

# GitLab 任意文件读取漏洞复现

## 漏洞介绍

GitLab 是一个用于仓库管理系统的开源项目，使用 Git 作为代码管理工具，并在此基础上搭建起来的 web 服务。GitLab 是由 GitLabInc. 开发，使用 MIT 许可证的基于网络的 Git 仓库管理工具，且具有 wiki 和 issue 跟踪功能。

在 Gitlab 8.5–12.9 版本中，存在一处任意文件读取漏洞，攻击者可以利用该漏洞，在不需要特权的状态下，读取任意文件，造成严重信息泄露，从而导致进一步被攻击的风险。

## 漏洞编号

CVE-2020-10977

## CVSS 评分 / 漏洞等级

5.5 / 中危

## 漏洞影响范围

GitLab GitLab CE/EE  $\geq 8.5$  and  $\leq 12.9$

## 环境搭建

以在 Centos 7 环境中安装为例：

参考地址：<https://mirrors.tuna.tsinghua.edu.cn/help/gitlab-ce/>

在 / etc/yum.repos.d / 目录下新建 gitlab-ce.repo，内容为：

```
[gitlab-ce]
```

```
name=GitLab CE Repository
```

```
name=GitLab CE Repository
baseurl=https://mirrors.tuna.tsinghua.edu.cn/gitlab-ce/yum/el$releasever/
gpgcheck=0
enabled=1
```

在执行

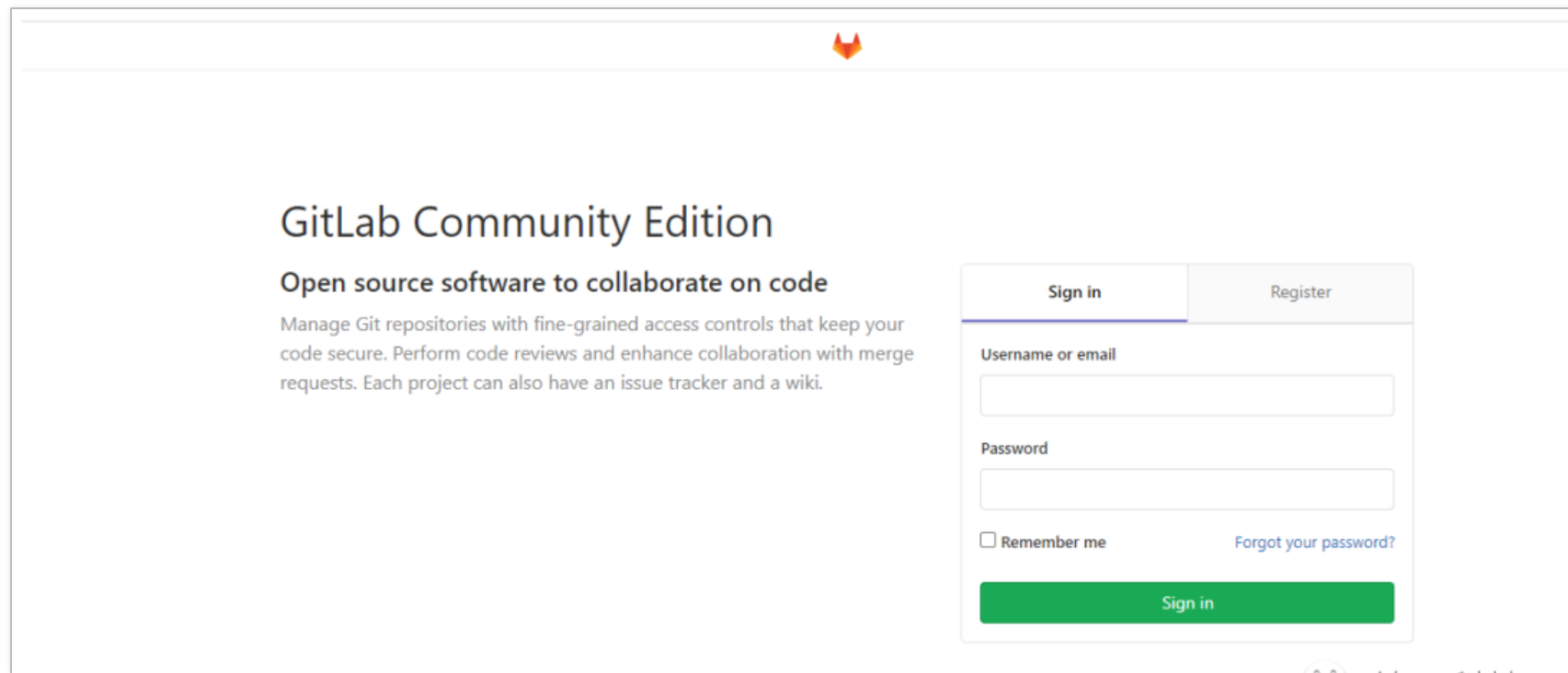
```
yum makecache
yum install gitlab-ce-12.8.7-ce.0.el7
```

在执行完成后，修改 / etc/gitlab/gitlab.rb 文件：

注释掉 `external_url 'http://gitlab.example.com'`

为什么要注释呢，不注释的话，后面只能用这里的域名访问，需要设置 hosts，用 IP 访问会有问题，为了方便，所以注释掉这一行。

保存退出后，使用命令 `gitlab-ctl reconfigure` 来进行安装，等待安装完成，完成后直接访问 IP 地址即可。



随便注册一个账号，然后登录。

## 漏洞复现

随便注册一个账号，然后登录。



在这里创建两个 project，名字随意。

Blank projectCreate from templateImport project

Project name

project1

Project URL

http://10.0.0.5/test/

Project slug

project1

Want to house several dependent projects under the same namespace? [Create a group.](#)

Project description (optional)

Description format

Visibility Level ?

☒ Private

Project access must be granted explicitly to each user.

☐ Internal

The project can be accessed by any logged in user.

☐ Public

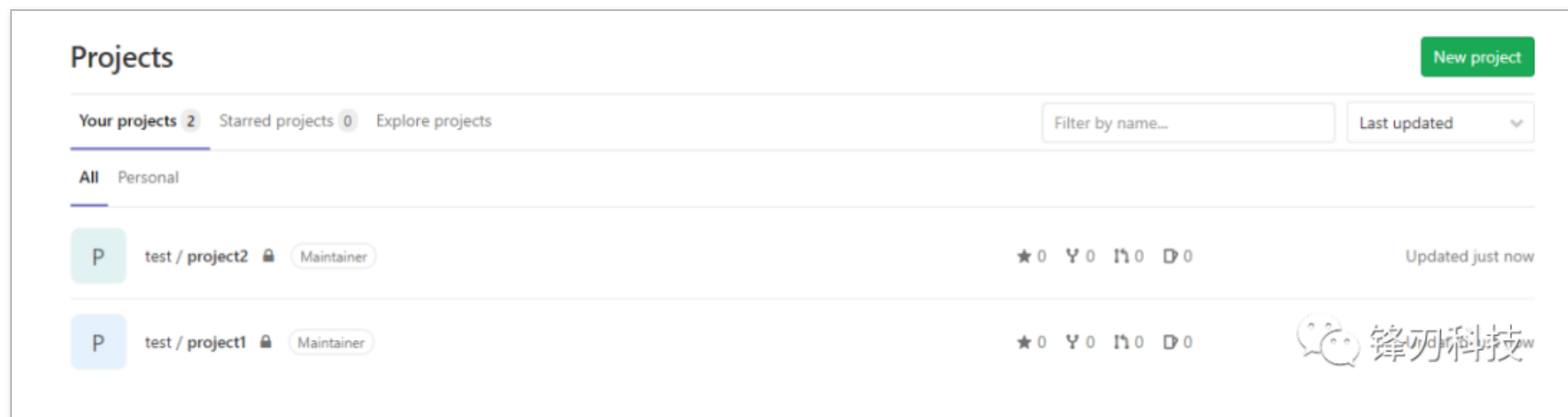
The project can be accessed without any authentication.

☐ Initialize repository with a README

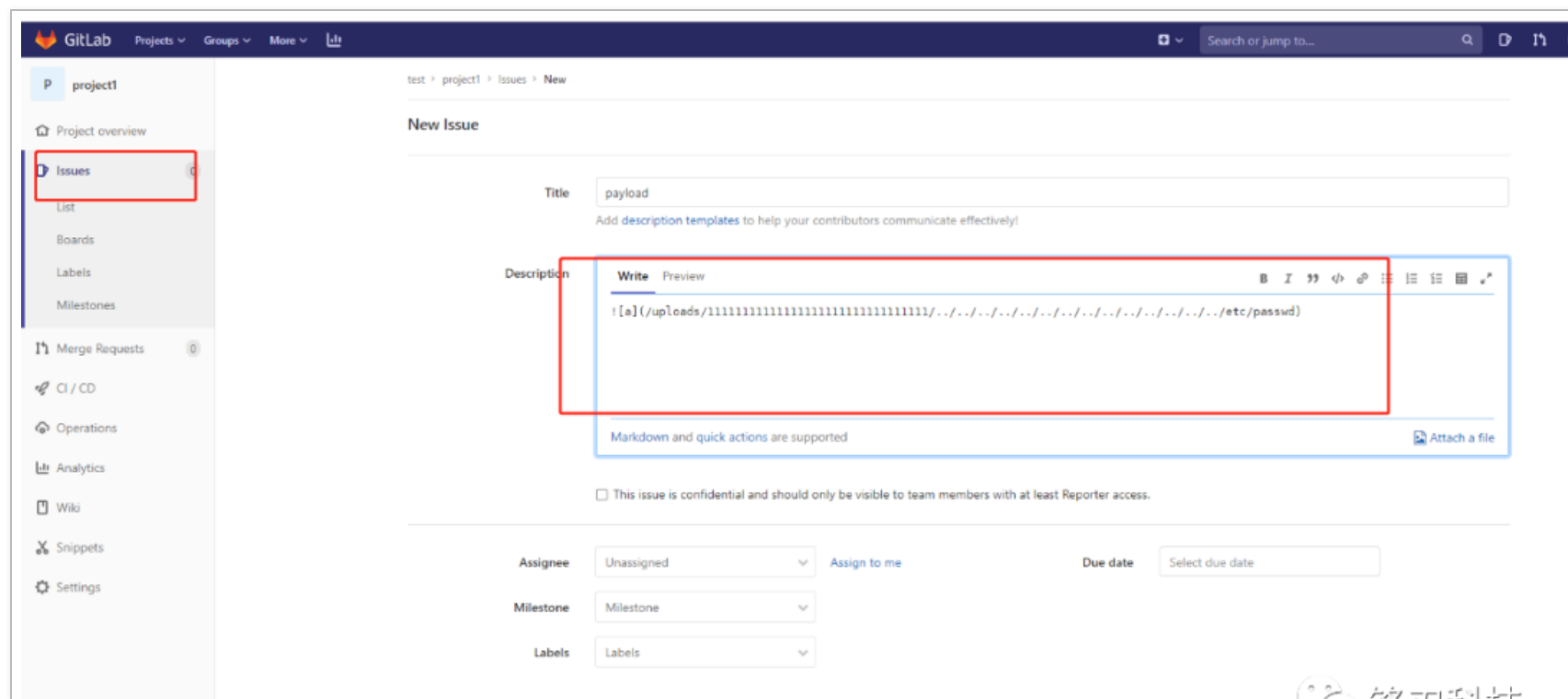
Allows you to immediately clone this project's repository. Skip this if you plan to push up an existing repository.

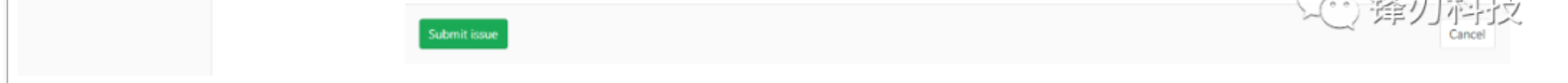
Create project

Cancel

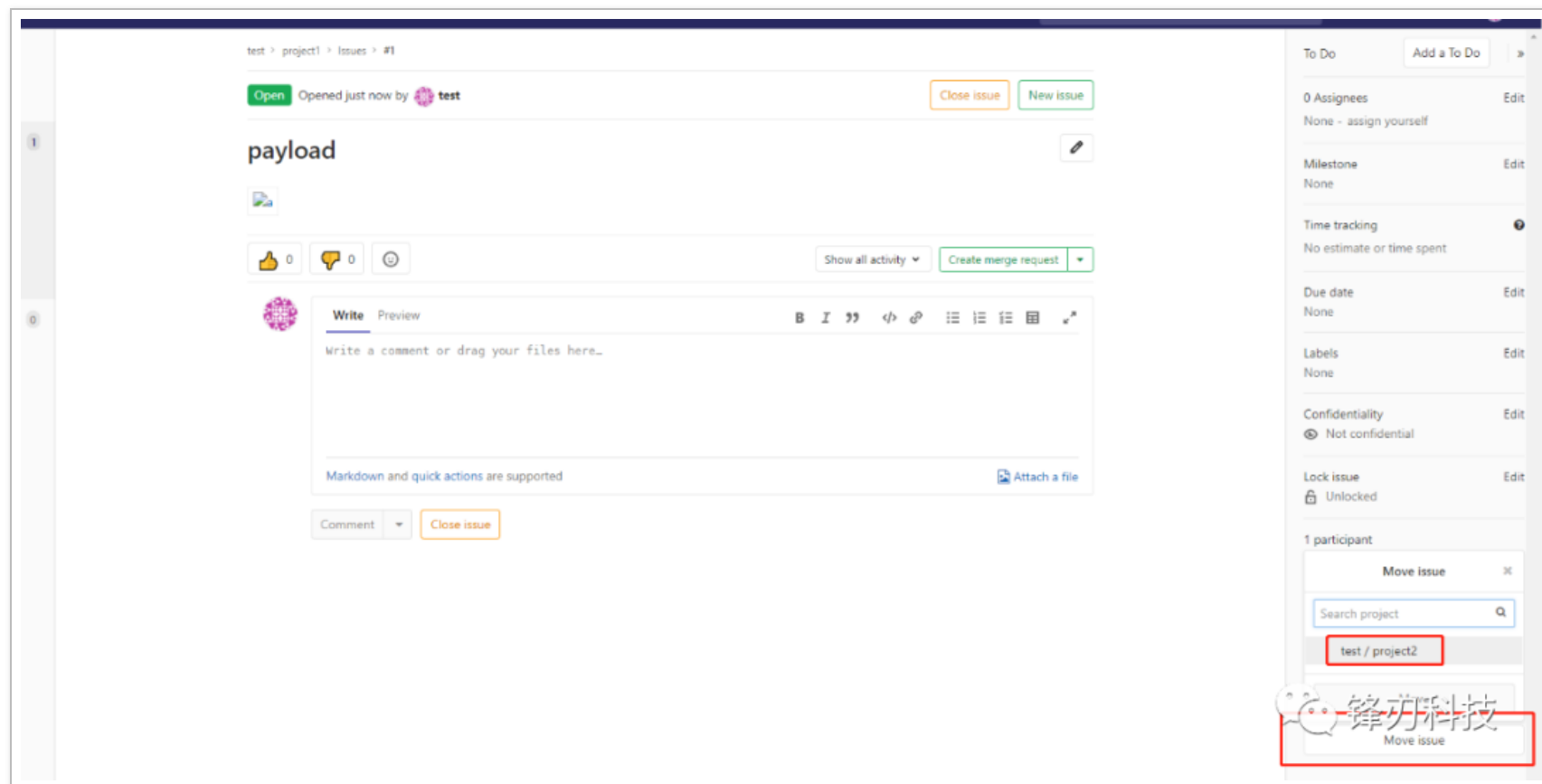


两个 project 创建完成后，在 project1 中创建一个 issues。内容为 POC 内容：





提交后，将这个创建好的 issues move 到前面创建好的 project2 中。



MOVE 完成后，从 project2 中就可以看到 passwd 文件的连接地址，可以直接点击下载。

- project2
- Project overview
- Issues 1
  - List
  - Boards
  - Labels
  - Milestones
- Merge Requests 0
- CI / CD
- Operations
- Analytics
- Wiki
- Snippets
- Settings

