main

Trendnet_TW100-S4W1CA / writeup_XSS.txt

Galapag0s Update and rename writeup.txt to writeup_XSS.txt History

1 contributor

12 lines (6 sloc) | 634 Bytes

```
1  XSS VULNERABILITY
2
3  While observing traffic sent to the “cli.cgi” file, I found it was possible to inject arbitrary JavaScript into the router's web interface via the "echo" command. The below URL fur
4
5  PAYLOAD
6
7  http://192.168.10.1/cli.cgi?cmd=echo%20%3Cscript%3Ealert(1)%3C/script%3E%;
8
9  If the above URL was loaded by a logged in user, either through a phishing attack, or some other vector, a threat actor could execute arbitrary JavaScript in the user's browser, Th
10
11 To remediate this, input echoed back to the user should be escaped.
12
```