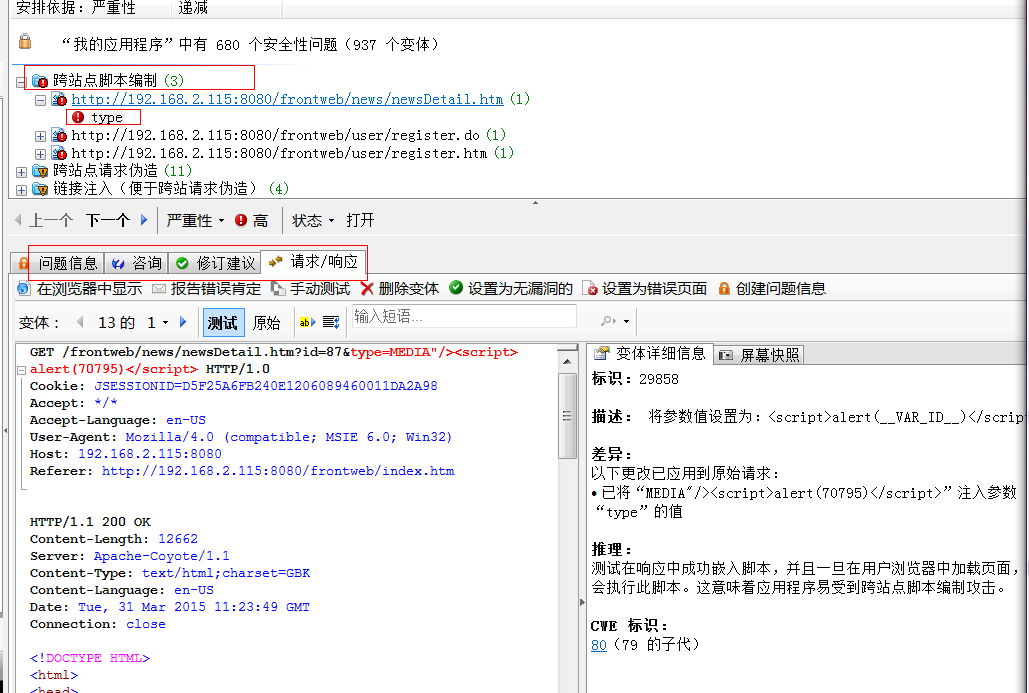
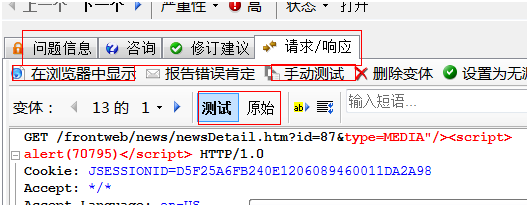
我使用appscan扫描，在报告中针对某一个XSS漏洞进行了学习。以下是我学习的方法，分享大家参考。一起学习。

一、先来看看下图中的这个XSS漏洞，是怎么样的表现形式



|  |  |  |
| --- | --- | --- |
|  | 原始 | 加入脚本后 |
| url | <http://192.168.2.115:8080/frontweb/news/newsDetail.htm?id=87&type=NEW> | [http://192.168.2.115:8080/frontweb/news/newsDetail.htm?id=87&type=MEDIA"/><script>alert(70795)</script>](http://192.168.2.115:8080/frontweb/news/newsDetail.htm?id=87&type=MEDIA) |
| 执行后的区别 | 页面展示这一篇新闻，页面左侧的导航链接为：最新动态>详情 | 页面弹对话框，框的内容为70795。并且页面左侧的导航链接为：">>详情 |
| 执行结果 |  |  |
|  |  |  |

二、在appscan中可以针对脚本进行改动和调试、查看此漏洞的原理，解决方法等



1）问题信息中描述了此漏洞的信息

2）咨询中针对这种漏洞类型进行了详细解释

3）修订建议是解释了怎么去修复这个漏洞，可以学学怎么破漏洞

4）请求/响应中，可以查看原始页面和测试页面的代码，选手动测试时，可以去修改地址去执行；在浏览器中显示，可以直接展示原始或测试页面的结果。

三、理解一下所添加的代码的意义，理解它为什么能发现漏洞，从而去学习怎么现去通过人工的方式来发现类似漏洞。

1）先看下所添加的url中，改动后是：type=MEDIA"/><script>alert(70795)</script>  改之前是：type=NEW

     我们在此漏洞中的”请求/响应“，原始页面中，搜索NEW,可以看到如下图的内容，我们复制出来： <h3><a href="/frontweb/news/newsList.htm?type=NEW ">最新动态</a>>详情</h3>



然后使用同样的方法，取测试中的对应的内容，<h3><a href="/frontweb/news/newsList.htm?type=MEDIA"/><script>alert(70795)</script> "></a>>>详情</h3>



2）我们来分析上面取到的原始代码和测试代码：

原始： <h3><a href="/frontweb/news/newsList.htm?type=NEW ">最新动态</a>>详情</h3>

测试：<h3><a href="/frontweb/news/newsList.htm?type=MEDIA"/><script>alert(70795)</script> "></a>>>详情</h3>

原始地址执行后，页面上展示：最新动态>详情

测试地址执行后，页面上展示：先弹框，然后这块文案为：“>详情

来分析下.

原始代码中，都可以理解，没什么可讲的。看测试代码中，type的值，将原来的NEW，替换为MEDIA"/><script>alert(70795)</script>

一个个解释。”MEDIA“是随便一个单词，可替代的，没有什么特别的意义。

” ”  “ 这个是对应href中前面的那个"，符合html的表达方式。

“/>" 这个是对应a标签，结束a标签的意思。

<script>alert(70795)</script> 这个是script脚本，可被执行。

因href是可执行JS的，所以本测试代码先闭合了href标签，保证符合html的标准，然后在href属性中植入的JS，得到了执行。

3）怎么样去设计测试代码呢？

我讲讲我理解的方法：可以在页面源码中寻找适合JS执行的属性，然后去闭合标签，植入JS。JS执行不成功，不代表一定没漏洞。也有可能是中间做了转义，比如对某些字符，如‘   ”    \   空格等，做了转义，这样的话，可以通过反转义来不断尝试。

**以上是，针对这个漏洞的分析和学习。XSS漏洞的表现形式很多，建议大家一种一种的去理解和分析。**

另附一篇XSS的介绍：<http://www.2cto.com/Article/201211/168950.html>

三、其它找漏洞的方法

上面那个漏洞是通过script脚本来渗透到漏洞的。开发如果过滤了script标签，那上面的漏洞就不存在了。

1）通过html中的body标签中的onload、onerror这样的事件来寻找

<IMG SRC="" onerror="alert('XSS')">   如果场景中存在图片为空的情况，则会执行到这个代码