Magento商务平台的XSS漏洞

Agostop / 2019-01-11 09:09:00 / 浏览数 11018

原文链接：https://www.fortinet.com/blog/threat-research/magento-commerce-widget-form--core--xss-vulnerability.html

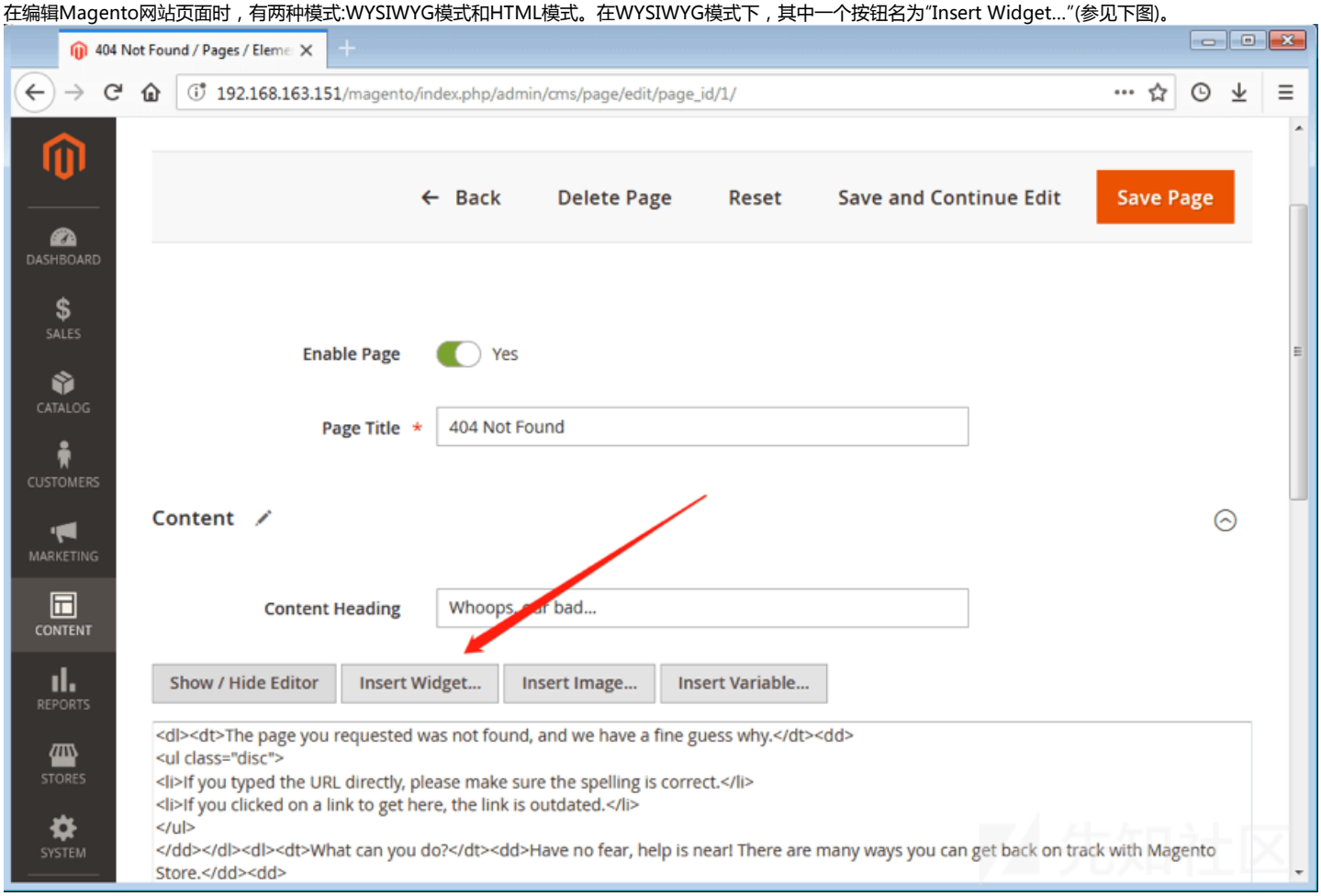
虽然电子商务给我们带来了更方便的生活，但它在互联网上正面临着越来越多的威胁。根据Alexa 2018年前百万电子商务平台排名显示，Magento Commerce目前拥有超过14%的市场份额，是全球第二大电子商务平台。Magento的客户中有很多知名公司，包括惠普、可口可乐和佳能等。

FortiGuard Labs团队最近在Magento中发现了一个跨站脚本攻击(XSS)漏洞。这个漏洞产生的原因是因为Magento在将用户提供的数据插入到动态生成的表单控件之前没能对其做好安全

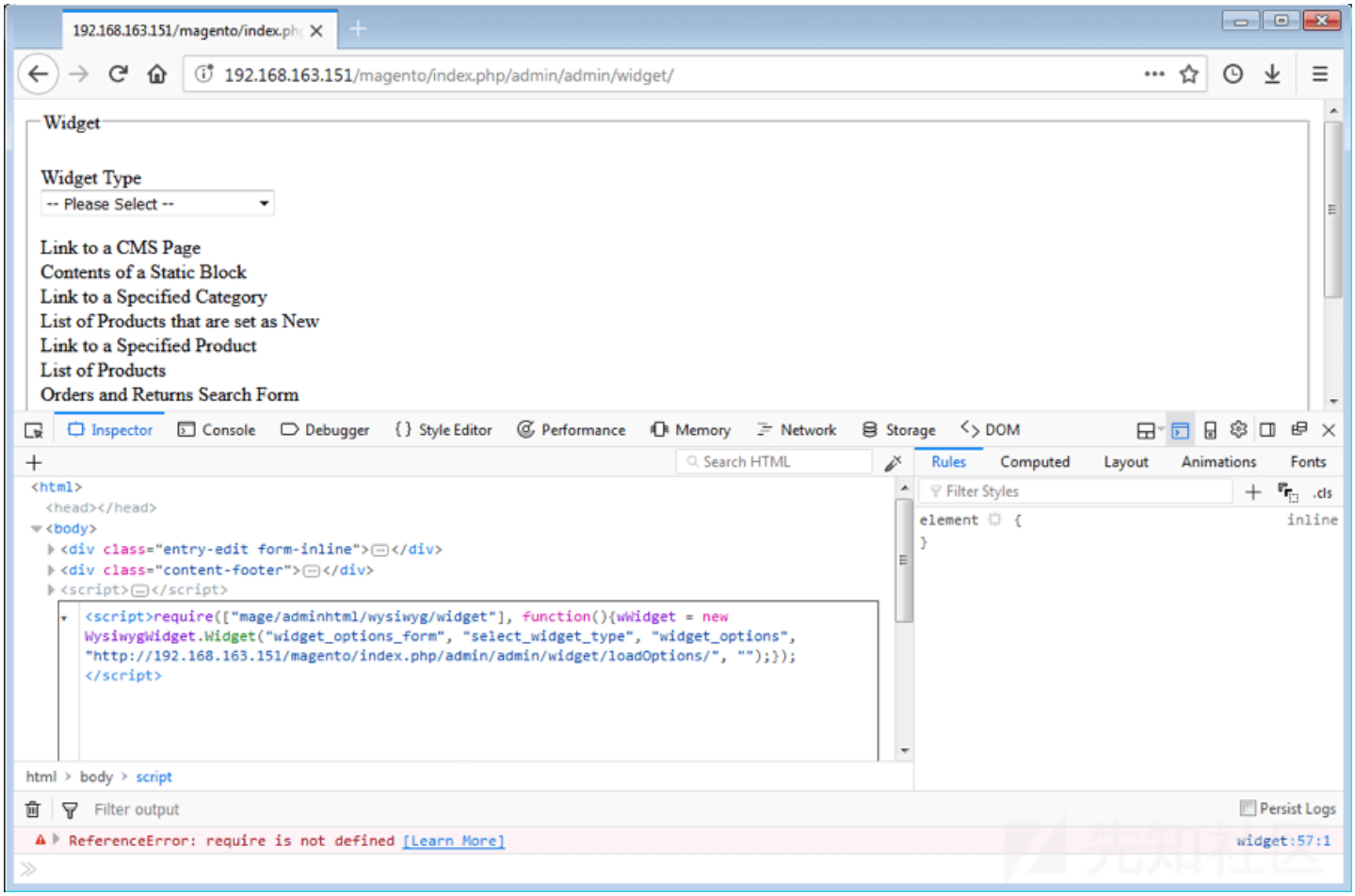
此XSS漏洞影响到2.1.16版本之前的Magento Commerce 2.1系列版本和2.2.7之前的Magento Commerce 2.2系列版本。

漏洞分析

在编辑Magento网站页面时，有两种模式:WYSIWYG模式和HTML模式。在WYSIWYG模式下，其中一个按钮名为"Insert Widget..."(参见下图)。



