

main

...

opencats_zero-days / XSS_in_callback.md



hansmach1ne Update XSS_in_callback.md

History

1 contributor



12 lines (6 sloc) | 460 Bytes

...

Cross Site Scripting vulnerability in the OpenCats 'callback'.

OpenCats version 0.9.6 PHP7.2 suffers from reflected XSS vulnerability. This allows attackers arbitrary JavaScript injection, which compromises secure session between client and server.

PoC

```
GET /index.php?m=toolbar&callback=<script>alert`xss`</script>&a=authenticate
```

