浅谈SSRF漏洞—安全小课堂第三十一期

2016-10-28 京东安全应急响应中心

安全小课堂第三十一期

企业对安全的防护往往针对于外网，相对于外网，内网的安全一般做得比较鸡肋，而SSRF漏洞正好为外网与内网之间打开了大门，让原本看似固若金汤的防护瞬间崩塌，为企业和个人带来了巨大危害，轻则导致内网服务器及系统相关敏感信息泄漏，重则导致内网漫游，结合其它漏洞获取内网系统webshell以及进行内网渗透，敏感数据被窃取。本期，我们来聊一聊SSRF漏洞。

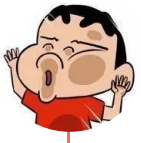
本期我们邀请到
优酷安全专家PyNerd
唯品会安全专家LooKe
猪八戒网Ant
大家欢呼
ヽ(*°▽°*)ノ

/ 01 /

豌豆妹

SSRF是什么？

小新



SSRF(Server-Side Request Forgery ，服务器端请求伪造)是一种由攻击者构造形成由服务器发起请求的一个安全漏洞，SSRF的主要攻击目标为外网无法访问的内部系统。

/ 02 /

豌豆妹

SSRF形成的原因有哪些呢？

小丸子 

SSRF形成的原因是服务端提供了从其他服务器应用获取数据的功能，在用户可控的情况下，未对目标地址进行过滤与限制，导致此漏洞的产生。

哆啦A梦 

比如从指定URL地址获取网页文本内容，加载指定地址的图片等，都是SSRF容易出现的点。图片地址这种较为常见，其它的发生点，需要具体情况具体判断。

葫芦娃 

对内网IP和端口进行扫描，也能获取内网的系统指纹，同时对内网主机发起请求，经过精心的构造还可以获得内网主机的权限，从而进一步的对内网渗透。

/ 03 /

豌豆妹

攻击者利用SSRF可以实现的攻击有哪些呢？

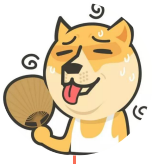
小新 

就我看来，攻击者利用SSRF可以实现的攻击主要有3种：

1、获取web应用可达服务器服务的banner信息以及收集内网web应用的指纹识别，如开放的端口，中间件版本信息等。
2、攻击运行在内网的系统或应用程序，获取内网各系统弱口令进行内网漫游、对有漏洞的内网web应用实施攻击获取webshell，如st2命令执行、discuz ssrf通过redis实施getshell等。
3、利用有脆弱性的组件结合ftp://,file:///,gopher://,dict://等协议实施攻击。如FFmpeg任意文件读取，xxe攻击等。

豌豆妹

有什么好的方式检测正在实施的SSRF攻击呢？

柴可夫斯基 

SSRF是含有一定特征性的，一般一个接口，异常的请求内网IP，在日志系统中都有记录，且很可能是连续性的，因为他要猜测，所以在一定时间段会有明显的请求量。你可以通过这个特征去做初步判断。

/ 04 /

豌豆妹

防御SSRF的攻击的必要性能说说么~

小丸子 

企业对安全的防护往往针对于外网，相对于外网，内网的安全一般做得比较鸡肋，而

SSRF漏洞正好为外网与内网之间打开了大门，让原本看似固若金汤的防护瞬间崩塌，为企业和个人带来了巨大的危害，轻则导致内网服务器及系统相关敏感信息泄漏，重则导致内网漫游，结合其它漏洞获取内网系统webshell以及进行内网渗透，敏感数据被窃取。

/ 05 /

豌豆妹

既然如此重要，那如何防御SSRF呢？

葫芦娃 

1、过滤返回信息，验证远程服务器对请求的响应是比较容易的方法；
2、统一错误信息，避免用户可以根据错误信息来判断远端服务器的端口状态；
3、限制请求的端口为http常用的端口，比如，80,443,8080,8090；
4、黑名单内网ip。避免应用被用来获取获取内网数据，攻击内网；
5、禁用不需要的协议。仅允许http和https请求；
6、使用正则对参数进行效验，防止畸形请求绕过黑名单。

 哆啦A梦

收集了些自己看过的文章，有兴趣的小伙伴可以去具体看看：

http://www.freebuf.com/articles/web/20407.html；
https://sobug.com/article/detail/11；
http://bobao.360.cn/learning/detail/2502.html；
https://habrahabr.ru/company/mailru/blog/274855/；
http://docs.ioin.in/writeup/xdxd.love/_2016_01_18_ffmpeg_SSRF_E6_BC_8F_E6_B4_9E_E5_88_86_E6_9E_90_/index.html；
http://bobao.360.cn/learning/detail/2889.html；
http://mp.weixin.qq.com/s?__biz=MzI0NjQxODg0Ng==&mid=2247483798&idx=1&sn=65cdf852dffd63b9d4ec41c31d9a5365；
https://docs.google.com/document/d/1v1TkWZtrhzRLy0bYXBcdLUedXGb9njTNIJXa3u9akHM/edit#heading=h.um15e9fhmngt；
http://fuzz.wuyun.org/src/build_your_ssrf_exp_autowork.pdf；
http://docs.ioin.in/writeup/blackbap.org/_thread_7416_1_1_html/index.html；
http://wufeifei.com/ssrf/；
http://docs.ioin.in/writeup/xdxd.love/_2016_10_19_discuz_E6_9C_80_E6_96_B0_E7_89_8820160601_SSRF_E6_BC_8F_E6_B4_9E_E5_88_86_E6_9E_90_/index.html。

豌豆妹

那有哪些常用的绕过方法和利用方法呢？

小新

绕过的方法有ip地址转换、url跳转、短网址绕过、xip.io绕过。在获取内网系统的指纹后(如resin、struts2)，可以配合任意文件读取、命令执行获取更多权限和信息，比如这个：http://wooyun.jozxing.cc/static/bugs/wooyun-2016-0187550.html。
比如wp的通过pingback实现的SSRF，是通过gethostbyname函数发起的请求，那就检测请求的域名咯~

```
532         if ( ! $same_host ) {
533                 $host = trim( $parsed_url['host'], '.' );
534                 if ( preg_match( '#^(([1-9]?\d|1\d\d|25[0-5]|2[0-4]\d)\.){3}([1-9]?\d|1\d\d|25[0-5]|2[0-
    4]\d)$#', $host ) ) {
535                         $ip = $host;
536                 } else {
537                         $ip = gethostbyname( $host );
538                         if ( $ip === $host ) // Error condition for gethostbyname()
539                                 $ip = false;
540                 }
541                 if ( $ip ) {
542                         $parts = array_map( 'intval', explode( '.', $ip ) );
543                         if ( 127 === $parts[0] || 10 === $parts[0] || 0 === $parts[0]
544                                 || ( 172 === $parts[0] && 16 <= $parts[1] && 31 >= $parts[1] )
545                                 || ( 192 === $parts[0] && 168 === $parts[1] )
546                         ) {
547                                 // If host appears local, reject unless specifically allowed.
548                                 /**
549                                  * Check if HTTP request is external or not.
550                                  *
551                                  * Allows to change and allow external requests for the HTTP request.
552                                  *
553                                  * @since 3.6.0
554                                  *
555                                  * @param bool   false Whether HTTP request is external or not.
556                                  * @param string $host IP of the requested host.
557                                  * @param string $url  URL of the requested host.
558                                  */
559                                 if ( ! apply_filters( 'http_request_host_is_external', false, $host, $url ) )
560                                         return false;
561                         }
562                 }
563         }
564
```



微信公众号：jsrc_team
新浪官方微博：
京东安全应急响应中心

固定栏目

技术分享 | 安全意识 | 安全小课堂