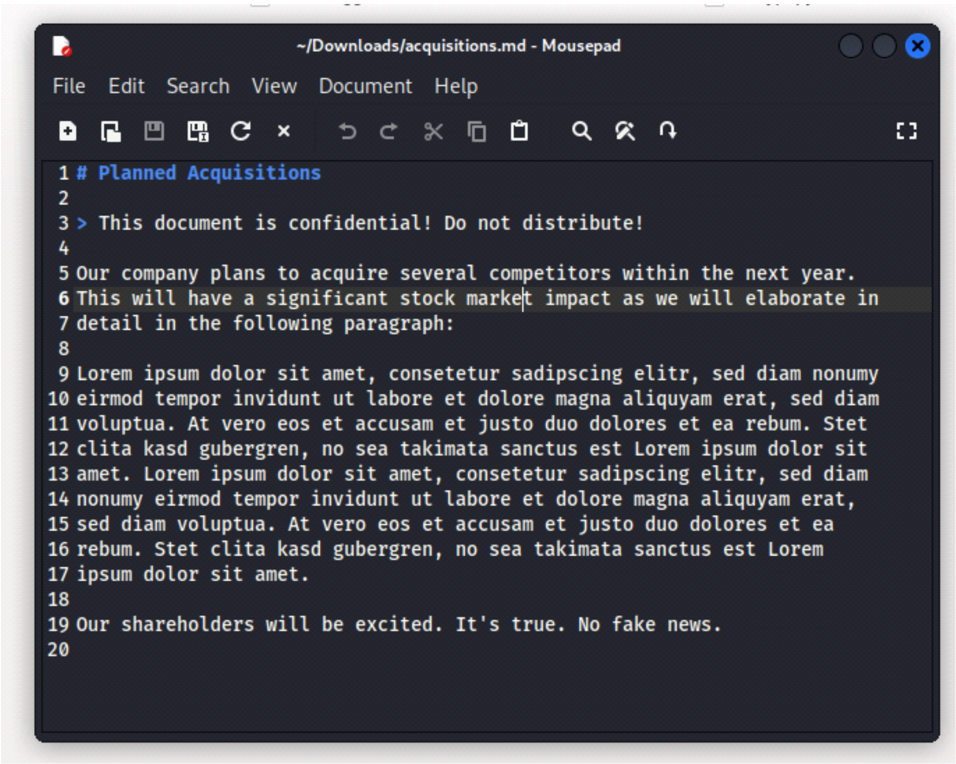
```
┌──(kali㉿kali)-[~]
└─$ dirb http://10.10.54.100:3000

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

START_TIME: Thu May 23 19:19:29 2024
URL_BASE: http://10.10.54.100:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.54.100:3000/ ----

+ http://10.10.54.100:3000/assets (CODE:301|SIZE:179)
+ http://10.10.54.100:3000/ftp (CODE:200|SIZE:11072)
^C> Testing: http://10.10.54.100:3000/outcome
```

Interface exposta:
http://10.10.54.100:3000/ftp



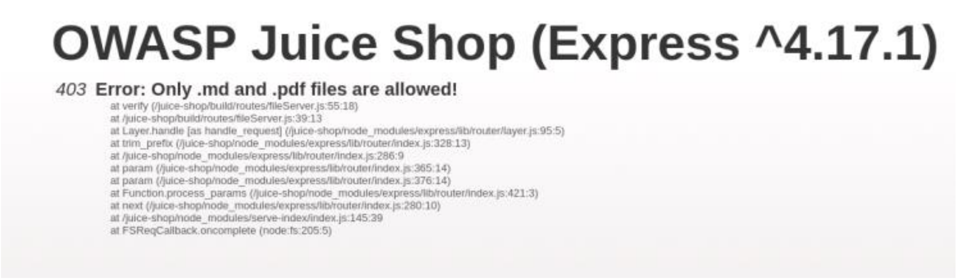
```
~ / ftp

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
```

Documento confidencial exposto encontrado no FTP*:*


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

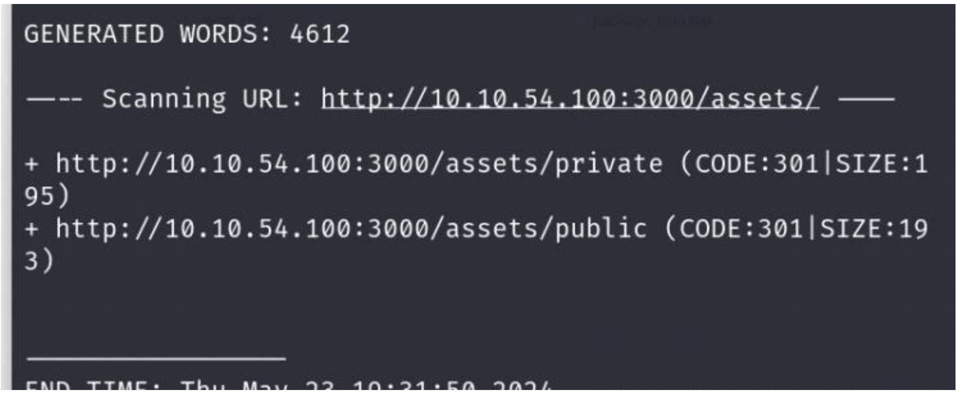
```
# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year.
This will have a significant stock market impact as we will elaborate in
detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.
```

Erro exposto não permitido:



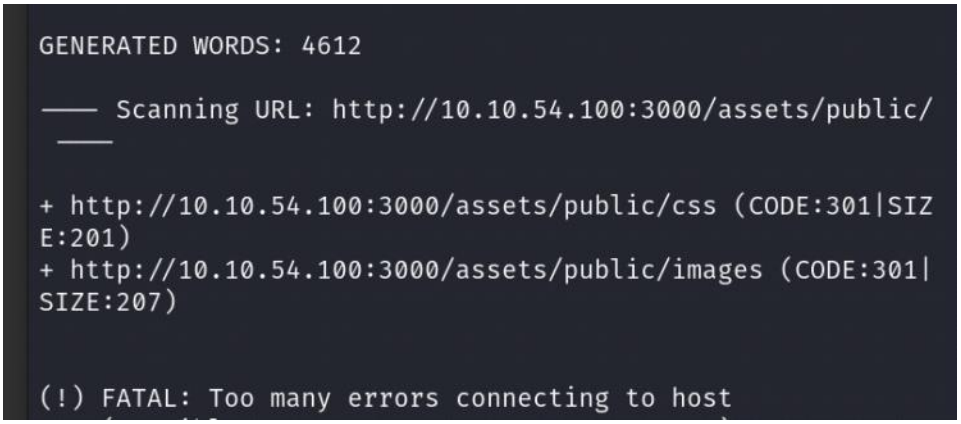
```
OWASP Juice Shop (Express ^4.17.1)

403 Error: Only .md and .pdf files are allowed!
        at verify (/juice-shop/build/routes/fileServer.js:55:18)
        at /juice-shop/build/routes/fileServer.js:39:13
        at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
        at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)
        at /juice-shop/node_modules/express/lib/router/index.js:286:9
        at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
        at param (/juice-shop/node_modules/express/lib/router/index.js:376:14)
        at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:421:3)
        at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)
        at /juice-shop/node_modules/serve-index/index.js:145:39
        at FSReqCallback.oncomplete (node:fs:205:5)
```

Na /assets, ao colocarmos na web não encontramos uma interface exposta.
Ao usarmos o comando Dirb na /assets encontramos 2 URLs ativas também:



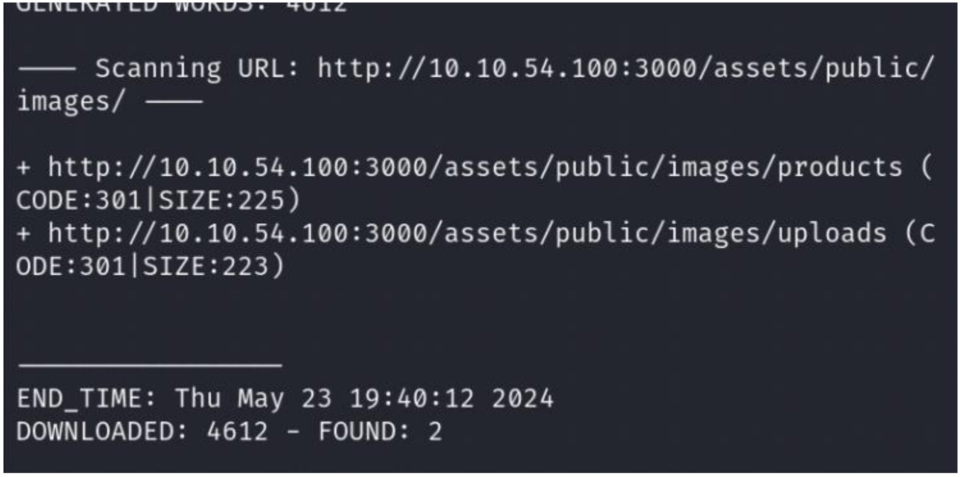
```
GENERATED WORDS: 4612

---- Scanning URL: http://10.10.54.100:3000/assets/ ----

+ http://10.10.54.100:3000/assets/private (CODE:301|SIZE:1
95)
+ http://10.10.54.100:3000/assets/public (CODE:301|SIZE:19
3)


-----------------
END TIME: Thu May 23 10:31:50 2024
```

Mas nenhuma das duas não estão mostrando interfaces expostas também.
Na /private não possui direcionamentos.
Na /public encontramos dois direcionamentos:



```
GENERATED WORDS: 4612

---- Scanning URL: http://10.10.54.100:3000/assets/public/
 ----

+ http://10.10.54.100:3000/assets/public/css (CODE:301|SIZ
E:201)
+ http://10.10.54.100:3000/assets/public/images (CODE:301|
SIZE:207)


(!) FATAL: Too many errors connecting to host
```

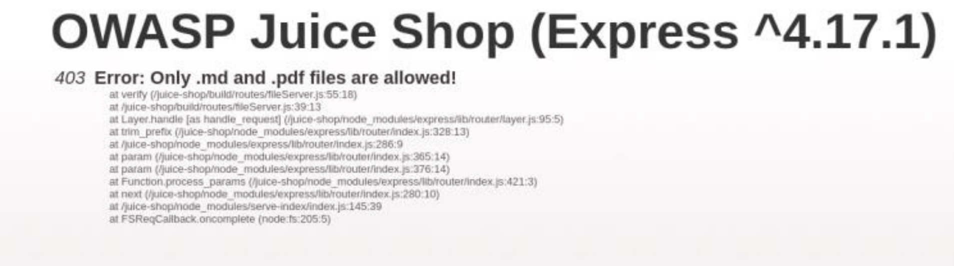
Dentro da /images encontramos dois direcionamentos também:



