New issue

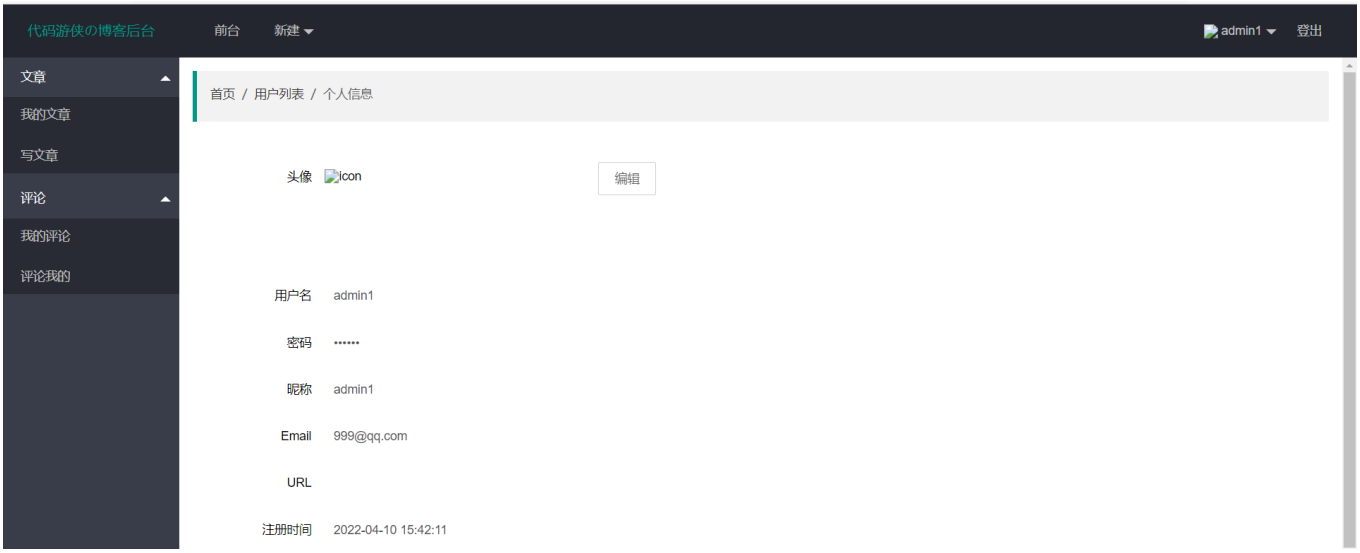
Jump to bottom

XSS attacks occur when user profile pictures are updated #76

Open **fiblue** opened this issue on Apr 10 · 0 comments

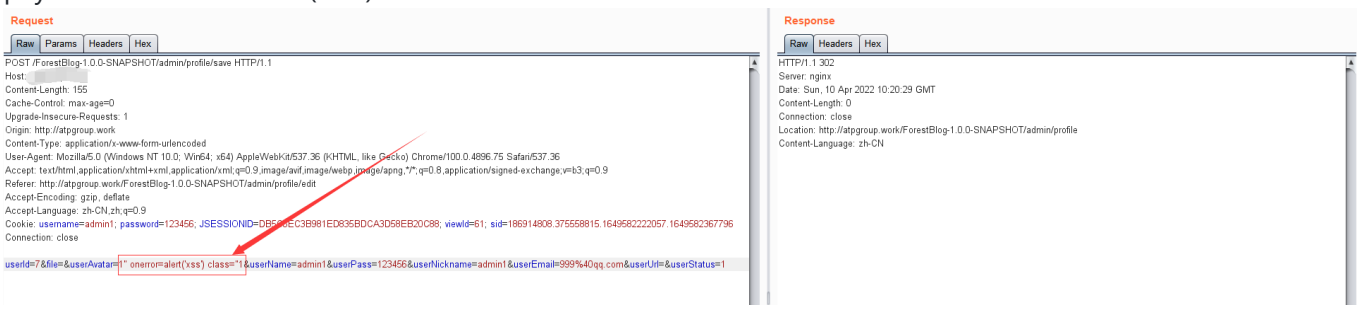
fiblue commented on Apr 10 • edited

1.Edit user information and save it

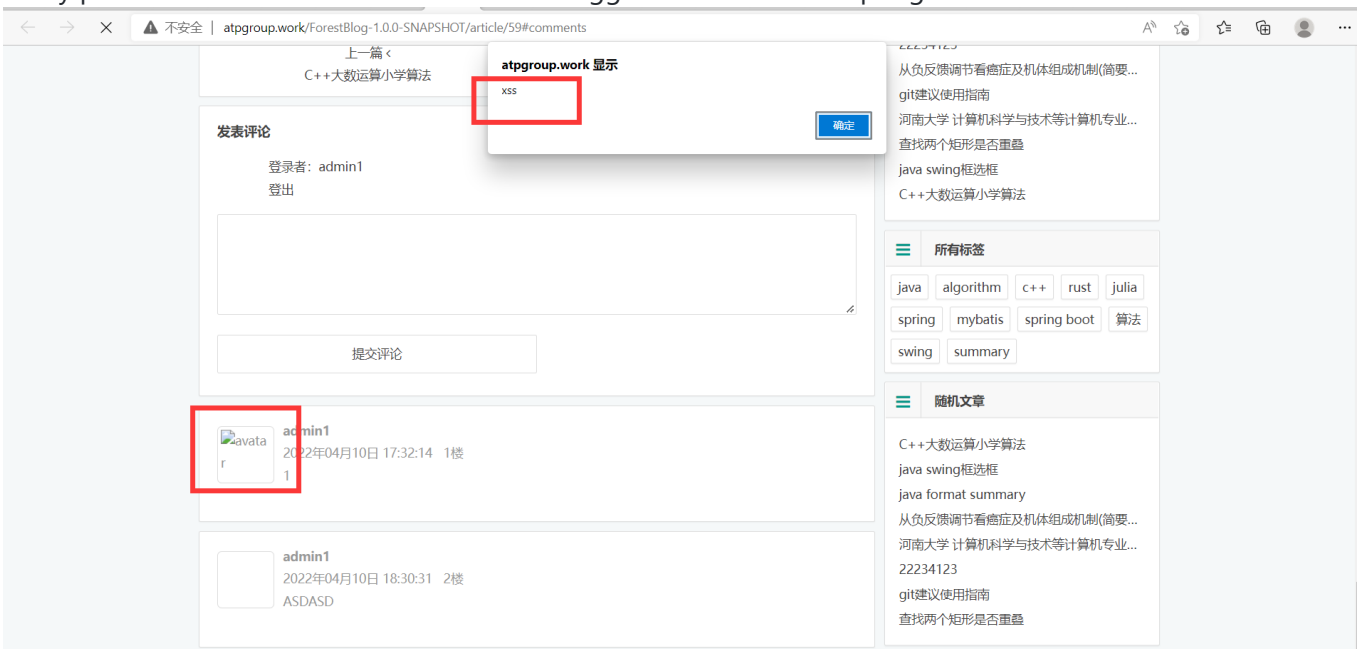


2.The profile picture address in the packet capture request is changed

payload:1" onerror=alert('xss') class="1



3.Any place where the user's avatar is loaded triggers a Cross Site Scripting



4.User information should be added and modified with XSS detection

src/main/java/com/liuyanzhao/ssm/blog/controller/admin/AdminController.java

```
233 2021/2/25 saysky     /**
234 2021/2/25 saysky      * 编辑用户提交
235 2021/2/25 saysky      *
236 2021/2/25 saysky      * @param user
237 2021/2/25 saysky      * @return
238 2021/2/25 saysky      */
239 2021/2/25 saysky     @RequestMapping(value = "/admin/profile/save", method = RequestMethod.POST)
240 2021/2/25 saysky     public String saveProfile(User user, HttpSession session) {
241 2021/2/25 saysky         User dbUser = (User) session.getAttribute( s: "user");
242 2021/2/25 saysky
243 2021/2/25 saysky         user.setUserId(dbUser.getUserId());
244 2021/2/25 saysky         userService.updateUser(user);
245 2021/2/25 saysky         return "redirect:/admin/profile";
246 2021/2/25 saysky     }
247 2021/2/25 saysky
248 2021/2/25 saysky
249 2017/10/10 saysky }
250
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant