url重定向攻击的探讨

京东安全应急响应中心 2016-07-08

安全小课堂第十七期

由于应用越来越多的需要和其他的第三方应用交互，以及在自身应用内部根据不同的逻辑将用户引向到不同的页面，譬如一个典型的登录接口就经常需要在认证成功之后将用户引导到登录之前的页面，整个过程中如果实现不好就可能导致一些安全问题，特定条件下可能引起严重的安全漏洞。本期我们来聊一聊url重定向攻击。

本期小课堂邀请到
通付盾安全专家疯子
唯品会安全专家Look。

1

豌豆妹

哪些位置易出现url跳转？

小柴 

一般在登陆，提交，返回，退出等业务页面切换处容易出现url跳转漏洞。

2

豌豆妹

能说说url跳转的危害么？

能说说url跳转的危害么？

哆啦A梦

首先普及下url漏洞原理：在跳转链接中，攻击都可修改可疑参数为我们任意构造的url，根据是否跳转到指定地址判断漏洞是否存在。
url跳转漏洞危害用一句话来说，可大可小，可发挥空间大。常见的漏洞利用方式如下：
1、 钓鱼：结合存在漏洞网站（电商，银行、游戏等）的线上业务，如中奖，领券，账户异常等活动，利用url跳转欺骗用户跳转到指定的钓鱼网站，收集用户账户密码、银行卡密码、身份证等重要信息。
2、 其它的利用方式还有：读取服务器本地文件或探测内网。具体来说，目标网站后端使用curl库，同时未设置跳转过滤规则，攻击者就可以利用url跳转漏洞对服务器进行本地文件读取，当未设置网络边界时可对目标网站内网进行探测，甚至漫游目标内网。

小新

钓鱼的欺诈风险在于用户是否信任这样一个网站，例如百度网站我可信，可在手机端是隐藏url链接，用户在手机端访问不知不觉就去了一个钓鱼页面，也有因此被盗了资金。url上也有许多客户端的欺骗，例如在qq客户端中绕过绿色认证，让客户以为是信任网站，结果绕过认证进入欺诈网站，也是在url上进行欺骗。

3

豌豆妹

如何去发现url跳转呢？

哆啦A梦

邮箱、vpn这些边界点是最有效的途径，然后结合账号信息收集，密码字典进行下一步，这些是对企业安全最为危害的。

葫芦娃

修改可疑参数为我们任意构造的url，根据是否跳转到指定地址判断漏洞是否存在。当然也有些非参数的url跳转。利用协议实现跳转，如http://www.test.com@jd.com会跳转到www.jd.com，@字符前的信息被解析为登陆信息，@后被解析为主机信息，从而实现跳转。

4

豌豆妹

是否可以在代码阶段发现这个问题呢？

小柴

可以但不完整。因为跳转逻辑常常多由javascript实现，测试url漏洞主要以灰盒测试为主，如果后台没有对跳转参数进行过滤，且未加入referer或token等限制条件，那么跳转参数将存在跳转漏洞。

5

豌豆妹

那如何防御这种情况的出现呢？

葫芦娃 

1、签名验证。如果跳转的url事先可以确定，可以对跳转链接后端进行签名验证或token验证以防篡改。
2、白名单限制。如果跳转的url事先不确定，后端建立跳转过滤规则，保证跳转的url来自可信域。
3、还有一点就是要设置网络边界，对内外网系统进行访问边界访问控制。
当然，在建立过滤规则时，不能太过简单，应该考虑全面，防止绕过。

豌豆妹

能介绍下现在常见的绕过方式么？

葫芦娃 

现在常见的绕过方式中，有正则字符过滤不严导致的绕过，如www.test.com/autoLogin?r=http://www.1test.com 或www.test.com/autoLogin?r=http://test.com.test.com也有url地址转换导致的绕过，如base64加密、短地址、数字ip地址、特殊自带地址加密等。还有一种特殊的绕过方式进行url跳转利用。正常访问http://www.test.com/跳转到http://www.test.com/home。当我们特殊构造如下访问链接：http://www.test.com//evil.com访问后跳转到http://evil.com/home。要注意的是后面是两个斜杠。可以看到后端在提取主机时是提取最后一个主机，这类似http参数污染(HPP)漏洞，有异曲同工之处。

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。

jsrc_team

京东安全应急响应中心

动动手指~关注下呗~