New issue   Jump to bottom

XSS Vulnerability in "to_time" parameter #211

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

Assignees	🚍
Milestone	⬡ Seo panel 4.9.0

---

xoffense commented on Mar 19, 2021

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: 2021-03-17"autofocus onfocus=alert(1) //"

Vulnerable parameter: to_time

Steps to Reproduce the Issue:

1- Login to SEO admin panel
2- Paste below POC:

```
https://localhost/seopanel/webmaster-tools.php?fromPopUp=1&from_time=2021-03-02&rep=1&sec=viewWebsiteSearchReports&to_time=2021-03-17"autofocus onfocus=alert(1) //"&website_id=1
```

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

Video POC: https://drive.google.com/file/d/1EXu6uO7TOJLlaLbLpjuG-NbVW6GMI-vc/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.

⟲ **sendtogeo** pushed a commit that referenced this issue on Mar 22, 2021

    `fix for` **#211**   bcc29c0

🚍 **sendtogeo** closed this as completed on Mar 22, 2021

⚇ 🚍 **sendtogeo** self-assigned this on Mar 22, 2021

⬡ 🚍 **sendtogeo** added this to the **Seo panel 4.9.0** milestone on Mar 22, 2021

Assignees
🚍 sendtogeo

Labels
None yet

Projects
None yet

Milestone

Seo panel 4.9.0

Development

No branches or pull requests

---

2 participants
🚍 🔷