CVE-2019-9168：WordPress WooCommerce XSS漏洞

angel010 / 2019-03-06 01:21:00 / 浏览数 1472 安全技术 漏洞分析 顶(0) 踩(0)

本文翻译自：https://www.fortinet.com/blog/threat-research/wordpress-woocommerce-xss-vulnerability----hijacking-a-customer-.html

---

概述

FortiGuard
Labs研究人员发现WooCommerce的一个XSS漏洞。WooCommerce是基于WordPress之上的开源电子商务平台。根据BuiltWith的统计数据，WooCommerce是排名第一
该XSS漏洞CVE编号为CVE-2019-9168，位于Photoswipe函数的放大、缩小展示中，WooCommerce在处理图片的标题和注释数据时出现问题。该漏洞允许攻击者注入任意
该XSS漏洞影响WooCommerce v 3.5.4及之前版本。

根据FortiGuard Lab提供的0 day预警信息，WooCommerce已经发布了软件补丁。如图1所示，WooCommerce补丁在处理标题和注释数据时进行了修改。

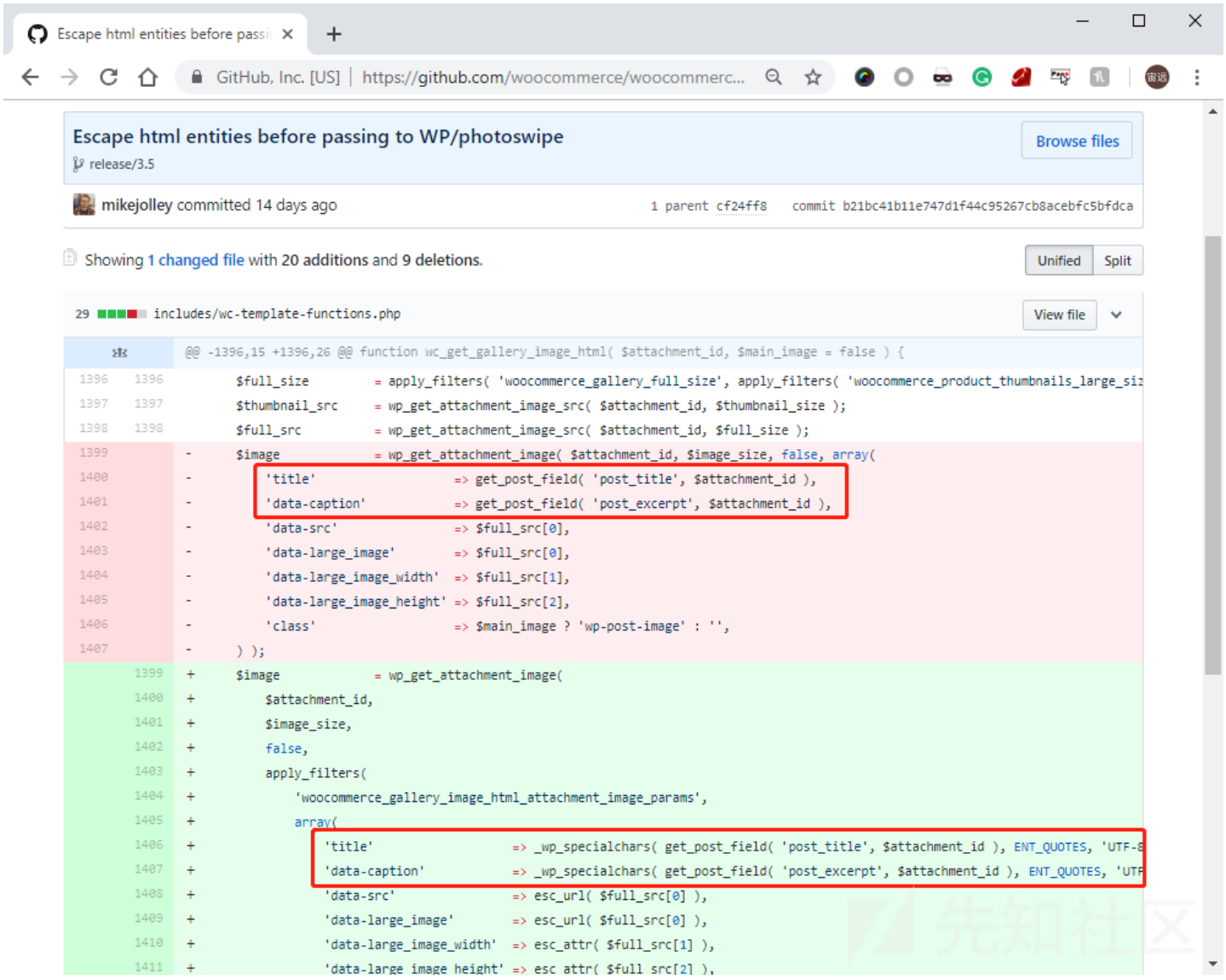

图1. CVE-2019-9168补丁

漏洞分析

为了复现该漏洞，第一步就是上传一个图片并在图片的caption域插入JS代码。在WordPress中，上传图片到低权限的账户并不需要访问WooCommerce插件，如图2所示。

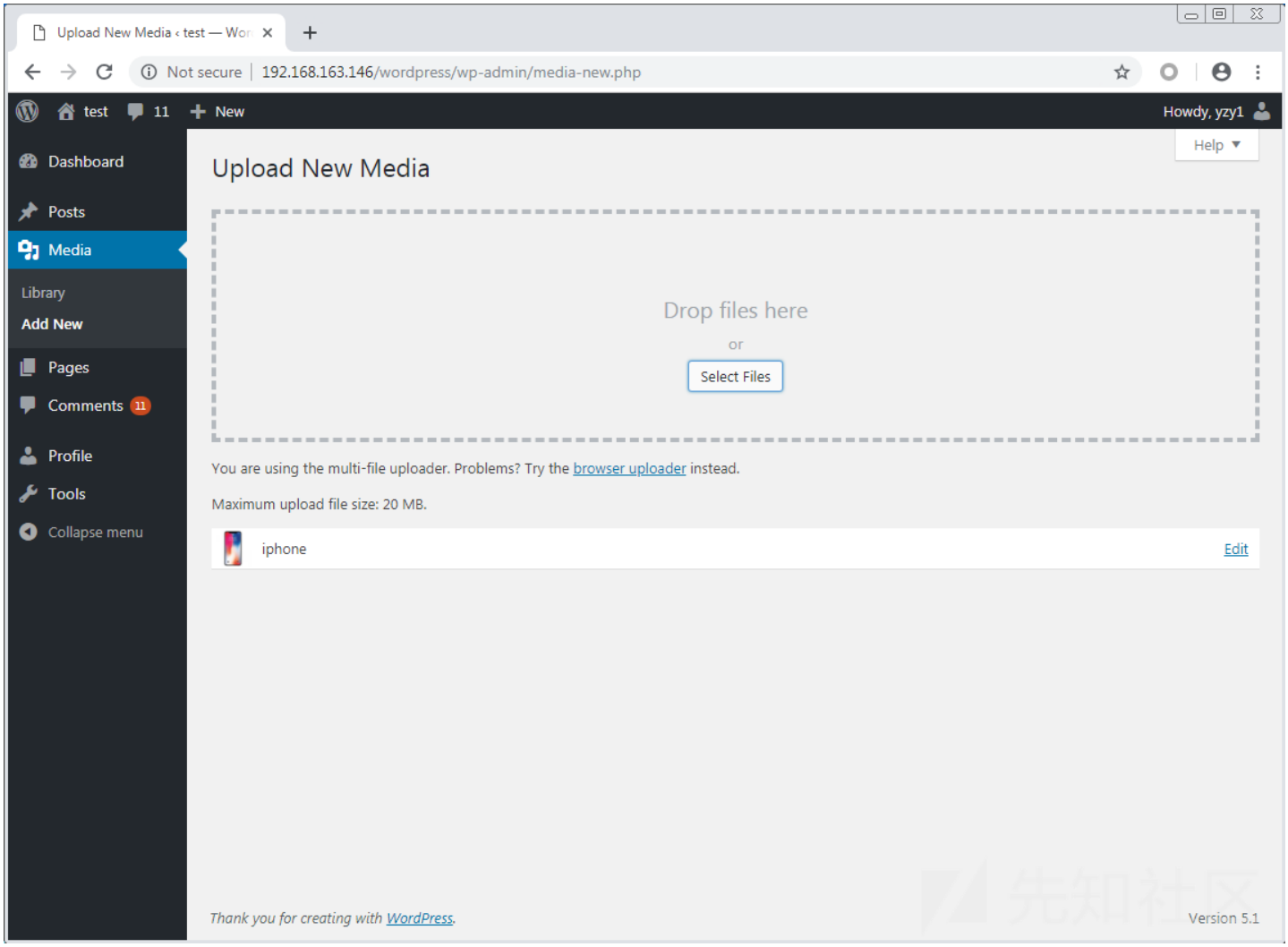

图2. 上传图片

因为像admin这样高权限的账户回可以添加任意JS代码，研究人员可以使用低权限的账户插入处理过的代码`"<img src=1 onerror=prompt('1')>"`，如图3所示。

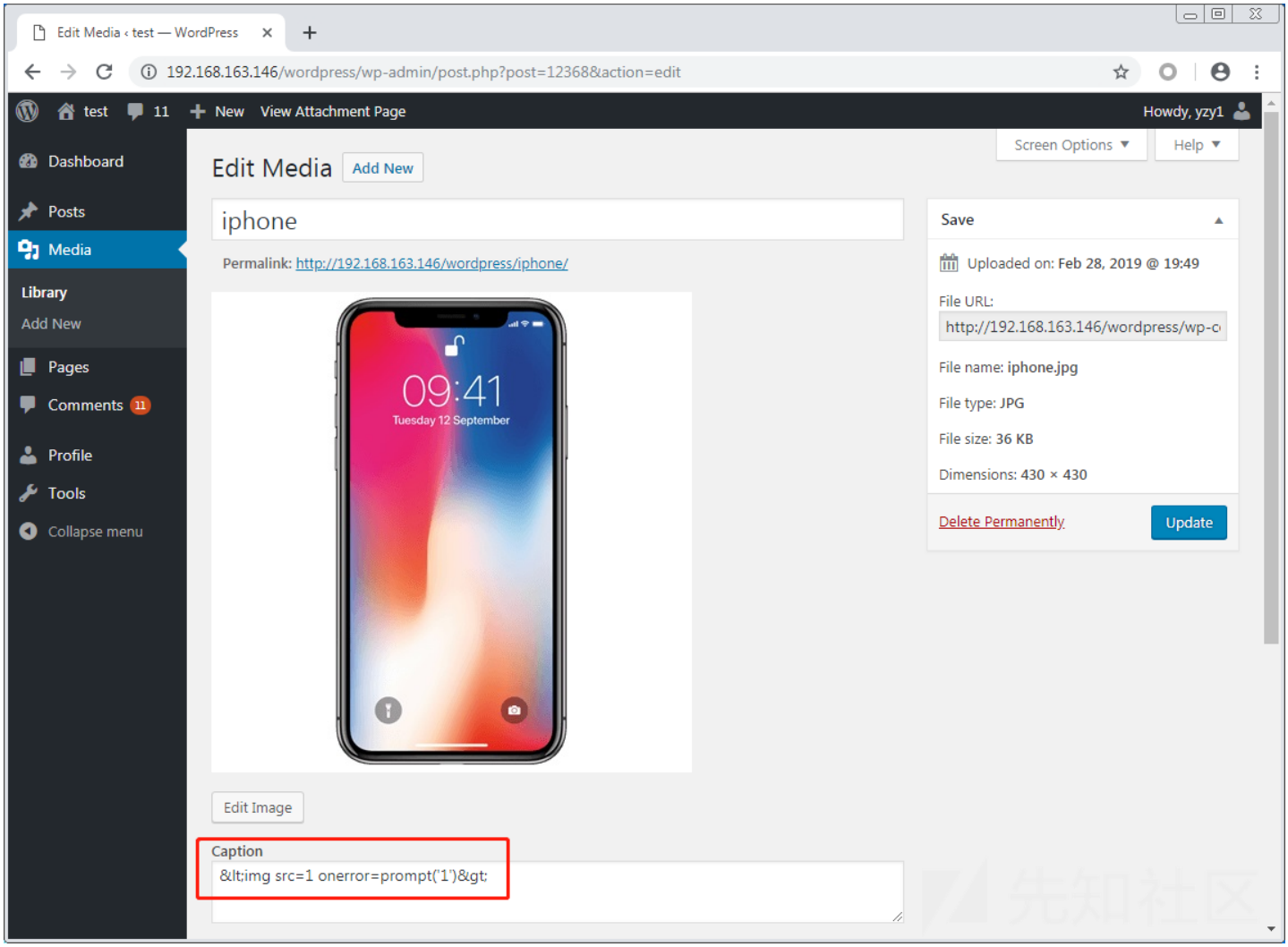

图3. 插入XSS代码

如果有低权限的用户将受感染的图片添加到产品图片或产品图集中，XSS代码就可以插入到产品页中，如图4所示。

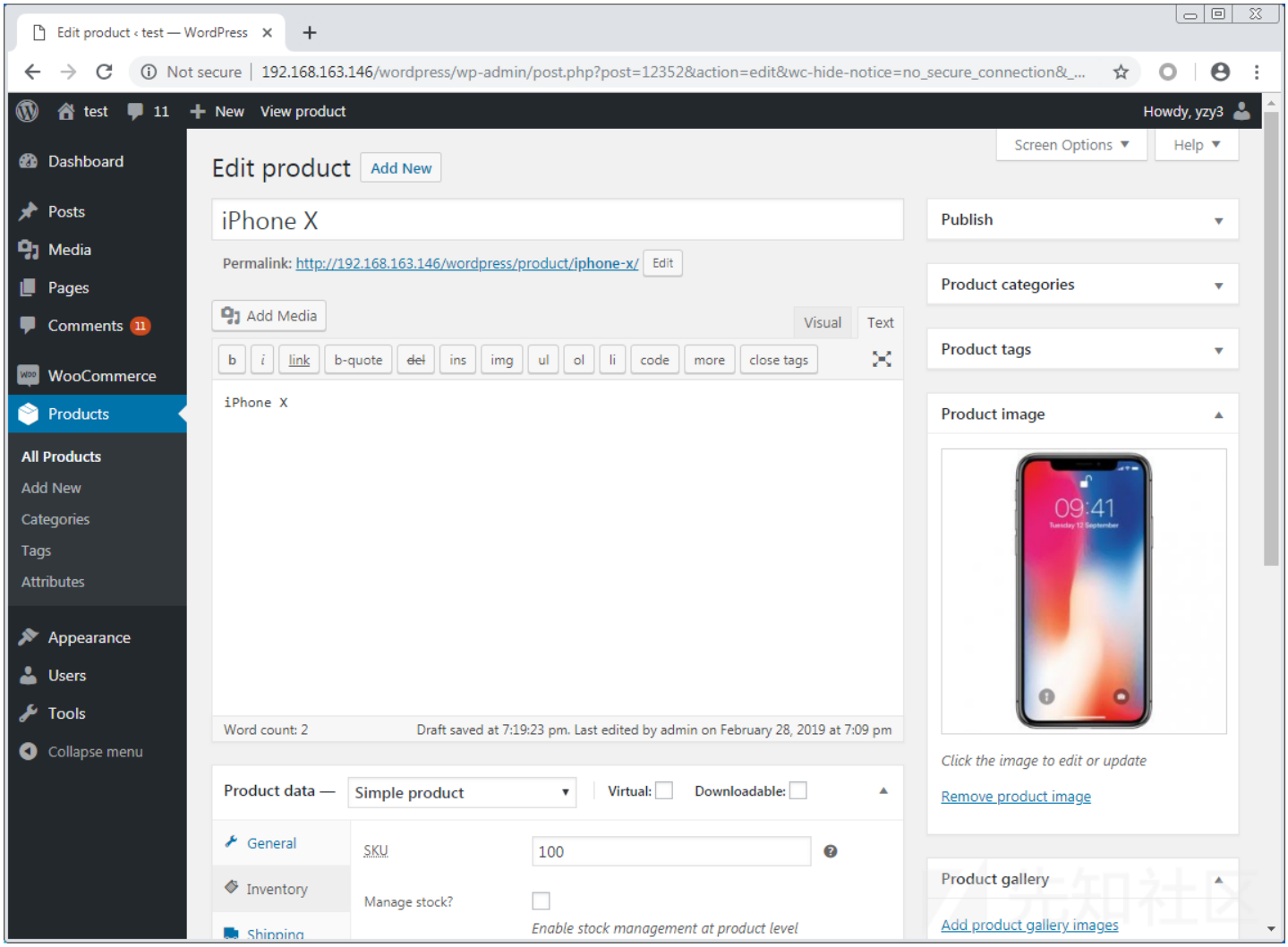

图4. 图片插入到产品页

当受害者查看产品，并放大到产品图片时，XSS代码就会自动执行，如图5和图6所示。

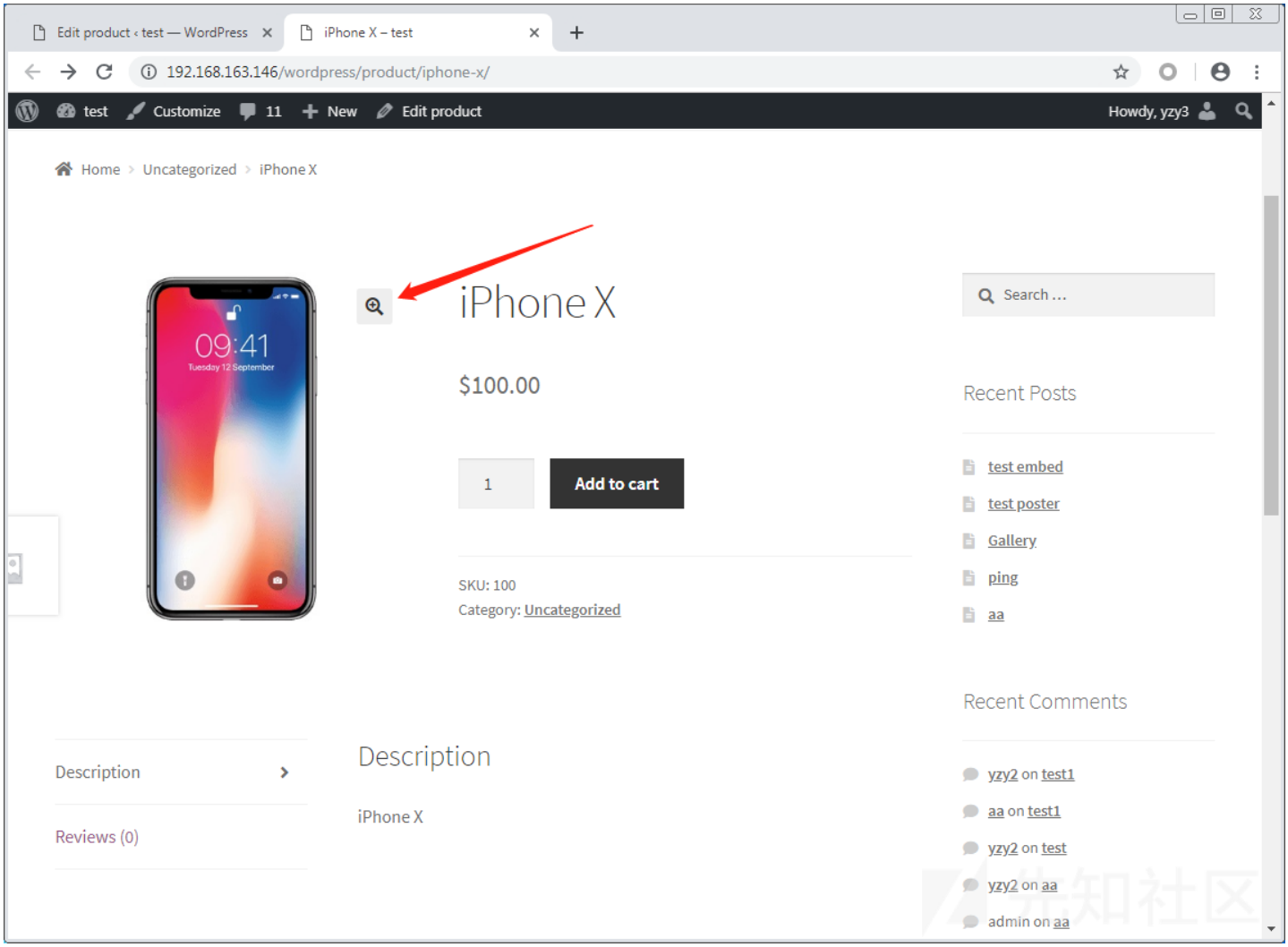
Edit product ‹ test — WordPress
iPhone X – test
192.168.163.146/wordpress/product/iphone-x/
test
Customize
11
New
Edit product
Howdy, yzy3
Home
Uncategorized
iPhone X
iPhone X
$100.00
1
Add to cart
SKU: 100
Category: Uncategorized
Search …
Recent Posts
test embed
test poster
Gallery
ping
aa
Recent Comments
yzy2 on test1
aa on test1
yzy2 on test
yzy2 on aa
admin on aa
Description
Reviews (0)
Description
iPhone X

图5. 产品图片放大

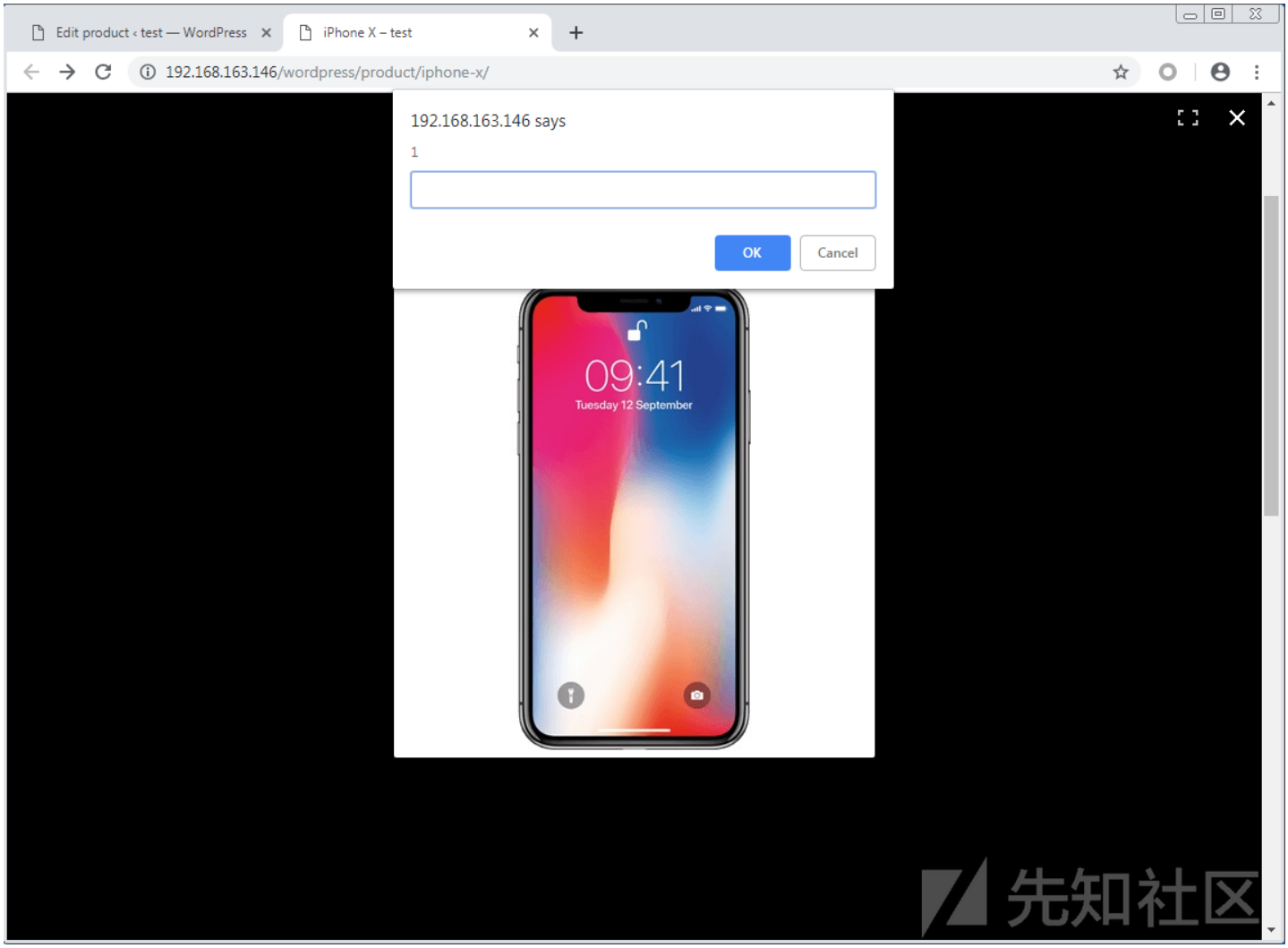

图6. 触发XSS漏洞

为了简化攻击过程，攻击者可以通过将这些图片的属性title和subject修改为"`<img src=1 onerror=prompt('2')>`"，如图7所示。

