

[New issue](#)[Jump to bottom](#)

XSS Vulnerability in "type" parameter #210

🔒 Closed

xoffense opened this issue on Mar 19, 2021 · 0 comments

Assignees



Milestone

🏷 Seo panel 4.9.0

xoffense commented on Mar 19, 2021 • edited

Hi team,

I would like to report XSS vulnerability.

Description

A cross-site scripting (XSS) issue in the SEO admin login panel version 4.8.0 allows remote attackers to inject JavaScript via the "redirect" parameter.

XSS Payload: 1"autofocus onfocus=alert(1) //"**Vulnerable parameter:** type

Steps to Reproduce the Issue:

1- Login to SEO admin panel

2- Paste below POC:

```
https://localhost/seopanel/archive.php?from_time=2021-03-18&order_col=followers&order_val=ASC&report_type=social-media-reports&search_name=&sec=reportSummary&to_time=2021-03-19&type=1"autofocus onfocus=alert(1) //"&website_id=0
```

As you can see, XSS is triggered and can send cookies to attacker.

Video POC: <https://drive.google.com/file/d/1d0TcAaax4Rfp1yKrqxhAY9W2pLtiXug/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 takeover and download a malware on their system, and there are many more attacking scenarios a skilled attacker can perform with xss.

sendtogo pushed a commit that referenced this issue on Mar 22, 2021

fix for #210

f72683a

sendtogo self-assigned this on Mar 22, 2021

 sendtogo added this to the **Seo panel 4.9.0** milestone on Mar 22, 2021

sendtogo closed this as completed on Mar 22, 2021

Assignees

sendtogo

Labels

None yet

Projects

None yet

Milestone

Seo panel 4.9.0

Development

No branches or pull requests

2 participants