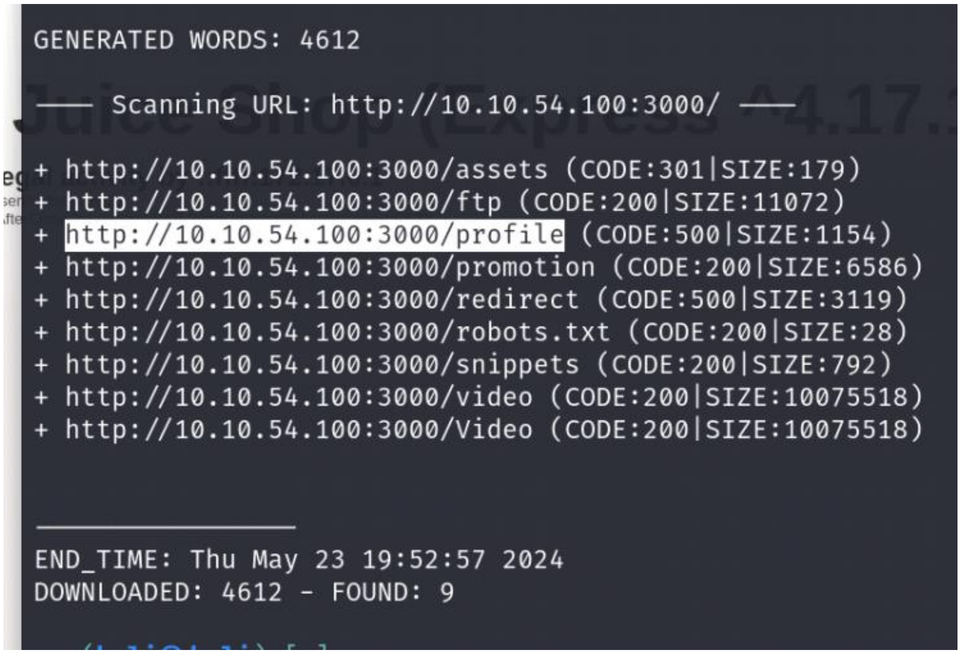
```
---- Scanning URL: http://10.10.54.100:3000/assets/public/
images/ ----

+ http://10.10.54.100:3000/assets/public/images/products (
CODE:301|SIZE:225)
+ http://10.10.54.100:3000/assets/public/images/uploads (C
ODE:301|SIZE:223)


-----------------
END_TIME: Thu May 23 19:40:12 2024
DOWNLOADED: 4612 - FOUND: 2
```

Mas nenhuma das duas não estão mostrando interfaces expostas também.

Descobrir paths no alvo usando o comando Dirb com o -404:

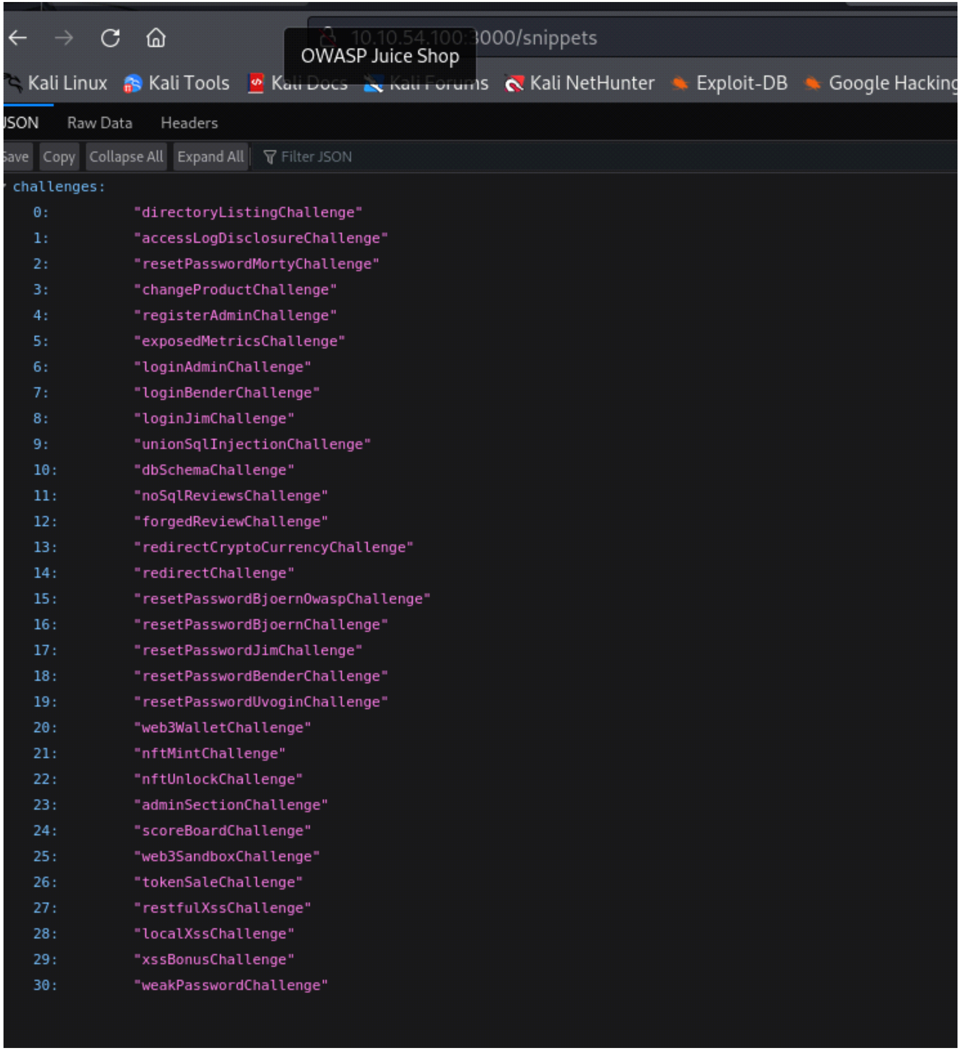


```
OWASP Juice Shop (Express ^4.17.1)

403 Error: Only .md and .pdf files are allowed!
    at verify (/juice-shop/build/routes/fileServer.js:55:18)
    at /juice-shop/build/routes/fileServer.js:39:13
    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)
    at /juice-shop/node_modules/express/lib/router/index.js:286:9
    at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
    at param (/juice-shop/node_modules/express/lib/router/index.js:376:14)
    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:421:3)
    at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)
    at /juice-shop/node_modules/serve-index/index.js:145:39
    at FSReqCallback.oncomplete (node:fs:205:5)
```



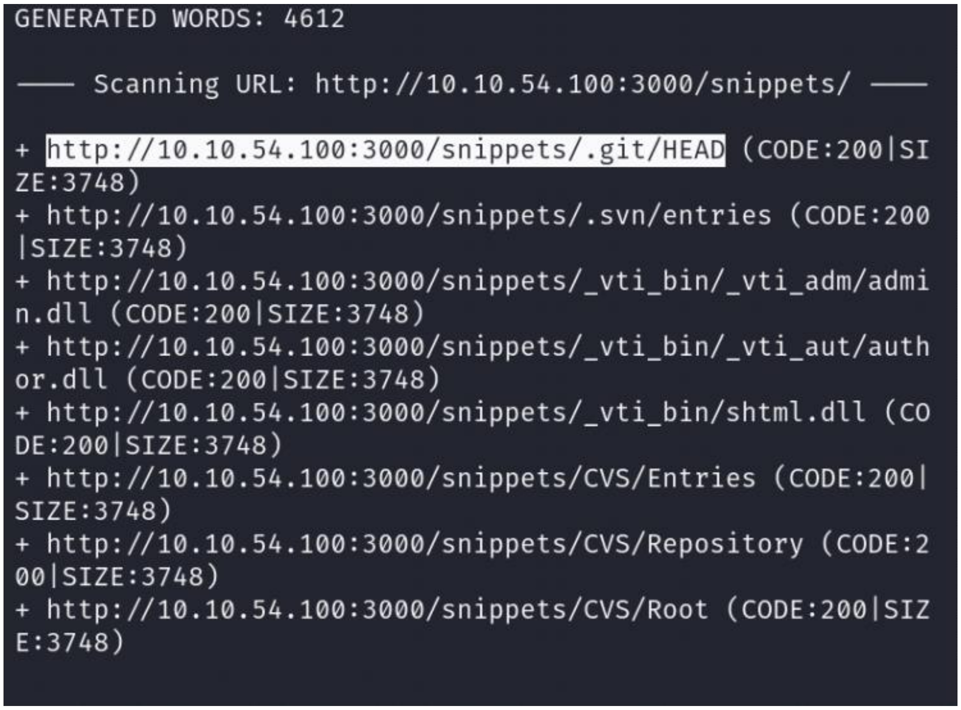
```
GENERATED WORDS: 4612

---- Scanning URL: http://10.10.54.100:3000/ ----
+ http://10.10.54.100:3000/assets (CODE:301|SIZE:179)
+ http://10.10.54.100:3000/ftp (CODE:200|SIZE:11072)
+ http://10.10.54.100:3000/profile (CODE:500|SIZE:1154)
+ http://10.10.54.100:3000/promotion (CODE:200|SIZE:6586)
+ http://10.10.54.100:3000/redirect (CODE:500|SIZE:3119)
+ http://10.10.54.100:3000/robots.txt (CODE:200|SIZE:28)
+ http://10.10.54.100:3000/snippets (CODE:200|SIZE:792)
+ http://10.10.54.100:3000/video (CODE:200|SIZE:10075518)
+ http://10.10.54.100:3000/Video (CODE:200|SIZE:10075518)

-----------------
END_TIME: Thu May 23 19:52:57 2024
DOWNLOADED: 4612 - FOUND: 9
```

Na /snippets encontramos uma página proíbida:



```
challenges:
  0:    "directoryListingChallenge"
  1:    "accessLogDisclosureChallenge"
  2:    "resetPasswordMortyChallenge"
  3:    "changeProductChallenge"
  4:    "registerAdminChallenge"
  5:    "exposedMetricsChallenge"
  6:    "loginAdminChallenge"
  7:    "loginBenderChallenge"
  8:    "loginJimChallenge"
  9:    "unionSqlInjectionChallenge"
  10:   "dbSchemaChallenge"
  11:   "noSqlReviewsChallenge"
  12:   "forgedReviewChallenge"
  13:   "redirectCryptoCurrencyChallenge"
  14:   "redirectChallenge"
  15:   "resetPasswordBjoernOwaspChallenge"
  16:   "resetPasswordBjoernChallenge"
  17:   "resetPasswordJimChallenge"
  18:   "resetPasswordBenderChallenge"
  19:   "resetPasswordUvoginChallenge"
  20:   "web3WalletChallenge"
  21:   "nftMintChallenge"
  22:   "nftUnlockChallenge"
  23:   "adminSectionChallenge"
  24:   "scoreBoardChallenge"
  25:   "web3SandboxChallenge"
  26:   "tokenSaleChallenge"
  27:   "restfulXssChallenge"
  28:   "localXssChallenge"
  29:   "xssBonusChallenge"
  30:   "weakPasswordChallenge"
```

E dentro de /snippets encontramos essas URLs ativas:



```
GENERATED WORDS: 4612

---- Scanning URL: http://10.10.54.100:3000/snippets/ ----

+ http://10.10.54.100:3000/snippets/.git/HEAD (CODE:200|SI
ZE:3748)
+ http://10.10.54.100:3000/snippets/.svn/entries (CODE:200
|SIZE:3748)
+ http://10.10.54.100:3000/snippets/_vti_bin/_vti_adm/admi
n.dll (CODE:200|SIZE:3748)
+ http://10.10.54.100:3000/snippets/_vti_bin/_vti_aut/auth
or.dll (CODE:200|SIZE:3748)
+ http://10.10.54.100:3000/snippets/_vti_bin/shtml.dll (CO
DE:200|SIZE:3748)
+ http://10.10.54.100:3000/snippets/CVS/Entries (CODE:200|
SIZE:3748)
+ http://10.10.54.100:3000/snippets/CVS/Repository (CODE:2
00|SIZE:3748)
+ http://10.10.54.100:3000/snippets/CVS/Root (CODE:200|SIZ
E:3748)
```