JSONP的SOME

jfeiyi / 2017-11-30 09:50:24 / 浏览数 2236 安全技术 技术讨论 顶(0) 踩(0)

今天看了HCTF2017的那个帖子，里面提到JSONP和same origin method execution。。我理解就是XSS的利用而已呀。。。难道我理解有问题？

上一篇：浅析PHP反序列化漏洞之PHP常见... 下一篇：Adobe ColdFusion ...

1. 4 条回复


hades 2017-11-30 10:01:25

@jfeiyi JSONP 劫持风险

应用为了跨域传输数据，有一种常用的技术方案：JSONP。
但是由于通过JSONP传输数据是难以做权限校验的，如果传输的数据本身涉及敏感信息，恶意第三方B可以将该JSONP接口嵌入自己的页面中，从而访问者A浏览页面时

0 回复Ta


hello_world 2017-11-30 19:05:00

举个栗子
中国最大的Webshell后门箱子调查，所有公开大马全军覆没
一文中写道■■■■■■■■■■■■■■■■■■■■■■■■QQ■

0 回复Ta


todaro 2017-12-04 10:58:35

不是，和xss还不一样
推荐你看一篇http://blog.safedog.cn/?p=13

0 回复Ta

lorexxar 2017-12-04 11:00:41

应该说是xss的一种利用手法吧，想法很精巧，题目里不能明显的提现这个攻击可以应用的特殊点，可以看看视频。

不过这个利用条件本来就苛刻，所以实际利用还很困难

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板