New issue

Jump to bottom

IDOR causes unauthorized changes to any user information #35

Closed Jayway007 opened this issue on May 26, 2020 · 1 comment

Jayway007 commented on May 26, 2020

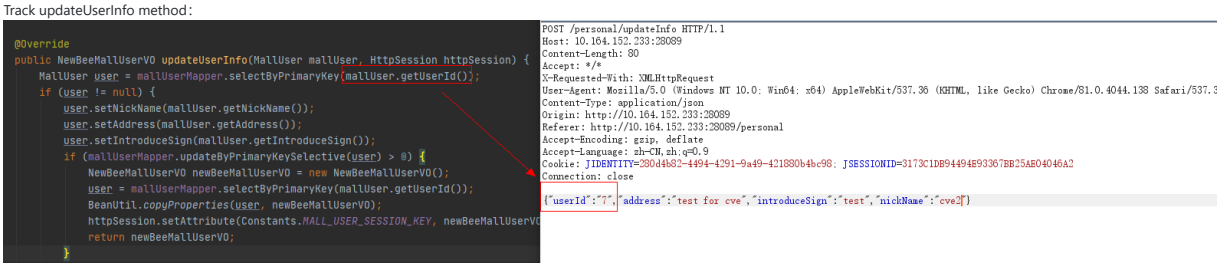
1、/personal/updateInfo，this interface can be used to update user information：

10.164.152.233:28089/personal

2、The corresponding code is as follows：

```
@PostMapping("/personal/updateInfo")
@ResponseBody
public Result updateInfo(@RequestBody MallUser mallUser, HttpSession httpSession) {
    NewBeeMallUserVO mallUserTemp = newBeeMallUserService.updateUserInfo(mallUser,httpSession);
    if (mallUserTemp == null) {
        Result result = ResultGenerator.genFailResult("修改失败");
        return result;
    } else {
        //返回成功
        Result result = ResultGenerator.genSuccessResult();
        return result;
    }
}
```

Track updateUserInfo method：



3、The code updates the information after querying by the value of userid, so you can modify any user information by tampering with the value of userId.

ZHENFENG13 commented on May 27, 2020 Collaborator

好的，我尽快修改，感谢！

newbee-mall referenced this issue on May 28, 2020

Fixing a bug. 427f579

newbee-mall closed this as completed on Oct 20, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants