

漏洞

挖洞经验 | UEditor编辑器存储型XSS漏洞

卡卡特_

2021-04-18 17:00:39

344930

10

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



卡卡特_ LV.3

努力努力再努力

关注

13

文章数

10

评论数

11

关注者

前言

UEditor是由百度web前端研发部开发的所见即所得富文本web编辑器，具有轻量，可定制，注重用户体验等特点。UEditor存在一个XSS漏洞，编辑器在定义过滤规则的时候不严和读取内容的时候的绕过导致了该漏洞，此漏洞已经上报，由于技术略菜，有分析不到位的还请多多见谅。

漏洞成因分析

漏洞文件产生在前端配置文件ueditor.config.js:

以下为纯文本粘贴为true时的过滤规则，对一些危险的标签没有做过滤，怪不得好多二次开发的。

```
//纯文本粘贴模式下的过滤规则
//filterTxtRules: function(){
//    function transP(node){
//        node.tagName = 'p';
//        node.setStyle();
//    }
//    return {
//        //直接删除及其子节点内容
//        '-': 'script style object iframe embed input select',
//        'p': {$:{}},
//        'br':{$:{}},
//        'div':!{$:{}},
//        'li':!{$:{}},
//        'caption':transP,
//        'th':transP,
//        'tr':transP,
//        'h1':transP,'h2':transP,'h3':transP,'h4':transP,'h5':transP,'h6':transP,
//        'td':function(node){
//            //没有内容的td直接删掉
//            var txt = !!node.innerText();
//            if(txt){
//                node.parentNode.insertAfter(UE.uNode.createText(' &nbsp;');
//            }
//        }
//    };
//}
```

如下图，在官方文档里也进行了说明，通过getContent和setContent方法用<p>标签读取编辑器内容

```
#通过getContent和setContent方法可以设置和读取编辑器的内容
var ue = UE.getEditor();//对编辑器的操作最好在编辑器ready之后再调用ue.ready(function(){
//设置编辑器的内容
ue.setContent('hello');
//获取html内容，返回: <p>hello</p>
var html = ue.getContent();
//获取纯文本内容，返回: hello
var txt = ue.getContentTxt();});
```

HTML中的p标签为段落标签，目前所有主流浏览器都支持<p>标签。

从编辑器里的左上角显示html可以看出，是带有<p>标签的，所以在标签内写入payload是不被执行的

如下图，在删除掉<p>标签后写入payload可触发XSS漏洞

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按钮触发xss

漏洞利用

漏洞

99+

10

☆


1617006369_60618f21778f46d9f3e6e.png!small?16170063695031617006404_60618f44963b9894db568.png!small?1617006404641

抓包并将<p>标签以及原本的文本删除


1617006439_60618f6743357de1b6253.png!small?1617006439339

插入payload:

%3Cp%3E11111111">%3Cbr%2F%3E%3C%2Fp%3E

1617006474_60618f8a7495ed8da15a6.png!small?1617006474352

成功触发存储型XSS漏洞

1617006515_60618fb3439e3d17ccab9.png!small?16170065154191617006641_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，威力也不容小觑。

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

评论 10

与 按热度排序



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



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

亮了 回复



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

亮了 回复



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

漏洞



攻防演练蓝军队长

还好XSS漏洞挖出来了不然就是不****

2021-05-10 10:09:15



山水有幸逢星城 LV.3 (这家伙太懒了，还未填写个人描述！)

大佬

2021-05-10 09:56:30



请 登录 / 注册 后在FreeBuf发布内容哦

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

99+

10



相关推荐

基于python: XSS漏洞检测脚本 (以pikachu靶场的"反射型xss(get)"关为例)

Web安全



一、前言编写XSS漏洞测试脚本的最主要思路是，如何检测页面的弹窗呢？方法是多种多样的，本文利用的是selenium模块来检测页面是否有弹窗，...

安全大头兵

已有 19065 人围观 · 发现 2 个不明物体

2022-11-19

PHP代码审计系列基础文章（二）之XSS漏洞篇

原创

Web安全



XSS漏洞黑盒注重一个原则见框就插，白盒只需关注输出函数。

不懂代码的匹夫

已有 16897 人围观 · 发现 1 个不明物体

2022-11-14

来玩玩pikachu靶场之XSS模块

Web安全



pikachu的XSS

bat01762

已有 270647 人围观 · 发现 1 个不明物体

2022-11-13

XSS小游戏2过关思路总结

原创

Web安全



xss小游戏2试玩总结

康qeroo

已有 37352 人围观

2022-09-15

toxssin: 一款功能强大的XSS漏洞扫描利用和Payload生成工具

Web安全



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。

Alpha h4ck

已有 208494 人围观 · 发现 1 个不明物体

2022-08-31

