New issue

Jump to bottom

/sys/duplicate/check存在sql注入漏洞 #4129

Closed azraelxuemo opened this issue on Oct 25 · 10 comments

azraelxuemo commented on Oct 25

jeecg-boot漏洞.pdf

zhangdaiscott commented on Oct 30 Member

你这个是哪个版本，针对注释这种我们处理过

azraelxuemo commented on Oct 30 Author

就是最新的，但是可以绕过
...

zhangdaiscott commented on Oct 30 Member

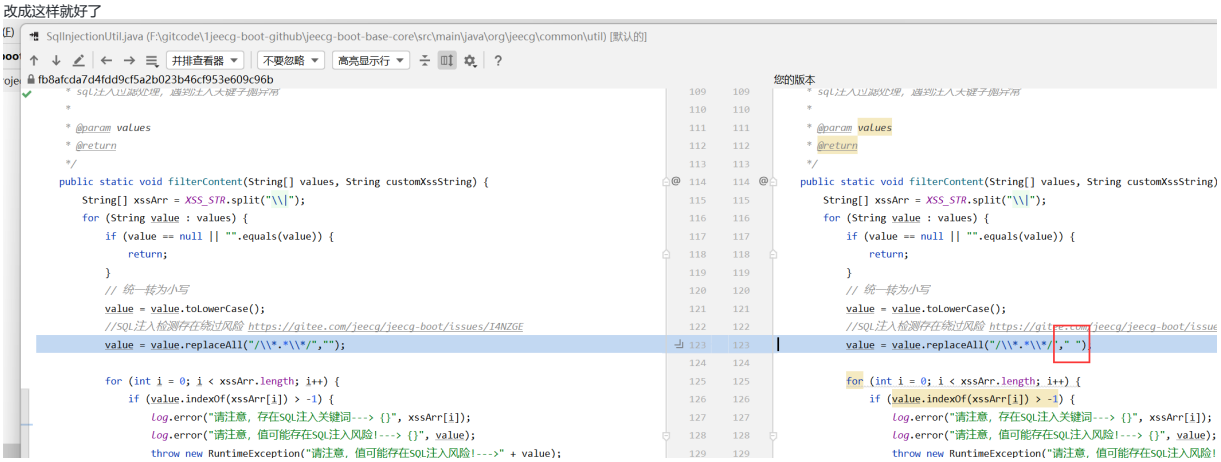
截图版本号

azraelxuemo commented on Oct 30 Author

你们自己看我发的内容，里面你们加check了啊，但是check有问题，可以被bypass我已经说的很详细了，我是直接clone你们的项目
...

zhangdaiscott commented on Oct 30 Member

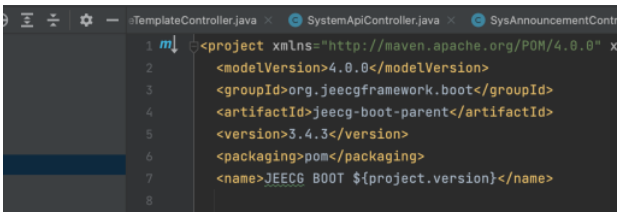
改成这样就好了



azraelxuemo commented on Oct 30 Author

okok好的好的，因为我看到的是checksql可以被绕过，所以就提出来了哈哈哈2333
...

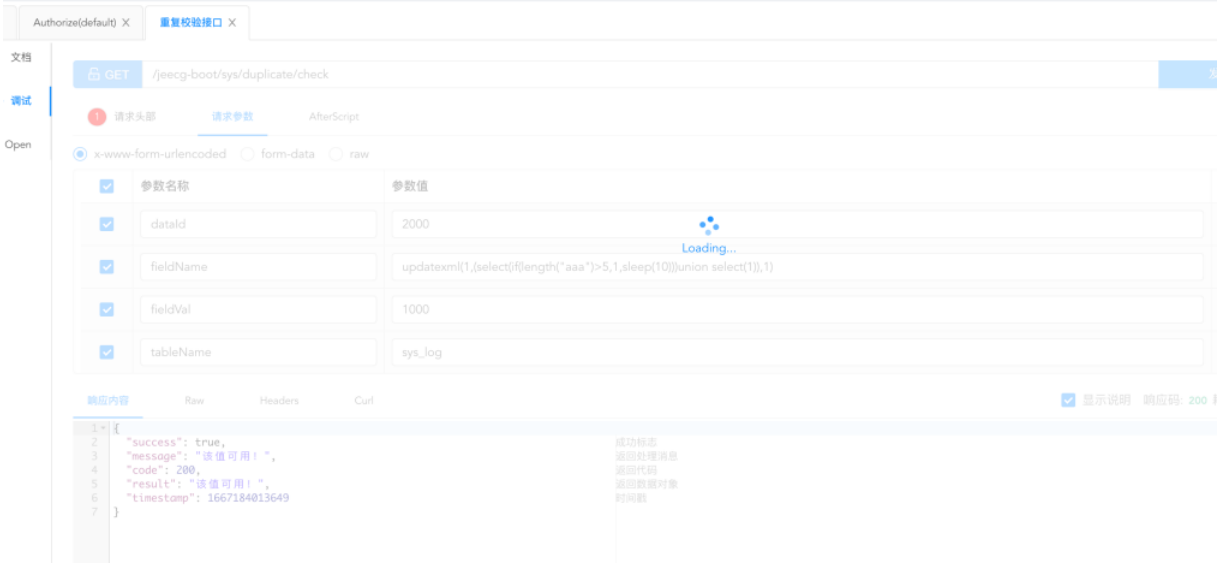
azraelxuemo commented on Oct 30 Author



这个是我的版本号

azraelxuemo commented on Oct 30 • edited Author

我个人建议还是把sql注入里面的空格删掉
因为你们替换了//
但还可以用()绕过
updatexml(1,(select(if(length("aaa")>5,1,sleep(10)))union select(1)),1)
所以索性你们就不替换//这些
然后直接把输入的整个字符串转成小写
判断有没有select,这种关键字



您看这样还是可以注入的
就算我修改了还是可以绕过的

zhangdaiscott added a commit that referenced this issue on Nov 1

sql注入检查更加严格，修复/sys/duplicate/check存在sql注入漏洞 #4129 — f18ced5

zhangdaiscott commented on Nov 1 — Member

已修复

zhangdaiscott closed this as completed on Nov 1

azraelxuemo commented on Nov 1 — Author

好的，辛苦嘞

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants