Buuctf Easy Calc --> WriteUp

原创

山中雨客 于 2021-08-20 22:17:35 发布 21 收藏

分类专栏： PHP代码审计

本文链接：https://blog.csdn.net/weixin_51313108/article/details/119831786

Easy Calc ： WriteUp

大佬的WP

Buuctf Easy Calc --> WriteUp

本题得到知识

以下是从这道ctf题中学到的一些知识

什么是Waf

Waf：Web应用的防火墙，原来的防火墙已经不够抵挡攻击了，所以有了Waf作用是对web应用程序客户端发出的流量进行内容检测和验证，检测其安全性与合法性，来屏蔽常见的网站漏洞攻击，如SQL注入，XML注入、XSS等。WAF的介绍。

利用PHP的字符串解析特性Bypass绕过

Waf可能会限制只通过数字不让通过字符，这时可以利用字符串解析的特性来绕过，所谓的字符串解析即是对查询字符串进行解析到PHP代码中。 利用PHP的字符串解析特性Bypass。

什么是查询字符串(URL参数)

在URL中的“？●=▲×■＆○=△×□”的部分是查询字符串（URL参数）查询字符串。

如何绕过Waf对字符的限制

PHP需要将所有参数转换为有效的变量名，因此在解析查询字符串时，它会做两件事：

- 1.删除空白符
- 2.将某些字符转换为下划线（包括空格）
  我们可以在变量前加上一个空格绕过Waf对字符的限制。

一句话木马的system无法使用

`<?php @eval($_POST['str']); ?>`：str可以是调用外部指令的system函数的字符串，Linux指令的大多数字符被限制了怎么办？PHP中也有文件查找和读取文件函数

- `scandir()`：以数组形式列出参数目录下的目录和文件
- `readfile()`：读取参数里的内容

PHP代码无法使用flag

可以使用chr函数来把ASCII码转换为字符即可实现绕过`chr(47)`就是/。