

聊聊XML注入攻击

2016-07-29 京东安全应急响应中心

安全小课堂第二十期

XML注入通过构造恶意内容，可导致权限绕过及伪造、读取任意文件、执行系统命令、探测内网端口（SSRF等）、攻击内网网站等危害，后果严重，本期我们来聊一聊XML注入攻击。

本期邀请到了
安识科技安全专家神奇四侠
唯品会安全专家feng
大家欢迎~

1



豌豆妹

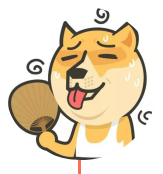
能说说XML注入的攻击原理么？



葫芦娃

XML 指可扩展标记语言，XML 被设计用来传输和存储数据。XML注入一般指在请求的XML数据中插入攻击利用代码，根据不同的场景，可能会形成以下的漏洞形式：

- 1、xee XML Entity Expansion；
- 2、xxe XXE Injection即XML External Entity Injection；
- 3、soap注入；
- 4、XPath注入。



小柴

我觉得是攻击者对XML插入了一些恶意构造的数据或者一些payload，达到了一些攻击效果。



豌豆妹

那形成原因呢？



哆啦A梦

个人觉得，是因为研发人员对用户输入的XML内容没有做合法性校验，安全性过滤，没有了解过常见的危害。研发人员毕竟不是安全人员，仍然需要安全教育和培训指导。

2



豌豆妹

XML注入的攻击方式有哪些呢？



小新

- 1、XML数据注入 (XML Data Injection) ；
- 2、XML外部实体注入(XML External Entity) XXE ；
- 3、可扩展样式表语言转换 (Extensible Stylesheet Language Transformation , XSLT) 注入 ；
- 4、XPath/XQuery注入 ；
- 5、SOAP webservice注入等。



针对不同类型的xml注入，会有不同的攻击利用方式，比如soap注入就是利用sql注入的原理，而xxe、xee等，则需要借助实体来进行利用。



豌豆妹

对于XML外部实体注入，如果读取的文件本身就是xml或者存在特殊字符的情况下，怎么能把他发送出来呢？主要是java和.net的。



小丸子

遇到这种，我们知道php可以使用php:// 协议base64-encode来读取。
不同程序支持的协议不一样，下面是一些可以选择的协议：

libxml2	PHP	Java	.NET
file http ftp	file http ftp php compress.zlib compress.bzip2 data glob phar	http https ftp file jar netdoc mailto gopher *	file http https ftp



豌豆妹

能说说XML注入攻击的危害么？

葫芦娃



危害方面，我觉得有很多。通过构造恶意内容，可导致权限绕过及伪造、读取任意文件、执行系统命令、探测内网端口（SSRF等）、攻击内网网站等危害。还有可能有DOS，也就是xee漏洞。soap注入的话，那么就是数据丢失。

4

豌豆妹



那检测XML注入攻击的小工具有哪些呢？

小新



小工具的，有 BurpSuite，AWVS，或者自写Python脚本。

豌豆妹



xpath注入的场景能列举一些吗？

哆啦A梦



xpath注入的场景确实比较少，主要出现在利用xml进行数据存储的时候，也就是当使用

xml取代mysql这种数据库的功能时。我自己构造了一个简单的场景，就是用xml进行用户信息存储的。在登陆的场景时候 当用户登录请求是以下情况时，就可以正常登陆：
//user[username/text()='Jhon' and password/text()='123456']。如果有一个字段与xml存储的不一样就拒绝登陆，那么这个时候我们就可以利用sql注入绕过登陆的思路来了。构造以下请求可以登录
//user[username/text()='John' and password/text()=' or 'a'='a']。

```
<userBook>
  <user>
    <username>John</username>
    <password>123456</password>
    <email>John@vip.com</email>
  </user>
  <user>
    <username>Lucy</username>
    <password>123456</password>
    <email>Lucy@vip.com</email>
  </user>
</userBook>
```

5



豌豆妹

那如何预防XML注入呢？



小柴

禁用外部实体；判断数据合法性；过滤非法数据。上层弄个WAF拦截和可疑数据包分析告警，应该也挺好。



豌豆妹


hhha~感谢！今天就聊到这儿，本宝宝意犹未尽呢~下期再见哟！

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；
- 7、XSS之攻击与防御；
- 8、电商和O2O行业诈骗那些事儿（上）；
- 9、电商和O2O行业诈骗那些事儿（下）；
- 10、CSRF的攻击与防御；
- 11、账户体系安全管理探讨；
- 12、远程代码执行漏洞的探讨；
- 13、服务器安全管控的探讨；
- 14、畅谈端口安全配置；
- 15、谈一谈github泄露；
- 16、撞库攻击是场持久战；
- 17、url重定向攻击的探讨；
- 18、聊聊弱口令的危害（一）；
- 19、聊聊弱口令的危害（二）。



 jsrc_team

 京东安全应急响应中心

动动手指~关注下呗~

