New issue   Jump to bottom

后台头像管理模块存在任意文件上传getshell #51

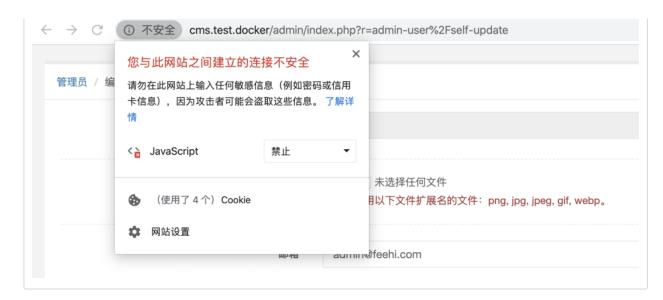⊙ Closed   whb5974 opened this issue on Mar 27, 2020 · 1 comment

---

whb5974 commented on Mar 27, 2020

1. The administrator will use the beforSave function in the /common/models/AdminUser.php file to modify the avatar.
   This function will call Util's handleModelSingleFileUpload function

2. We continue to use the handleModelSingleFileUpload function to find that the function directly calls the upload function without filtering the file name.

3. We followed up the saveAs function and found that the temporary file was directly moved to an undetected file name.

4. Vulnerability verification

---

liufee commented on Apr 6, 2020   Owner

cms.test.docker/admin/index.php?r=admin-user%2Fself-update

不安全

您与此网站之间建立的连接不安全

请勿在此网站上输入任何敏感信息（例如密码或信用卡信息），因为攻击者可能会盗取这些信息。 了解详情

JavaScript 禁止

（使用了 4 个）Cookie

网站设置

管理员 / 编

未选择任何文件

月以下文件扩展名的文件：png, jpg, jpeg, gif, webp。

邮箱 admin@feehi.com

liufee closed this as completed on Apr 6, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants