**GitLab任意文件读取**

**漏洞复现(CVE-2020-10977)**

(By Jean)

目录

[1. 漏洞描述 2](#_Toc28622)

[2. 影响范围 2](#_Toc8090)

[3. 环境部署 2](#_Toc6733)

[3.1. Centos7.6安装GitLab 2](#_Toc22942)

[4. 漏洞复现 3](#_Toc25694)

[4.1. 查看版本 3](#_Toc9519)

[4.2. 用户创建 4](#_Toc19962)

[4.3. issues创建 4](#_Toc9874)

[4.4. 任意文件读取 5](#_Toc9682)

[5. 修复建议 6](#_Toc18215)

[6. 参考 6](#_Toc5975)

# 漏洞描述

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。

# 影响范围

GitLab GitLab EE >=8.5，<=12.9  
GitLab GitLab CE >=8.5，<=12.9

# 环境部署

|  |  |  |
| --- | --- | --- |
| **主机** | **操作系统** | **IP** |
| 靶机 | Centos7 | 192.168.42.128 |
|  |  |  |

## Centos7.6安装GitLab

操作系统版本：CentOS Linux release 7.6.1810 (Core)

新建 /etc/yum.repos.d/gitlab-ce.repo，内容为

[gitlab-ce]

name=Gitlab CE Repository

baseurl=https://mirrors.tuna.tsinghua.edu.cn/gitlab-ce/yum/el$releasever/

gpgcheck=0

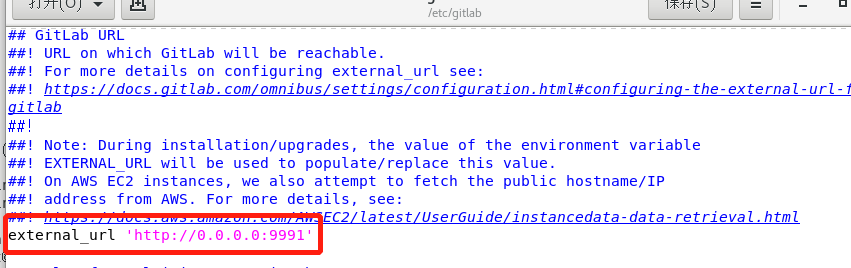
enabled=1

再执行

yum makecache

yum -y install gitlab-ce-12.8.7-ce.0.el7

在执行完成后，修改/etc/gitlab/gitlab.rb文件：



