

漏洞利用

发xss

21617005840_60618d10d6d6b15edb3f9.png!small?1617005840843

31617006008 60618db845b43ac326228.png!small?1617006008695

如果没有提交或者保存的功能,那么无法与数据库交互形成存储XSS,但是依然可多次点击左上角html按钮触

漏洞

21617006369_60618f21778f46d9f3e6e.png!small?1617006369503

21617006404_60618f44963b9894db568.png!small?1617006404641

抓包并将标签以及原本的文本删除

21617006439_60618f6743357de1b6253.png!small?1617006439339 插入payload:

点我创作

试试在FreeBuf发布您的第一篇文章 让安全圈留下您的足迹

我知道了

%3Cp%3E1111111">%3Cbr%2F%3E%3C%2Fp%3E

21617006474_60618f8a7495ed8da15a6.png!small?1617006474352

成功触发存储型XSS漏洞

21617006515_60618fb3439e3d17ccab9.png!small?1617006515419

21617006641_60619031caf0d7311cafd.png!small?1617006642187

经笔者调查在互联网上存在着许多ueditor编辑器在线展示的网站,这些大都存在没有与后端交互的反射型 XSS, 但是如果存在与后端数据库交互的功能譬如一些写作平台即可形成存储型XSS漏洞,结合一些xss平台, 或者再和其他漏洞配合形成组合拳,威力也不容小藐。

防御措施

- 1、修改 xss过滤白名单 配置文件ueditor.config.js,增加白名单过滤,比如对一些非法的参数和标签,像 <>、,",', img标签的onerror属性, script标签等进行自动转义, 或者是强制的拦截并提示。
- 2、对输入的数据也进行html转义,使其不会识别为可执行脚本。

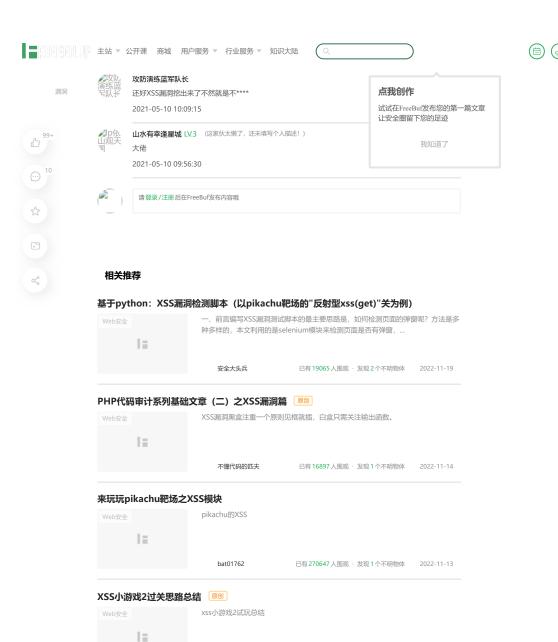
本文作者:卡卡罗特_, 转载请注明来自FreeBuf.COM

● # 富文本编辑器漏洞 ● # XSS漏洞

被以下专辑收录,发现更多精彩内容

+ 收入我的专辑 + 加入我的收藏

与 按热度排序 评论 10 **贝米少年 LV.1** (这家伙太懒了,还未填写个人描述!) 不知道为啥复现不了 2021-05-12 21:33:33 ♡ 亮了 (7) □回复 卡卡罗特 作者 LV.3 (努力努力再努力) 做过二次开发? 2021-05-13 12:55:14 ♡ 亮了 ◎回复 以 **贝米少年 LV.1** (这家伙太懒了,还未填写个人描述!) @卡卡罗特_复现了,但是我现在这个实战环境这个文章别人访问不到。。。。。可惜 2021-05-13 13:09:40 ⊕回复 ※ 高了 蠢蠢的叶小烦 LV.1 来自新浪微博 😚 @存活不超过三集的人 2021-05-10 19:37:42 ♡ 亮了 (3) □回复 安全漏洞报告中心 我司就用的这个...这玩意几乎没对xss进行过滤,毕竟是祖传的 2021-05-10 17:50:38 ♡ 亮了(2) □回复 **卡卡罗特_ 作者 LV.3** (努力努力再努力) 对的,强烈建议做二次开发 2021-05-13 12:59:15 ○回复 ☆ 高了 网瘾患者 也不看看这玩意几年没更新了吗。。。 2021-05-10 17:28:13 ○ 亮了 (2) 回复



已有37352人围观 toxssin: 一款功能强大的XSS漏洞扫描利用和Payload生成工具 这款渗透测试工具能够帮助广大研究人员自动扫描、检测和利用跨站脚本XSS漏洞。

li: 已有 208494 人围观 · 发现 1 个不明物体 2022-08-31 Alpha h4ck





FreeBuf+小程序

扫码把安全装进口袋

登录 注册