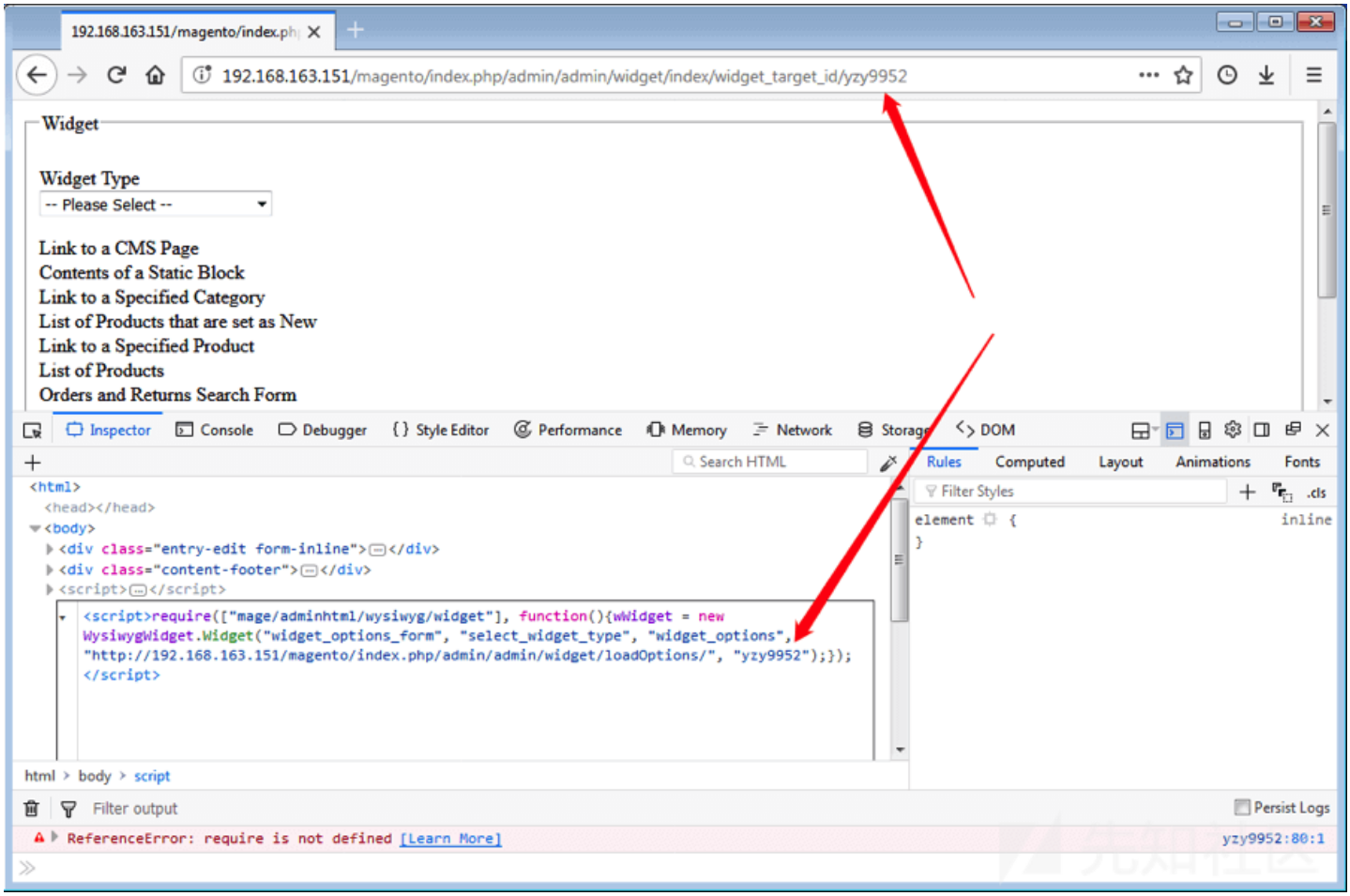
下图中我们发现，可以通过直接访问链接http://IP/magento/index.php/admin/admin/widget/index/ 来调用有插入控件函数的表单。



上图中的表单是由位于/vendor/magento/module-widget/Block/Adminhtml/Widget.php (GitHub link)的Widget.php中的PHP函数生成的，它处理了用户提供的URL，过滤了参数"widget_target_id"的值，并将其插入到一个script标签中，如下图所示。

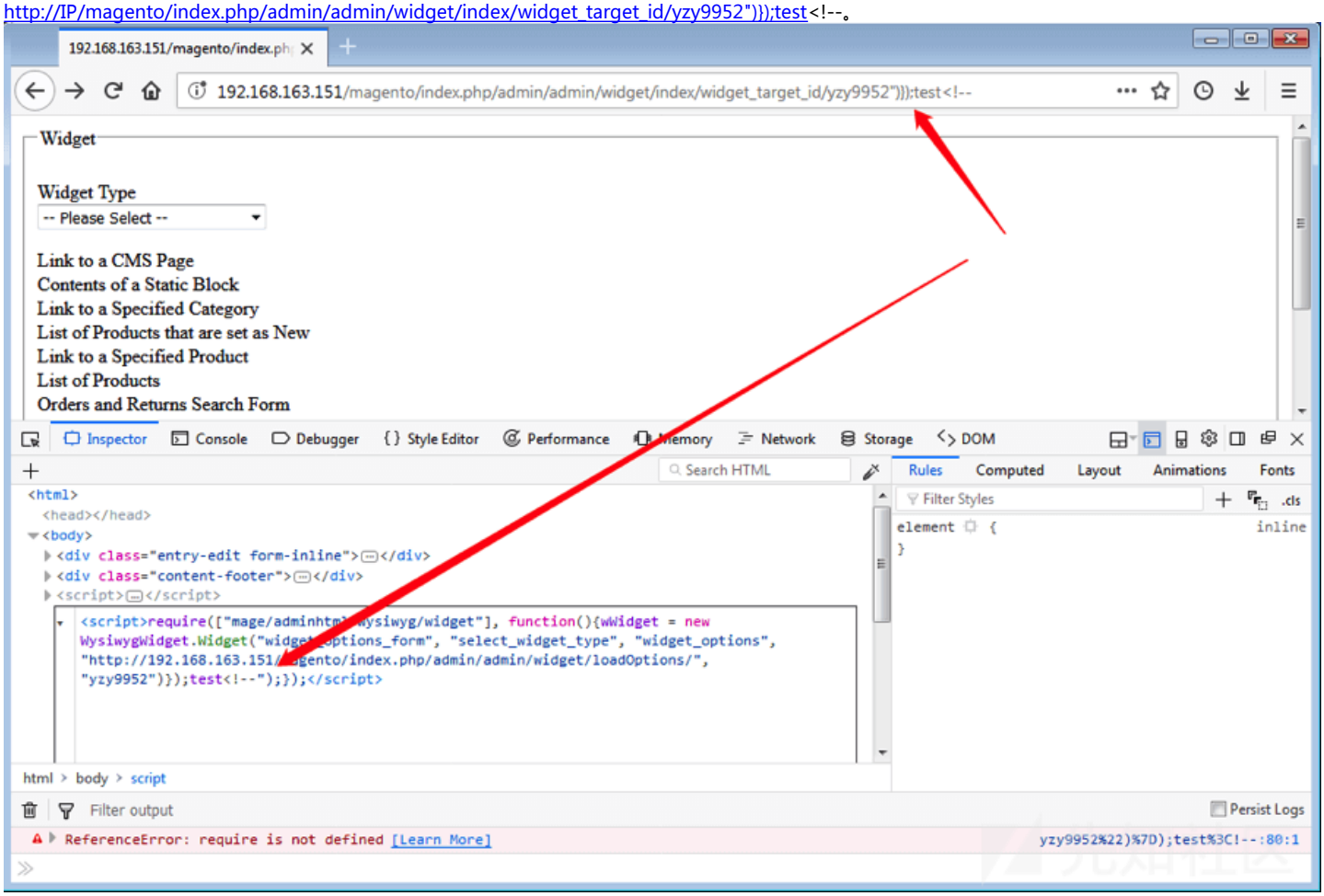
```
$this->_formScripts[] = 'require(["mage/adminhtml/wysiwyg/widget"], function(){wWidget = new WysiwygWidget.Widget(' .
    '"widget_options_form", "select_widget_type", "widget_options", "' .
    $this->getUrl(
        'adminhtml/*/loadOptions'
    ) . '", "' . $this->getRequest()->getParam(
        'widget_target_id'
    ) . '");});';
```

例如，当我们访问 http://IP/magento/index.php/admin/admin/widget/index/widget_target_id/yzy9952链接时，widget_target_id的值将会被插入到script标记中，如图所示。

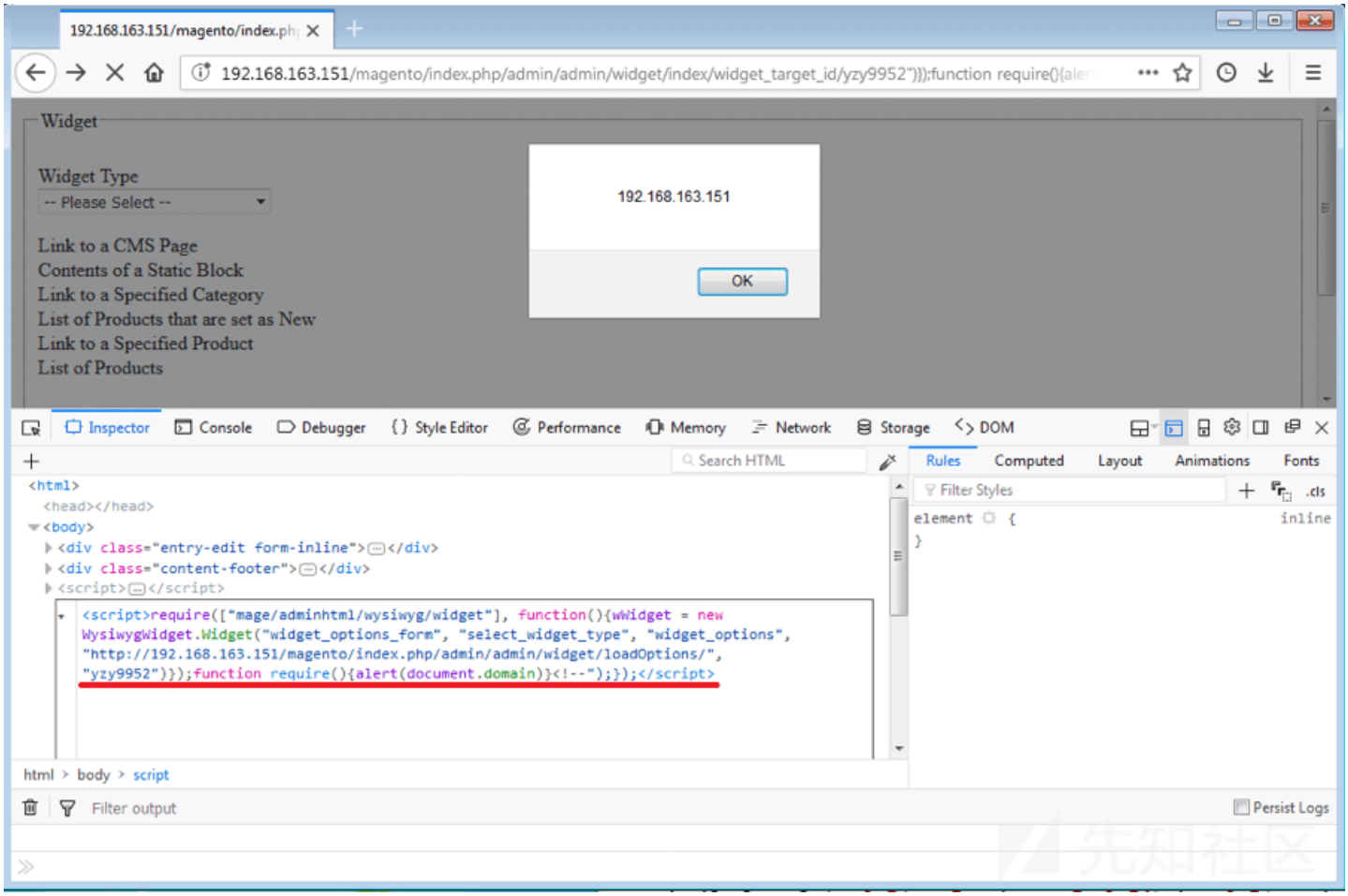


这个函数仅仅通过使用些例如“；”，“””和”}”等符号来闭合用户输入以作为安全处理。然而，这个处理可以通过添加另一组符号，如”}));”来闭合当前函数，并且再利用HTML注

http://IP/magento/index.php/admin/admin/widget/index/widget_target_id/yzy9952"}}));test<!--。



此时，攻击者可以向这个web页面插入任意代码。我们可以看到，在这个script标记开头调用了一个“require”函数，但是这个函数实际上并不存在。我们可以创建一个“requ



解决方案

所有能受攻击的Magento商业版本的用户应该立即升级到最新的Magento版本或应用最新的补丁。此外，已经部署了Fortinet IPS解决方案的组织已经通过以下签名免受此漏洞的影响:Adobe.Magento.Widget.XSS

上一篇：2018安恒杯12月月赛之pwn 下一篇：公链安全之比特币任意盗币漏洞浅析(...

1. 0 条回复
   - 动动手指，沙发就是你的了！