XSS之攻击与防御——安全小课堂第七期

2016-04-22 京东安全应急响应中心

安全小课堂第七期

在不少人看来，XSS漏洞造成的危害程度并不大，或者说，一个XSS漏洞的可利用价值并不高。但很多时候看起来一个不起眼的XSS漏洞，在高人的手里，就可能做出一番大动作。本期我们来聊一聊XSS之攻击与防御。

今天的特邀嘉宾是TSRC高级安全研究员深夜饮酒和唯品会高级安全研究员李帅，列队欢迎~

1

豌豆妹

简单介绍下XSS漏洞的分类呗~

小丸子

XSS常年位居Web top10漏洞之列。一般传统的分类，有反射型XSS、持久型XSS（包括存储、 DOM等类别）。根据跨站的成因或者特征进行分类，有Flash跨站、mXSS跨站、UBB跨站、宽字节跨站等等。当然这些分类有很多重叠的部分。

哆啦A梦

国外比较精确的将跨站分类为：服务端跨站（Server XSS）、客户端跨站（Client XSS），然后再细分反射型或者存储型等。这种分类是根据漏洞形成点的位置来看的。

豌豆妹

mXSS跨站、UBB跨站这类能详细介绍下么？

小新

mXSS 主要是在DOM操作的过程中浏览器渲染造成的畸变引起的。比如，将数据赋值到a.innerHTML后，再取出重新赋值到b.innerHTML的过程中产生畸变。UBB主要是论坛里用的比较多，如果存在XSS的话，可以类似这样利用：[img]javascript :alert();[/ img]，在转成html代码的时候造成跨站。

2

豌豆妹

在这些分类中，危害和影响最大的是哪个呢？

葫芦娃

一般来说存储型跨站危害相对较严重，攻击面也较广。此外，反射型的危害也不小。self-xss配合一些csrf漏洞，也可以达到利用效果。总体来说，企业反射型跨站出现的多一点。黑客可以钓鱼，或注入木马、广告链接。有些在主站注入非法网站的链接，对公司声誉还是有影响的。很多广告联盟等也会利用XSS跟踪用户行为，窃取用户数据等，利用跨站请求一些JSONP接口获取用户数据。

3

豌豆妹

分享下XSS漏洞的防御措施吧！

哆啦A梦

我们目前在做一个框架过滤，Java平台在做filter，通过filter做输入拦截。要全部开放使用，可能还需要再观察下。公司到一定量级后统一框架还是很难的，在现有基础上如何找到一个权衡点非常重要。

豌豆妹

是否可以分享下针对检测层面和主动检查层面的实践经验呢？

小丸子

一般反射型跨站比较容易检测。像DOM型跨站 ，我们现在有专门策略去扫描，会模拟webkit内核渲染网页并解析JS，根据执行结果来判断。相对来说误报率还是比较低的。

4

豌豆妹

业内是否有检测XSS漏洞好用的工具？

葫芦娃

kali里面有集成一些比较知名的检测工具，例如XSSER等。这种检测一般是上线前需要进行安全评审的规范环节之一。

葫芦娃

如何快速精准的发现XSS，降低垃圾数据呢？

小新

我们在检测XSS时都是用不同的语句去尝试，如果尝试的较多就会造成库中存储很多“脏”数据，对于测试环境还好，线上环境可能业务部门经常会报警了。针对这种情况，一般我们会有专门的扫描账号去进行检测，避免对正常业务的干扰。另外，扫描器有时候还会删除数据，针对这个问题，可以做个高危URL配置项来避免。

豌豆妹

扫描器漏报误报的问题，有什么方法解决吗？

哆啦A梦

可以把扫描规则策略做成插件式，还可以根据场景优化，缓解误漏报问题。

葫芦娃

分享个思路：是否可以针对检测范围做个基线性的安全检查，对结果做一次判定，误报的加flag，后续检测中如果一直为误报可加入黑名单。对于SRC来说也是一个好的思路收集，我们经常会把外部爆出来但扫描器没有发现的XSS构造语句放到扫描器中。

豌豆妹

哈哈~大家真是集思广益啊，不知屏幕前的你是否意犹未尽呢？这只是本期话题探讨内容的冰山一角，想知晓更多详细信息，拥有和大牛们积极互动的机会，请关注JSRC并成为我们的核心白帽子喲~下期话题由你决定。回复本公共微信号，快来告知你最想了解的话题吧！




安全小课堂往期回顾：

1、论安全响应中心的初衷；
2、安全应急响应中心之威胁情报探索；
3、论安全漏洞响应机制扩展；
4、企业级未授权访问漏洞防御实践；
5、浅谈企业SQL注入漏洞的危害与防御；
6、信息泄露之配置不当。

JSRC http://security.jd.com/

长按识别左侧二维码，关注我们