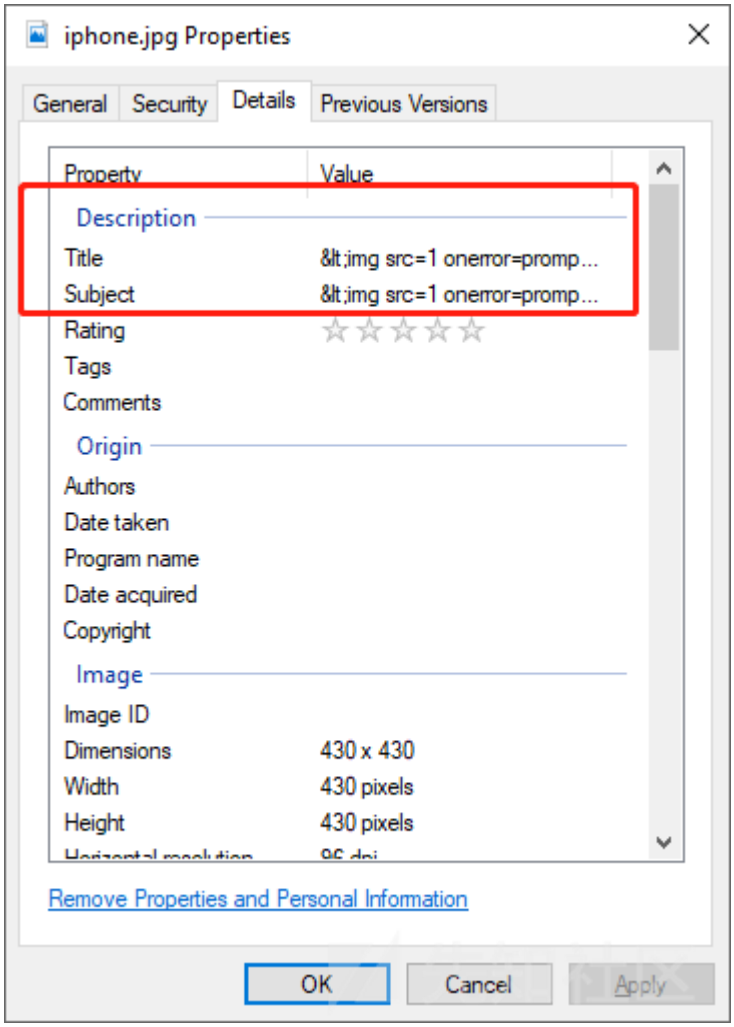

图7. 创建PoC

攻击者可以与站点管理员分享该图片。然后，当管理员使用该图片作为产品图片或加入到产品图集时，XSS代码就被成功插入了，如图8所示。

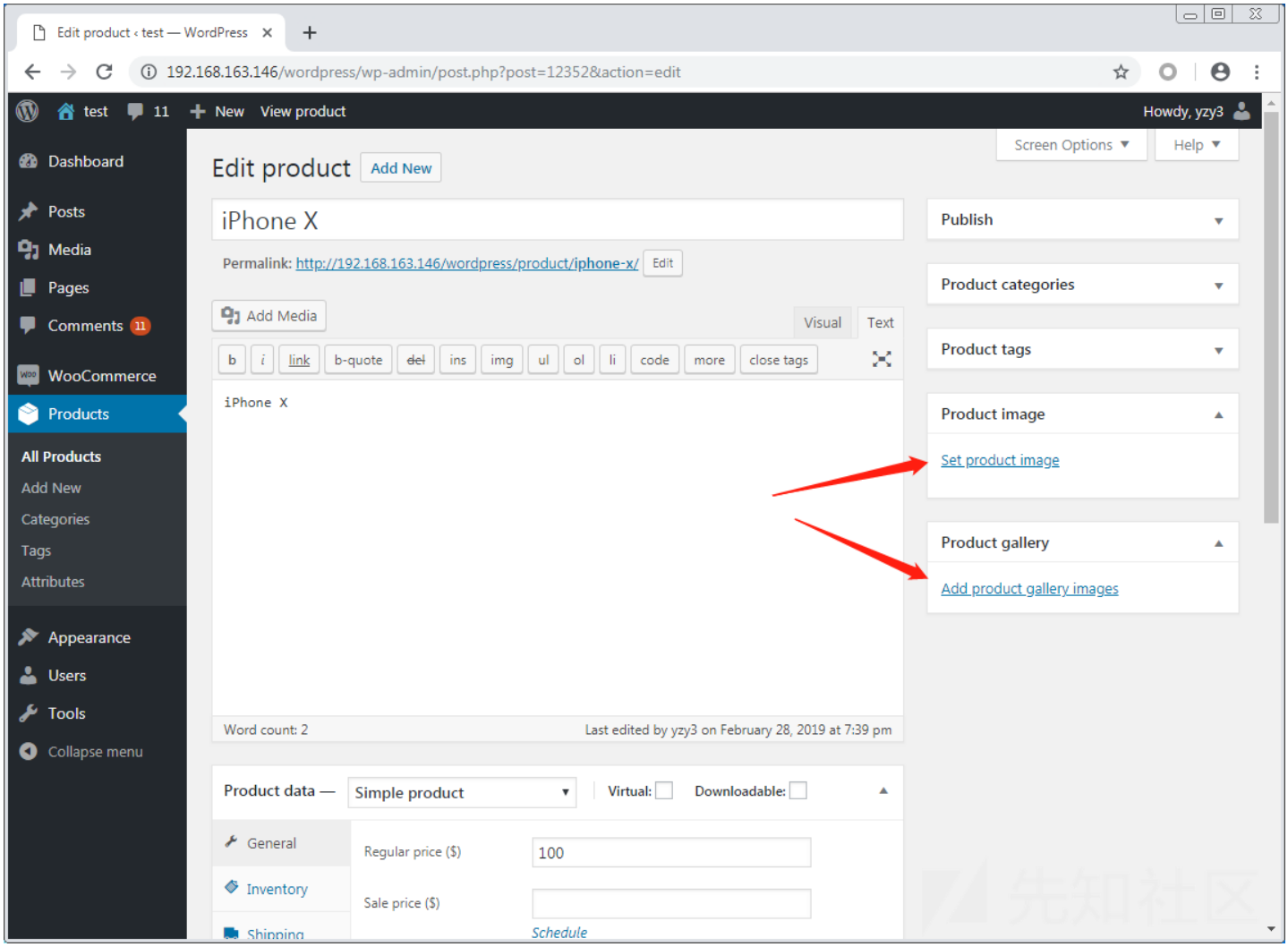

图8. 站点管理员使用PoC文件作为产品图片

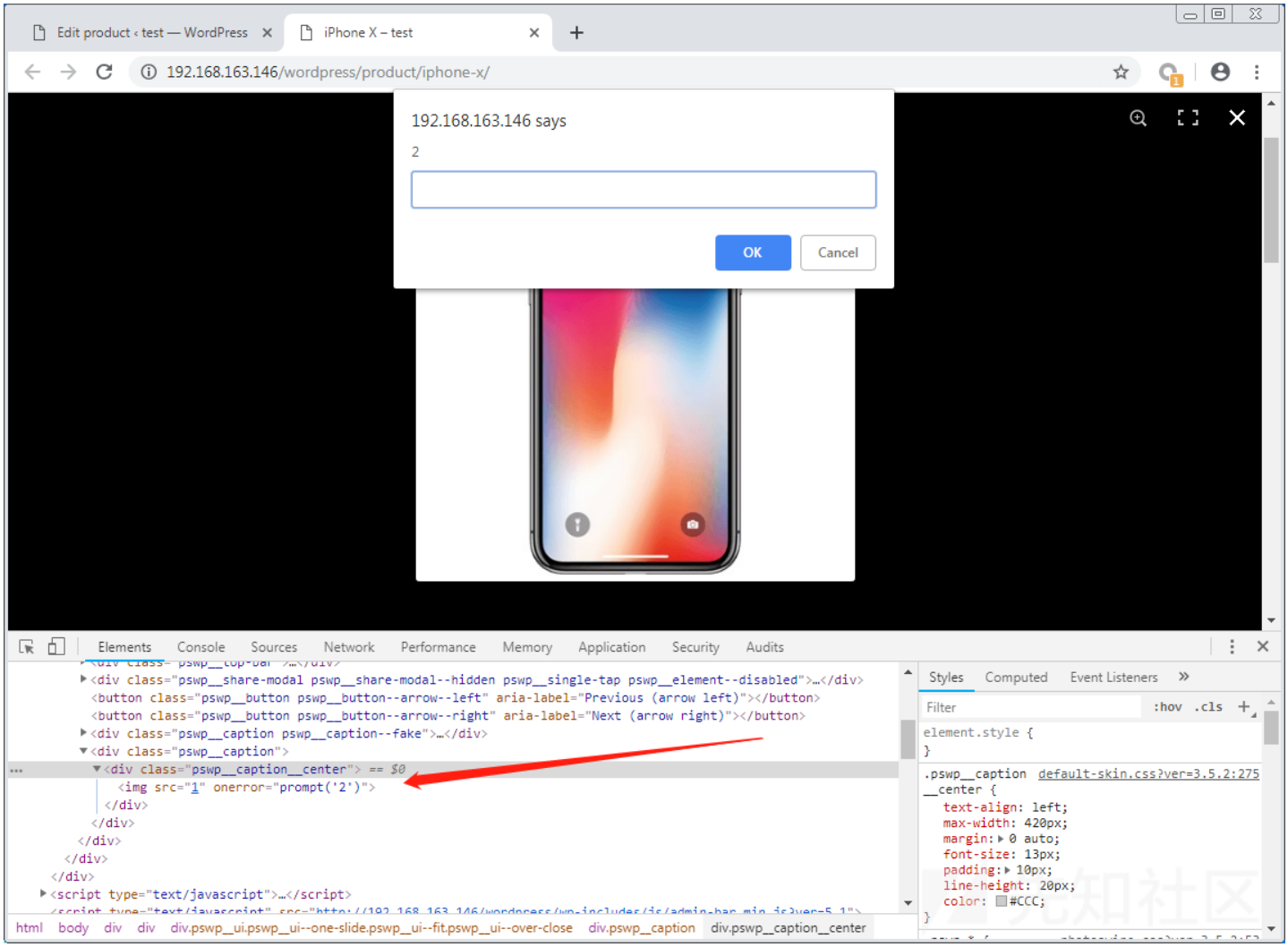

图9. 触发XSS攻击

攻击者可以利用该漏洞来劫持当前用户会话，以控制受害者的浏览器。因为被攻击的目标是电子商务网站，攻击者可以收集用户的银行卡信息、地址等敏感数据。

建议

研究人员建议所有受影响的有漏洞的WooCommerce版本用户尽快升级到最新版本。

点击收藏 | 0 关注 | 1

上一篇：漏洞分析之——顺瓜摸藤 下一篇：使用Seq2Seq自动编码器检测W...

1. 1 条回复

188****6649 2019-03-08 15:15:26

<script> </script>

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板