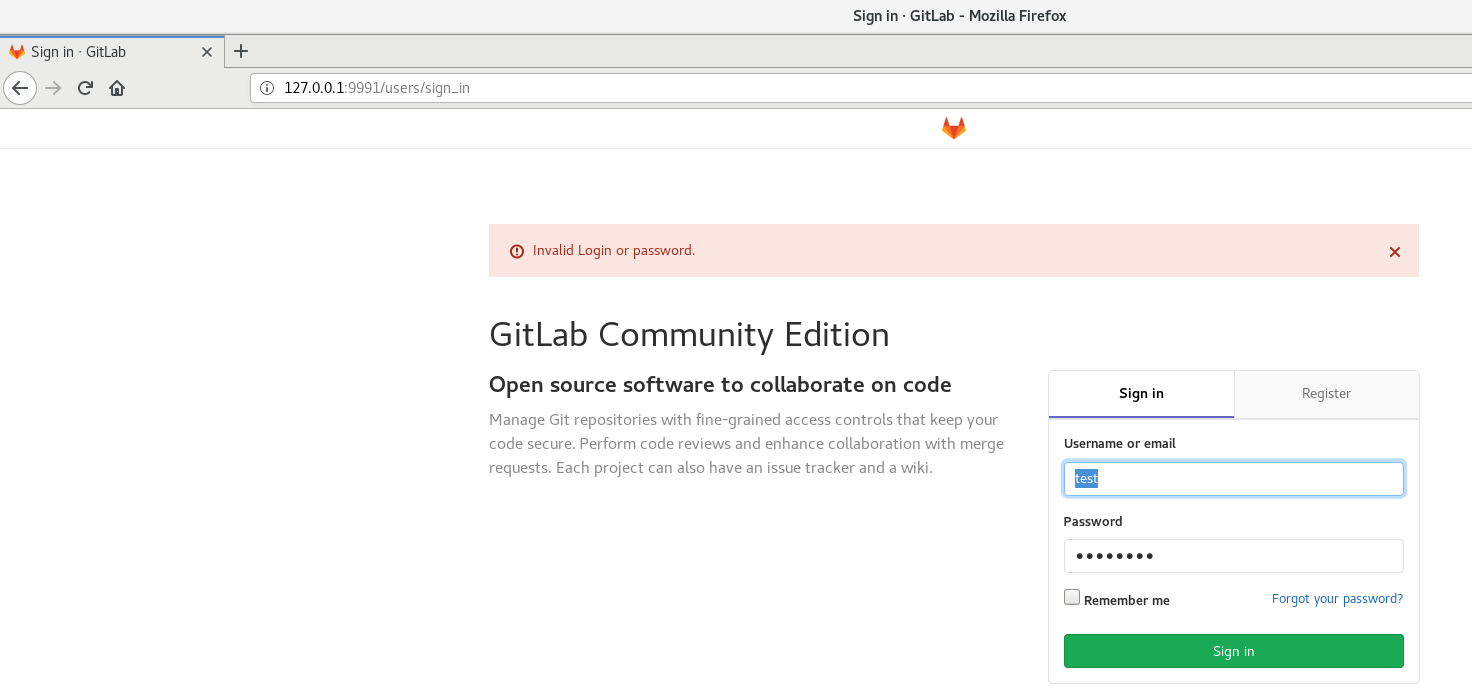
然后gitlab-ctl reconfigure 重新载入配置文件。

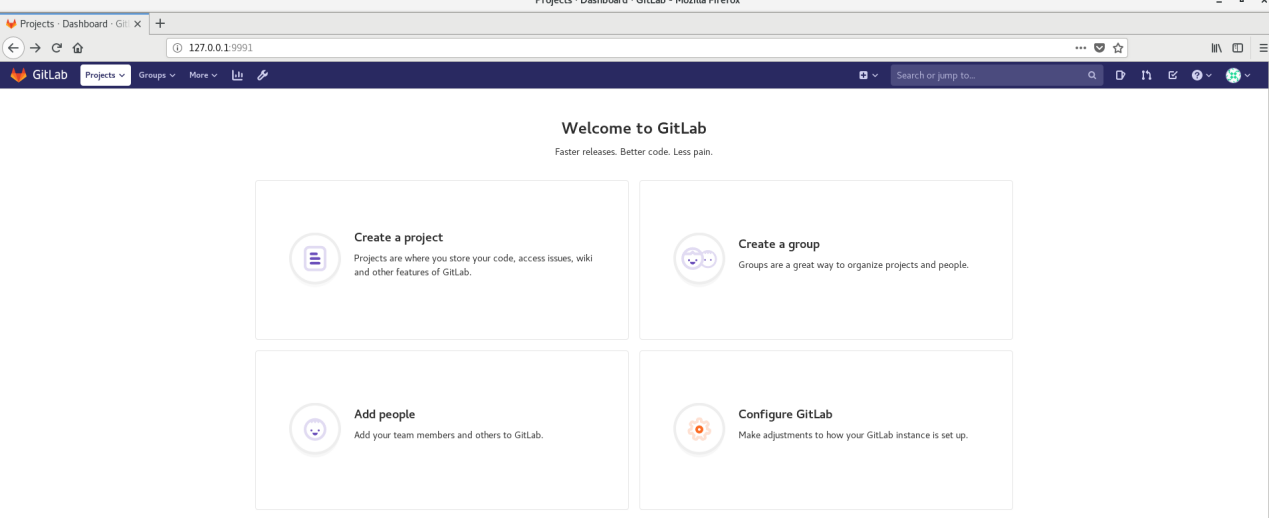
# 漏洞复现

## 查看版本

cat /opt/gitlab/embedded/service/gitlab-rails/VERSION





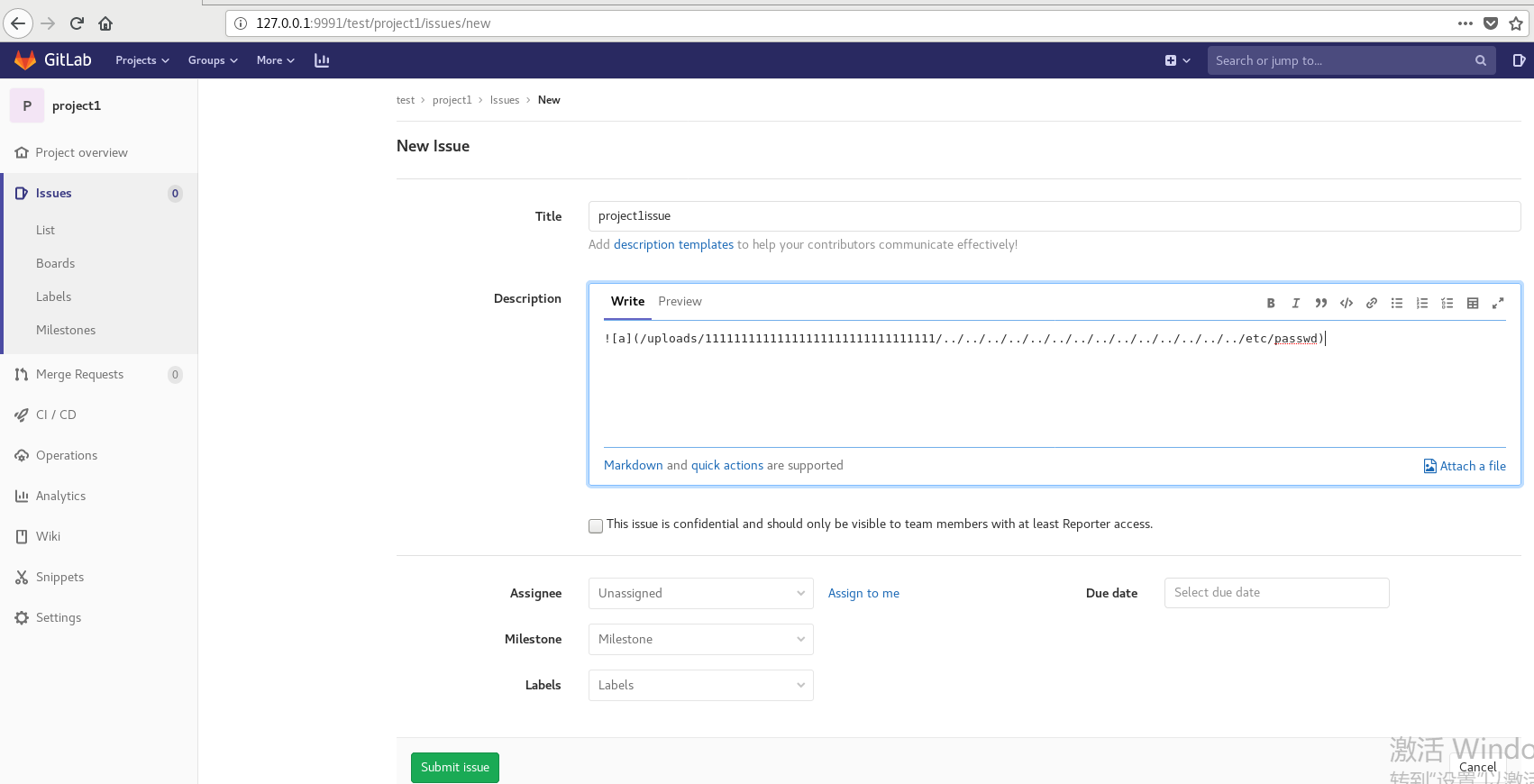


## 用户创建

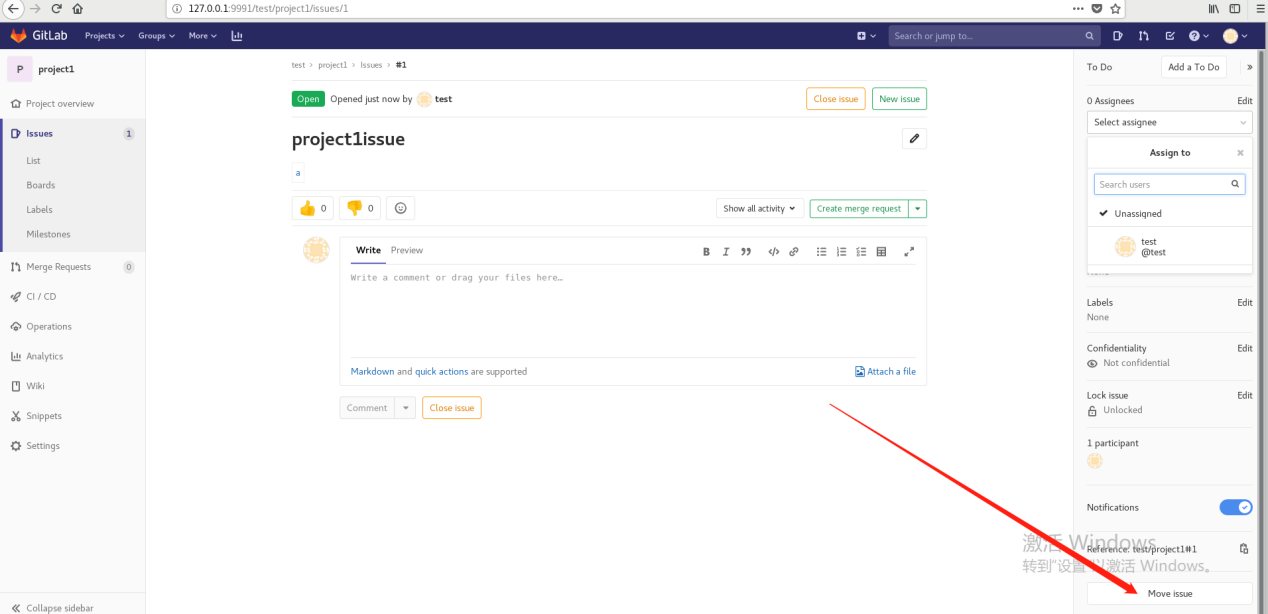
建一个普通用户test，然后使用test建立两个project

## issues创建

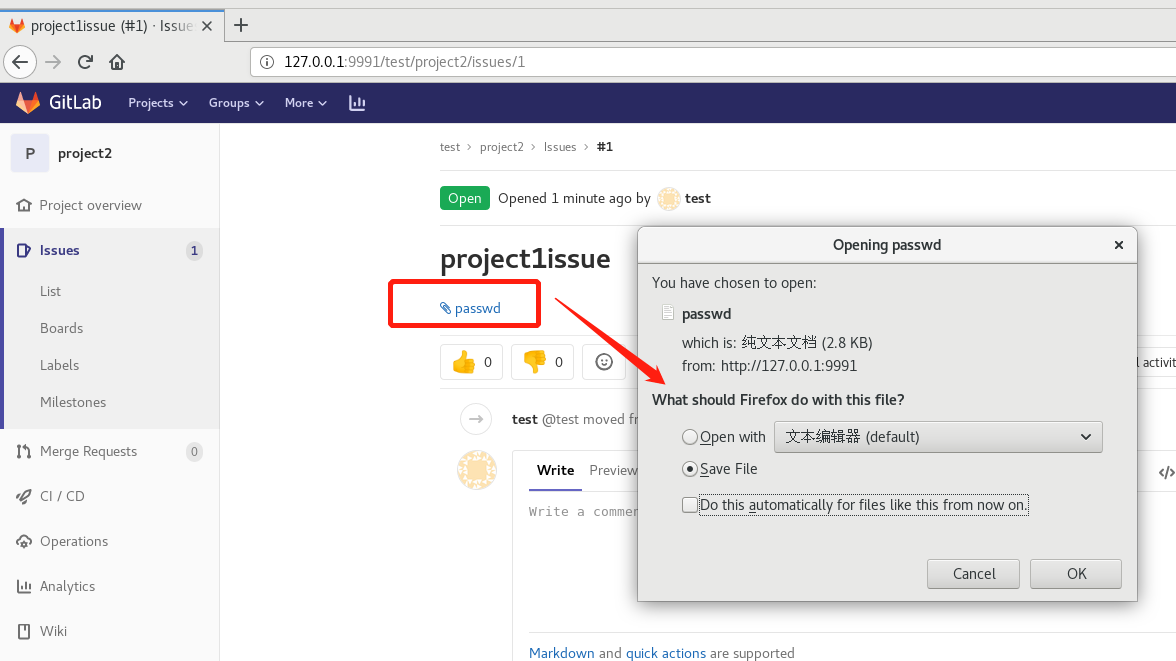
然后在project1中创建一个issues



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

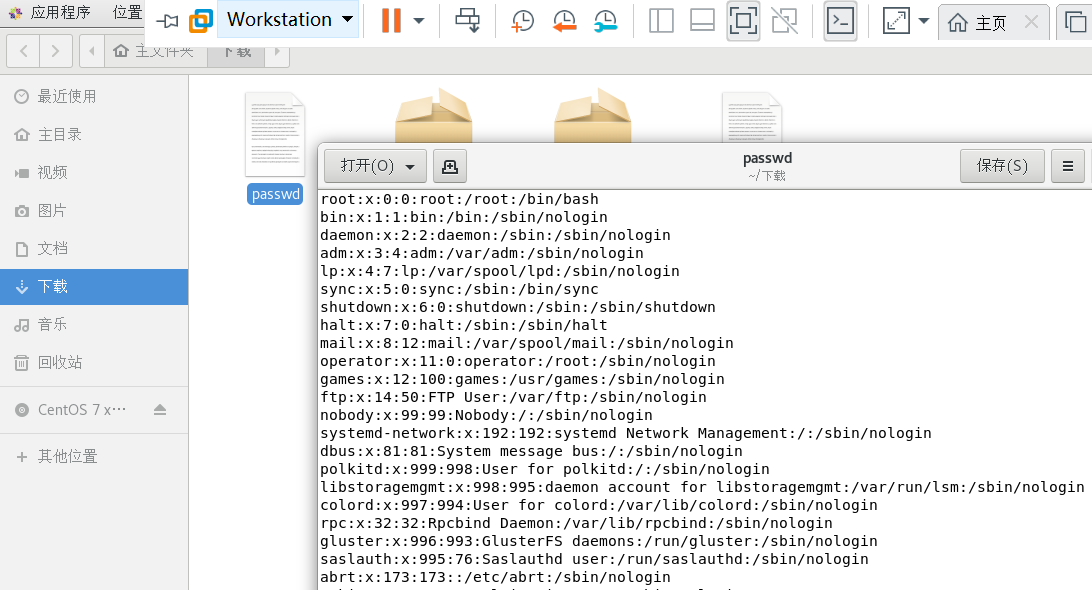


MOVE完成后，从project2中就可以看到passwd文件的链接地址，可以直接点击下载：



## 任意文件读取

查看下载的文件（成功读取/etc/passwd文件内容）：



# 修复建议

升级最新版的gitlab系统

# 参考

<https://idc.wanyunshuju.com/aqld/1892.html>