i春秋url地址编码问题

转载

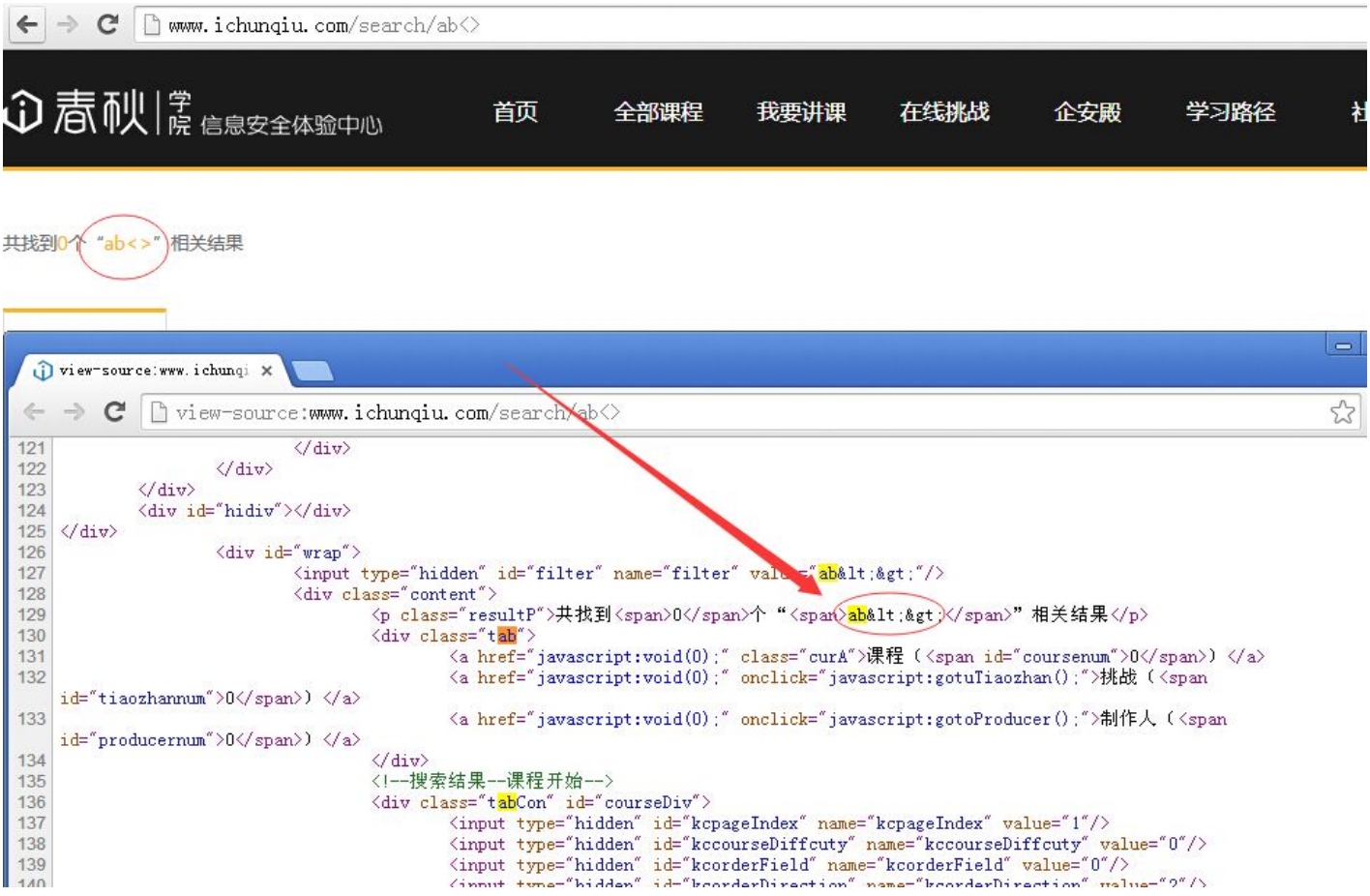
weixin_30378623 于 2015-11-19 22:21:00 发布 62 收藏
原文链接：http://www.cnblogs.com/Lawson/p/4979286.html
版权

i春秋学院是国内比较知名的安全培训平台，前段时间看了下网站，顺便手工简单测试常见的XSS，发现网站搜索功能比较有意思。

其实是对用户输入的内容HTML编码和URL编码的处理方式在这里不合理，提交到乌云被拒绝了，因为确实没啥危害，因此技术BLOG记录下。

如搜索：http://www.ichunqiu.com/search/ab<>，搜索内容为ab<>，页面会把<>做html编码后在页面展现，这样看起一切正常。

如：



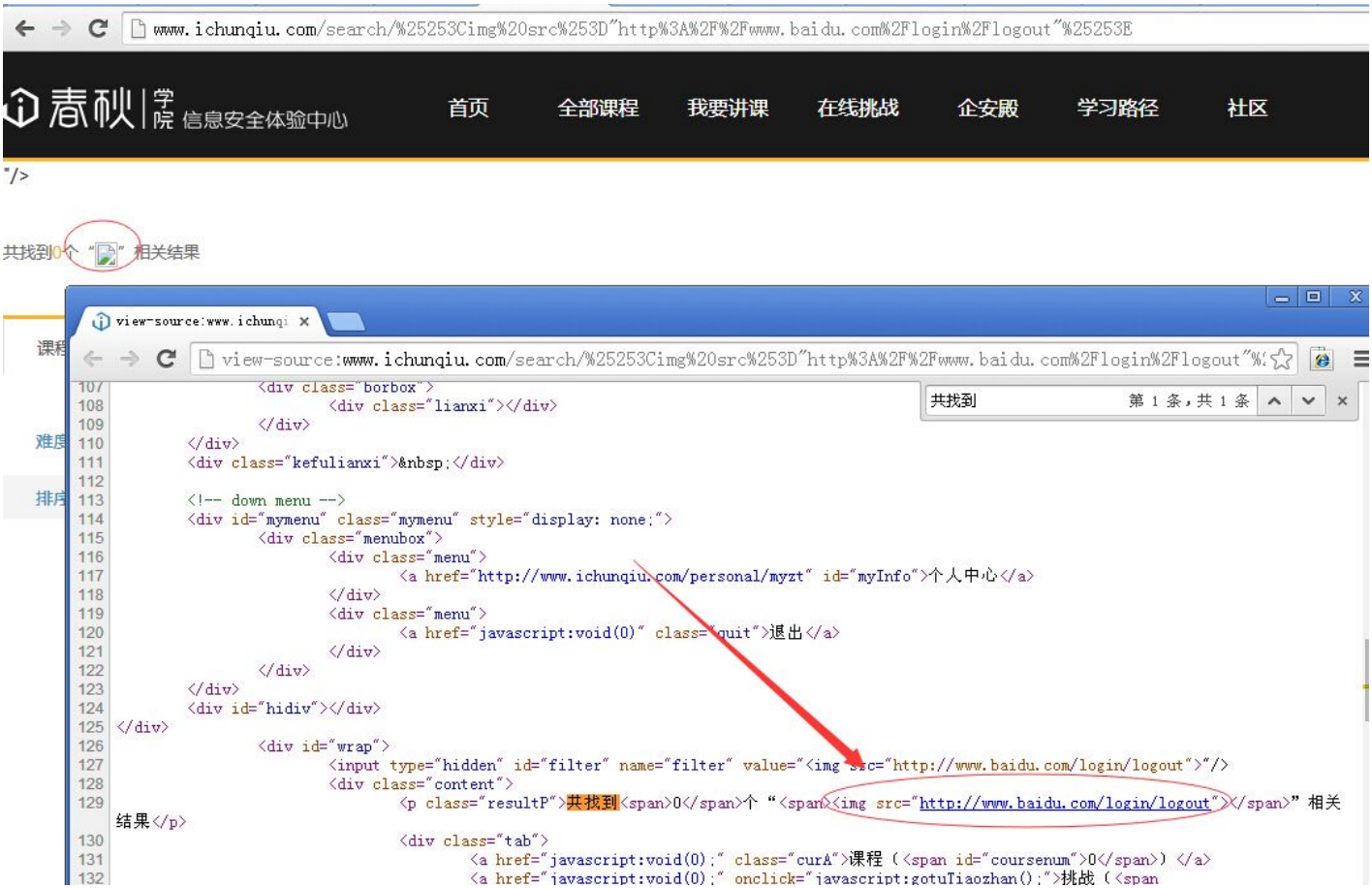
但经过多次分析，发现把搜索的内容用URL多次编码或html多次编码后，服务端后台都会自动解码然后输出到客户端，那是否可以把恶意的标签通过多次编码后来搜索，伪造一个URL地址，达到XSS的攻击效果呢。

结果经过多次测试，发现虽然多次URL和HTML编码后，后台会自动解码，但输出到客户端前，会再次对输出的内容做安全性检测，导致不能XSS。

比如输入：%25253Cimg%20src%253D"http%3A%2F%2Fwww.baidu.com%2Flogin%2Flogout"%25253E

该内容是标签：<img src="http://www.baidu.com/login/logout">，经过URL多次编码的效果，实际把英文字母用HTML多次编码一样可以，之前测试的时候用iframe,javascript等，都经过html多次编码字母内容也可以绕过，但输出到客户端时服务端又做了处理，所以导致不能XSS。

效果如下：



要是把img里的内容换成<img src="http://www.ichunqiu.com/login/logout">，则访问这个的地址会自动退出该网站。

最终没有对用户和网站造成任何安全影响，但觉得html这样处理的方式适合多文本框输入输出的处理方式，不适合对搜索内容的编码处理方式。

转载于:https://www.cnblogs.com/Lawson/p/4979286.html