test > project2 > Issues > #1

Open Opened 1 minute ago by test

## payload

passwd

0 0

Show all activity

test @test moved from project1#1 (moved) just now



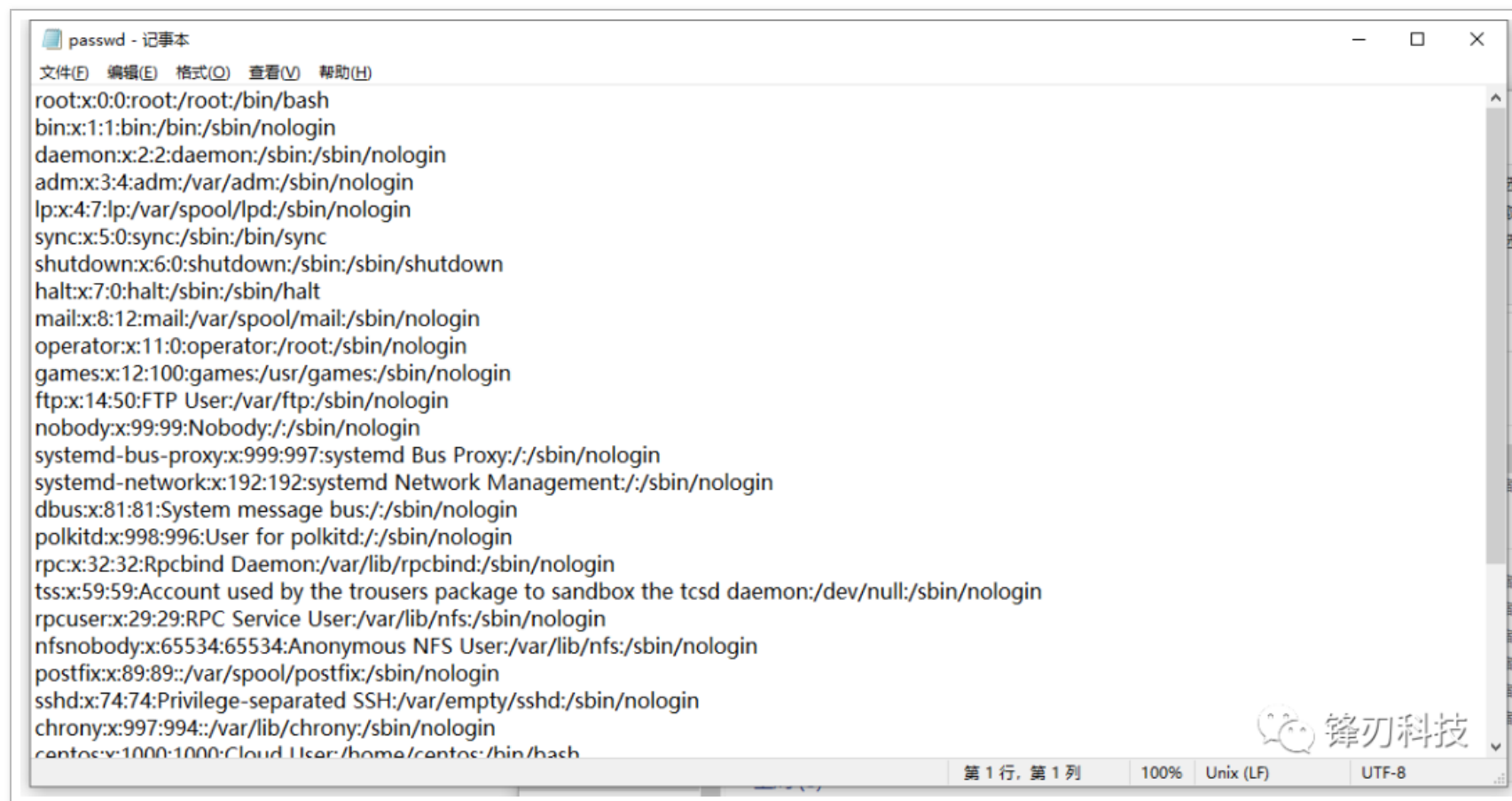
Write Preview B I " </>

Write a comment or drag your files here...

Markdown and quick actions are supported

Comment Close issue

然后打开下载的 passwd，可以看到读取到了 passwd 的文件内容。



```
passwd - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:./:/sbin/nologin
systemd-bus-proxy:x:999:997:systemd Bus Proxy:./:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:./:/sbin/nologin
dbus:x:81:81:System message bus:./:/sbin/nologin
polkitd:x:998:996:User for polkitd:./:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
postfix:x:89:89:./var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
chrony:x:997:994:./var/lib/chrony:/sbin/nologin
centos:x:1000:1000:Cloud User:/home/centos:/bin/bash
```

## 安全防护

升级最新版的 gitlab 系统，可以直接使用 yum install 来安装指定的版本。

也可以上官网下载想要的版本进行安装使用：

地址：<https://packages.gitlab.com/gitlab/gitlab-ce>



