安全小课堂第121期【URL注入攻击】

京东安全应急响应中心 2018-12-05

URL注入攻击，与XSS、SQL注入类似，也是参数可控的一种攻击方式。URL注入攻击的本质是URL参数可控。攻击者可通过篡改URL地址，修改为攻击者构造的可控地址，从而达到攻击目的。

JSRC **安全小课堂第121期**，邀请到**IT小丑**作为讲师就**URL注入攻击**为大家进行分享。同时感谢小伙伴们的精彩讨论。

URL注入概念?

京安小妹

IT小丑：

输出HTML、JS，可引发XSS跨站攻击

调用SQL语句，可引发SQL注入攻击

使用SHELL命令，可引发OS命令注入

URL参数可控，可引发URL注入攻击

URL注入攻击与XSS跨站、SQL注入类似，也是参数可控的一种攻击方式。URL注入攻击的本质就是URL参数可控。攻击者可通过篡改URL地址，修改为攻击者构造的可控地址，从而达到攻击的目的。

URL注入攻击思路?

京安小妹

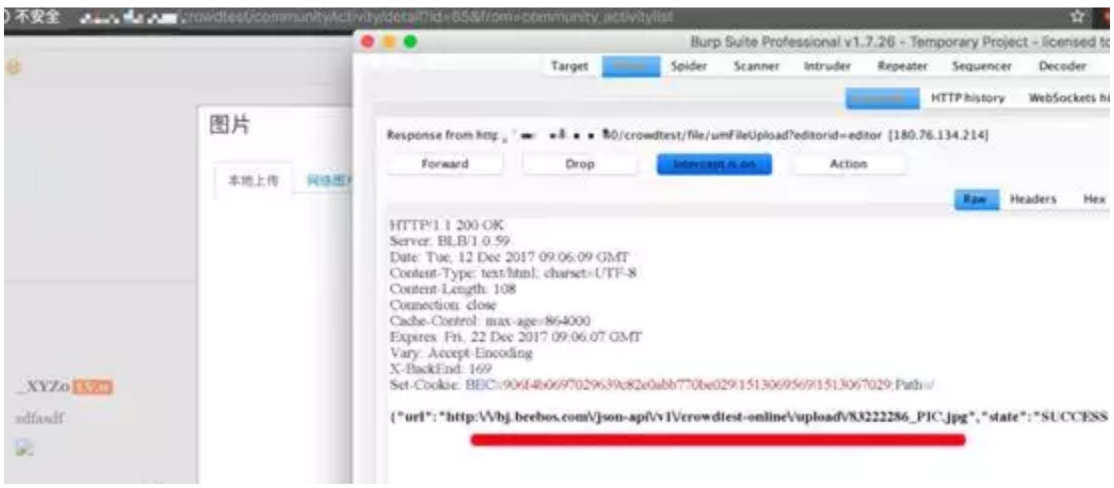
IT小丑：

安全届至理名言：永远不要相信用户的输入。

使用经典的输入——处理——输出模型来看Web应用，在有输入的地方，或者用户可控的地方均可能存在安全风险，处理过程和输出过程亦会产生安全风险。

攻击思路来源和某SRC审核小哥哥的撕逼，内容如下：“你好，非常感谢提交漏洞，该问题的核心我们认为是没有对提交的内容进行过滤，可以使用不可控的URL作为输入。这仅是针对这个网站而言的。但……”

URL可控，那但凡涉及到传递URL参数的地方均可能存在安全隐患。



URL注入漏洞测试方法很简单，只需要有一台公网可访问的VPS服务器，如想如虎添翼，可另配置一个401认证页面，并记录输入账号密码。

讲师

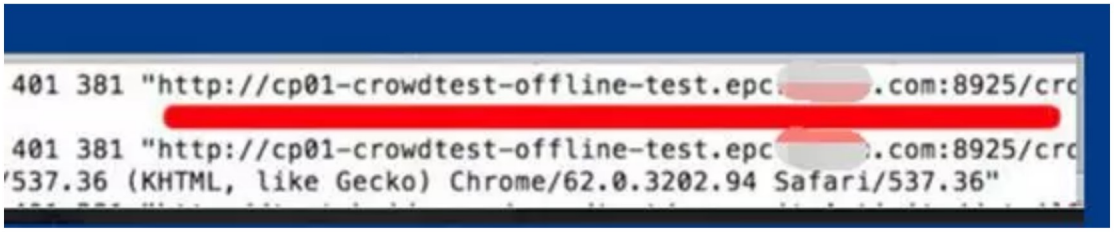
URL注入攻击漏洞的危害?

京安小妹

IT小丑：

1.管理后台

查找管理后台的方法：字典爆破、搜索引擎、Robots.txt、信息泄漏、社工等等，URL注入攻击，有时可以帮助你找到管理后台地址。



2.跨站XSS

URL可控处，输入XSS Payload，某些页面会加载此处URL地址，使用img标签，这时可能存在安全风险，导致跨站问题。

讲师

URL注入攻击的挖掘技巧?

京安小妹

IT小丑：

但凡传递URL参数的地方均有可能存在问题，常见的URL参数梳理如下：go、return、returnTo、logout、register、login、returnUrl、path、redirectURI、redir、returl share、wap、url、link、src、source、target、u、3、display、sourceURI、imageURL、domain。具体是哪个参数，取决于天马行空的程序员，但是如果看到某个请求中含有http://|https://开头的内容，不妨尝试替换一下。

另外，某些情形下，可能对域名做了限制，这时候可以尝试绕过，这里绕过的技巧类似URL重定向绕过或SSRF绕过技巧。主要说一下畸形构造绕过，当然也可以Fuzzing，畸形构造主要涉及如下字符：";"、"/"、"\"、"?"、":"、"@"、"="、"&"、"."。常见bypass方式：

a. 单斜线"/"绕过

https://www.xxx.com/redirect.php?url=/www.evil.com

b. 缺少协议绕过

https://www.xxx.com/redirect.php?url=//www.evil.com

c. 多斜线"/"前缀绕过

https://www.xxx.com/redirect.php?url=///www.evil.com

https://www.xxx.com/redirect.php?url=////www.evil.com

d. 利用"@"符号绕过

https://www.xxx.com/redirect.php?url=https://www.xxx.com@www.evil.com

e. 利用反斜线"\"绕过

https://www.xxx.com/redirect.php?url=https://www.evil.com\https://www.xxx.com/

f. 利用"#"符号绕过

https://www.xxx.com/redirect.php?url=https://www.evil.com#https://www.xxx.com/

g. 利用"?"号绕过

https://www.xxx.com/redirect.php?url=https://www.evil.com?www.xxx.com

h. 利用"\\"绕过

讲师

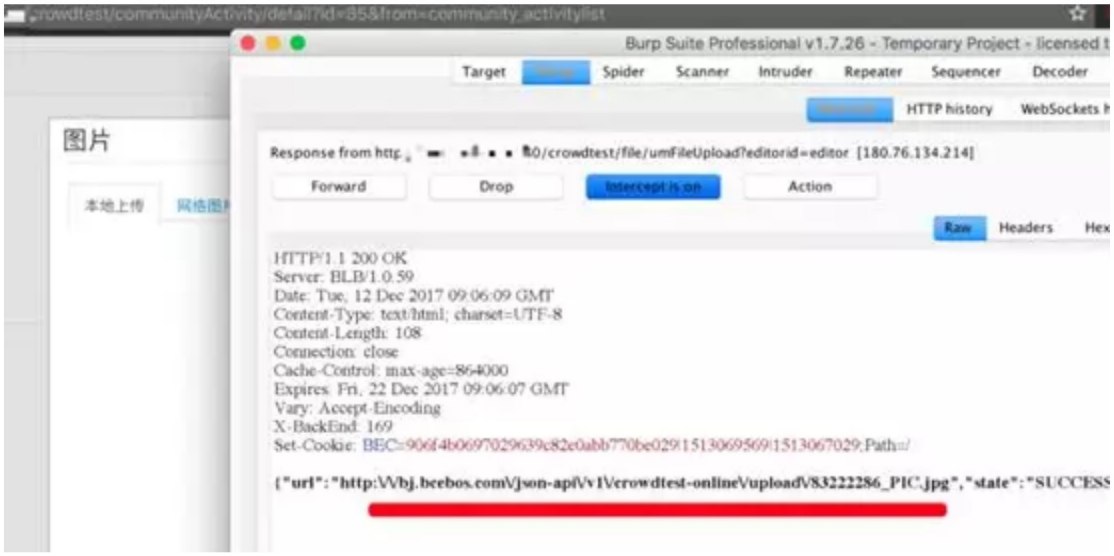
URL注入攻击的案例分析?

京安小妹

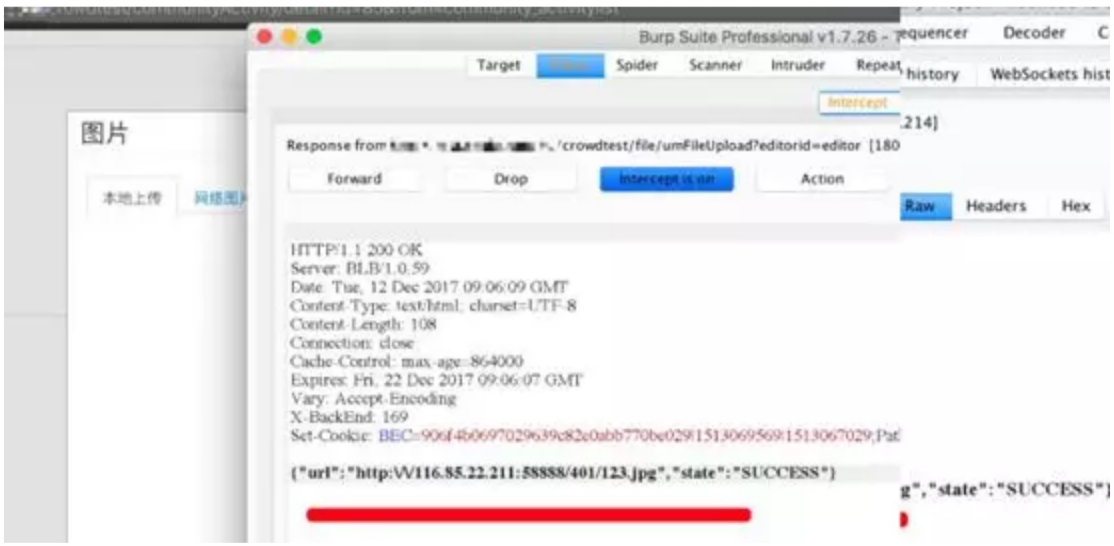
IT小丑：

某站点上传图片进行演示

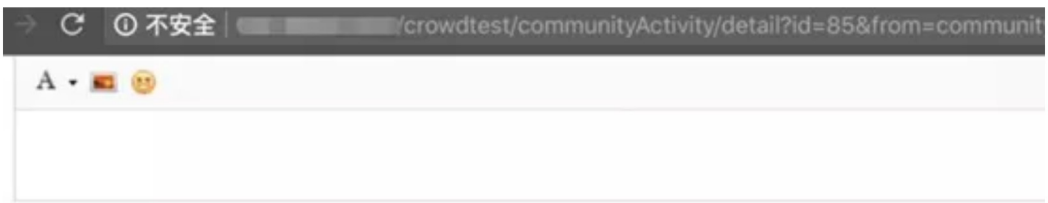
1上传时候，抓数据包，查看返回数据包内容



2.修改返回数据包URL地址，此处改为某401认证页面地址



3.放过数据包，进行保存



讲师

URL注入攻击的防御手段?

京安小妹

IT小丑:

检测URL中是否含有特殊字符;

对加载URL域进行检测，可正则匹配xxx.com域，只允许该域下地址;

讲师

互动问答环节:

1.如何利用401基础认证钓鱼?

讲师:

你先有台服务器，自定义一个401，然后配置一下，让日志记录输入的账号、密码，

2.如何利用URL注入获取后台地址?

讲师:

管理员访问你插入的URL后，后台地址会显示在Referer中。

3.如何把URL注入利用最大化?

讲师:

URL注入可以结合不同的环境、不同的场景，利用姿势很多，组合利用可能会有更大的危害。

本期JSRC　安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心