php伪协议语法,php文件包含漏洞（input与filter）

转载

weixin_39881167 于 2021-03-10 01:18:57 发布 678 收藏
文章标签： php伪协议语法

php://input

php://input可以读取没有处理过的POST数据。相较于$HTTP_RAW_POST_DATA而言，它给内存带来的压力较小，并且不需要特殊的php.ini设置。php://input不能用于enctype=multipart/form-data。

php://filter协议

协议语法：

php://filter:/=

php://filter 的 参数列表

read	读取
write	写入
resource	数据来源(必须的)

read的参数

string.strip_tags	将数据流中的所有html标签清除
string.toupper	将数据流中的内容转换为大写
string.tolower	将数据流中的内容转换为小写
convert.base64-encode	将数据流中的内容转换为base64编码
convert.base64-decode	与上面对应解码

漏洞应用

以i春秋上一道文件包含的CTF题为例：(来自rgrgrgrgrggrgrg大佬的Writeup)

```
show_source(__FILE__);

if(isset($_REQUEST['path'])){

include($_REQUEST['path']);

}else{

include('phpinfo.php');

}
```

path能以get与post形式传入，这里我们在url后加上?path=php://input,再以post形式传入ls指令，成功执行了指令。

```php
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

dle345aae.php index.php phpinfo.php

于是利用filter协议来读取dle345aae.php的内容，由于php文件不能直接读取，于是采用base64编码方式读取，成功得到一串base64编码，拿去一解就是flag啦。

```php
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

PD9waHAgCiRmbGFnPSJmbGFnezU1YThhN2YxLTAzMzQtNGVlMS1hZWNkLThiM2JhOTUzOTY0OX0iOwo=

php://filter(文件包含漏洞利用)及php://input

1. php://filter 文件包含漏洞:https://blog.csdn.net/fageweiketang/article/details/80699051 筛选过滤应用: 1. 字符串过滤 ...

PHP文件包含漏洞剖析

一. 什么才是”远程文件包含漏洞”?回答是:服务器通过php的特性(函数)去包含任意文件时,由于要包含的这个文件来源过滤不严,从而可以去包含一个恶意文件,而我们可以构造这个恶意文件来达到邪恶的目的. ...

百度杯”CTF比赛 2017 二月场 没错！就是文件包含漏洞。

题目源码: 文件包含漏洞的话,看一下 你么可以使用php://input 伪协议,执行代码(参考了大佬WP)这里使用了POSTMAN, 目录下还有一个dle345aae.php文件,呢么用cat命令打 ...

php伪协议，利用文件包含漏洞

php支持多种封装协议,这些协议常被CTF出题中与文件包含漏洞结合,这里做个小总结.实验用的是DVWA平台,low级别,phpstudy中的设置为5.4.45版本, 设置allow_url_fopen ...

本地文件包含漏洞(LFI漏洞)

0x00 前言 本文的主要目的是分享在服务器遭受文件包含漏洞时,使用各种技术对Web服务器进行攻击的想法. 我们都知道LFI漏洞允许用户通过在URL中包括一个文件.在本文中,我使用了bWAPP和DVW ...

python打造文件包含漏洞检测工具

0x00前言: 做Hack the box的题.感觉那个平台得开个Vlp 不然得凉.一天只能重置一次...mmp 做的那题毒药是文件包含漏洞的题,涉及到了某个工具 看的不错就开发了一个. 0x01代码 ...

文件包含漏洞(RFI)

1文件包含漏洞简介 include require include_once require_once RFI综述 RFI是Remote File Inclusion的英文缩写,直译过来就是远 ...

PHP文件包含漏洞总结

0x00 前言 PHP文件包含漏洞的产生原因是在通过PHP的函数引入文件时,由于传入的文件名没有经过合理的校验,从而操作了预想之外的文件,就可能导致意外的文件泄露甚至恶意的代码注入. 最常见的就属于本 ...

2. DVWA亲测文件包含漏洞

Low级: 我们分别点击这几个file.php文件 仅仅是配置参数的变化: http://127.0.0.1/DVWA/vulnerabilities/fi/?page=file3.php 如 ...

文件包含漏洞(file inclusion)

文件包含漏洞原理:(php) 是指当服务器开启allow_url_include选项的时候,通过php某些特性函数.如include().include_once().require().requir ...

随机推荐

Linux 第06天

Linux 第06天 1.SAMBA服务器————(linux和windows的文件共享) 1.1 安装 yum install samba -yum 1.2 配置文件 /etc/samba/smb. ...

Linux面试题汇总答案

转自:小女生的Linux技术~~~Linux面试题汇总答案~~ 一． 填空题:1. 在Linux系统中,以 文件 方式访问设备 .2. Linux内核引导时,从文件 /etc/fstab 中读取要加载的 ...

c++ 中static关键字

static可以用于修饰普通的变量和函数,也可以用于修饰类的成员 普通应用 1.修饰普通变量 修饰全局变量:将变量的作用域限制在所属文件 修饰局部变量:将变量的生存周期延迟到程序结束 2.修饰普通函数 ...

获取程序中无需释放的ViewController

AppDelegate.h @property (strong, nonatomic) UIViewController *viewController; 在需要用的地方 #define appDel ...

.NET基础——ASSCII码表

char类型不能直接强转为int32,因为强转后的结果是去ascii码表的值.如char 类型的1,强转为int32后的值是49. 要得到正确的结果,现将char类型转换为string类型,再转为in ...

XCTF(77777-2)

题目链接:http://47.52.137.90:20000 这道题目和前面的那道题目大致一样,只不过是过滤的函数不一样 检查过滤函数的方式就不写了,直接来解题 检查函数发现过滤了ord ascii ...

为git服务器配置gitosis管理权限

yum install python-setuptools git clone https://github.com/tv42/gitosis.git cd gitosis sudo python s ...

Python-使用PyQT生成图形界面

1.安装PyQT5以及QT Designer工具包 pip install PyQt5 pip install PyQt5-tools -i http://pypi.douban.com/simple ...

Java java.text.ParseException: Unparseable date

用java将字符串转换成Date类型是,会出现java.text.ParseException: Unparseable date异常. 例如下面的这段代码就会出现上面的异常: public bool ...

vue2.0组件之间的传值

1.父子组件--props props:需要注意的是,虽然的是单向的数据流,但是如果传递的是数组或是对象这样的引用类型,子组件数据变化,父组件的数据通也会变化 子组件代码