New issue

Jump to bottom

Identity authentication vulnerability in Latest Release #30

Closed **HatBoy** opened this issue on Mar 14, 2019 · 3 comments

HatBoy commented on Mar 14, 2019

Hi, I would like to report Cross Site Scripting vulnerability in latest release.

Description:
Identity authentication vulnerability in the logout, When you log out, the authentication token is still valid.

Steps To Reproduce:
1.Login the background
2.Do something, like list users
3.Logout
4.Replay packet, can see the user list.

Request

Raw Params Headers Hex

```
GET /cms/admin/users?count=10&page=0 HTTP/1.1
Host: 192.168.100.8:5000
Accept: application/json, text/plain, */*
Origin: http://192.168.100.8:8080
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE1NTI1NzI0NTQsIm5iZiI6MTU1MjU3MjQ1NCwianRpIjoiYjM5ZDIkNjktMzRhOS00OGY2LWE0NWUtZWNlZTBmYWRjMTZhIiwiZXhwIjoxNTUyNTc2MDU0LCJpZGVudGl0eSI6MSwiZnJlc2giOmZhbHNlLCJ0eXBlIjoiYWNjZXNzIn0.Yry2BhYCQs1RtKSFYA_s5YPlIXcLIkPhpz3XcJbfg-Y
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
DNT: 1
Referer: http://192.168.100.8:8080/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 1222
Access-Control-Allow-Origin: http://192.168.100.8:8080
Server: Werkzeug/0.14.1 Python/3.6.8
Date: Thu, 14 Mar 2019 14:23:11 GMT

{
  "collection": [
    {
      "active": 1,
      "create_time": 1552564105000,
      "email": "admifadvzcvdddzxcbfasdfn123@qq.com",
      "group_id": 1,
      "group_name": "\u7528\u6237",
      "id": 5,
      "nickname": "admin123",
      "super": 1
    },
    {
      "active": 1,
      "create_time": 1552564490000,
      "email": "admifasffvzcvzxczbasfasf@qq.com",
      "group_id": 1,
      "group_name": "\u7528\u6237",
      "id": 6,
      "nickname": "user.id",
      "super": 1
```

author by jin.dong@dbappsecurity.com.cn

7insummer commented on Mar 14, 2019

This should be a bug. Thank you very much. Let's check it out。

OS-WS commented on Aug 17, 2021

Hi **@7insummer** **@HatBoy** ,
Was this issue fixed?
if so, in what commit and what tag/version?
thanks!

sunlin92 commented on Dec 9, 2021 Member

This shouldn't be a bug and there is no plan to fix it.

sunlin92 closed this as completed on Jan 18

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

4 participants