New issue

Jump to bottom

v2.2.0 Stored XSS vulnerabilities #1866

Closed **wuguan8888** opened this issue on Jul 30, 2020 · 5 comments

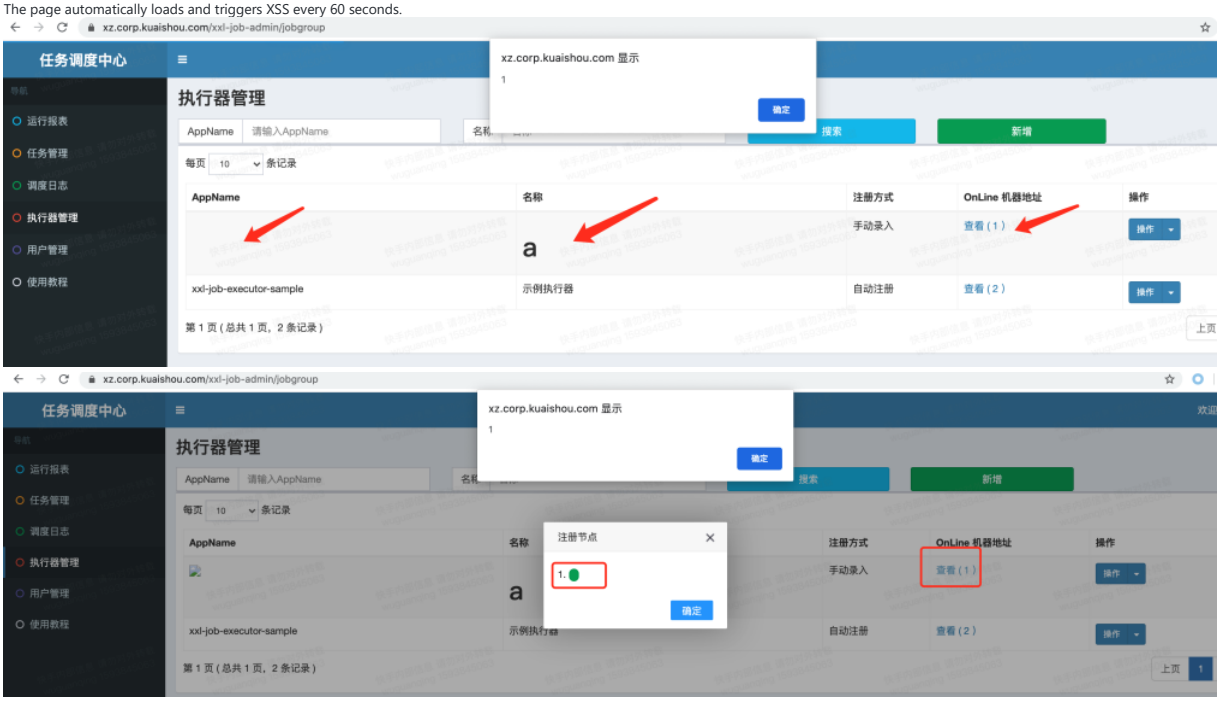
wuguan8888 commented on Jul 30, 2020 • edited

Locate the executor management function:
https://github.com/xuxueli/xxl-job/blob/289f02185b952f4652a4a7daf4ac3c6384f338bc/xxl-job-admin/src/main/java/com/xxl/job/admin/controller/JobGroupController.java
insert POC there has front-end validation,By code audit, I find that the back end only has length validation.Can be bypassed by Burp Intercept.
POC:<img/src=# onerror="alert(1)"/>

The code directly gets AppName and manually entered parameters for front-end display.No filtering or encoding .Causes storage XSS vulnerabilities.

```
90          @RequestMapping("/update")
91          @ResponseBody
92          public ReturnT<String> update(XxlJobGroup xxlJobGroup){
93                  // valid
94                  if (xxlJobGroup.getAppname()==null || xxlJobGroup.getAppname().trim().length()==0) {
95                          return new ReturnT<String>(500, (I18nUtil.getString("system_please_input")+"AppName") );
96                  }
97                  if (xxlJobGroup.getAppname().length()<4 || xxlJobGroup.getAppname().length()>64) {
98                          return new ReturnT<String>(500, I18nUtil.getString("jobgroup_field_appname_length") );
99                  }
100                 if (xxlJobGroup.getTitle()==null || xxlJobGroup.getTitle().trim().length()==0) {
101                         return new ReturnT<String>(500, (I18nUtil.getString("system_please_input") + I18nUtil.getString("jobgroup_field_title")) );
102                 }
103                 if (xxlJobGroup.getAddressType() == 0) {
104                         // 0=自动注册
105                         List<String> registryList = findRegistryByAppName(xxlJobGroup.getAppname());
106                         String addressListStr = null;
107                         if (registryList!=null && !registryList.isEmpty()) {
108                                 Collections.sort(registryList);
109                                 addressListStr = "";
110                                 for (String item:registryList) {
111                                         addressListStr += item + ",";
112                                 }
113                                 addressListStr = addressListStr.substring(0, addressListStr.length()-1);
114                         }
115                         xxlJobGroup.setAddressList(addressListStr);
116                 } else {
117                         // 1=手动录入
118                         if (xxlJobGroup.getAddressList()==null || xxlJobGroup.getAddressList().trim().length()==0) {
119                                 return new ReturnT<String>(500, I18nUtil.getString("jobgroup_field_addressType_limit") );
120                         }
121                         String[] addresss = xxlJobGroup.getAddressList().split(",");
122                         for (String item: addresss) {
123                                 if (item==null || item.trim().length()==0) {
124                                         return new ReturnT<String>(500, I18nUtil.getString("jobgroup_field_registryList_unvalid") );
125                                 }
126                         }
127                 }
128
129                 int ret = xxlJobGroupDao.update(xxlJobGroup);
130                 return (ret>0)?ReturnT.SUCCESS:ReturnT.FAIL;
131         }
```

The page automatically loads and triggers XSS every 60 seconds.



ggkitsas commented on Sep 17, 2020

Hi, any plans releasing a fix for this?

wuguan8888 commented on Sep 17, 2020 — Author

> Hi, any plans releasing a fix for this?
> The parameters are encoded as HTML entities or use blacklist filter labels

xuxueli commented on Oct 30, 2020 — Owner

感谢反馈！
已修复并推送mater分支，将会跟随下个版本一同发布。

xuxueli closed this as completed on Oct 30, 2020

NicoleG25 commented on Dec 1, 2020 • edited

你好 **@xuxueli**
您能告诉我该修复程序在哪里应用吗?

提前致谢！

Findorgri commented on Feb 15, 2021 • edited

> 你好 **@xuxueli**
> 您能告诉我该修复程序在哪里应用吗?
>
> 提前致谢！

Hi, **@NicoleG25** , did you find where the fix was applied? Because the controller is still the same.
Thanks!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants