云演CTF: 004.intval

转载

wangguixiu 于 2021-06-09 22:51:02 发布 318 收藏 1

云演CTF: 004.intval

- 作者: admin
- 时间: 2021-05-27
- 分类: 云演CTF

进去直接给了代码

```php
<?php
if(!isset($_GET['source'])){
    highlight_file('index.php');
    die();
}
include('flag.php');
$key1 = $_GET['f'];
$key2 = $_GET['l'];
$key3 = $_GET['a'];
$key4 = $_GET['g'];
if(isset($key1)&&isset($key2)&&isset($key3)&&isset($key4)) # 四个变量要存在
{
    if(intval($key1) > 1 || intval($key1) < 0) # f要在[0,1]之间，"key1 is error."有三个，开始没注意，卡在这了(注1)
        die("key1 is error.");
    elseif(intval(intval($key1)) < 1) # f取整小于1，继续
    {
        if($key1 == 1){
            if($key2 < 1){
                die("key2 is error.");
            }else{
                if(intval($key2 + $key1) > 1){ # l要小于1并且满足intval($l+$f)大于1(注2)
                    die("key is error.");
                }else{
                    $check = is_numeric($key3) and is_numeric($key4); # 两个相反的条件(注3)
                    if(!$check){
                        die("key3 or key4 is error.");
                    }elseif(!(is_numeric($key3) and is_numeric($key4))){
                        $key3 = $flag;
                        $key4 = $redpacket;
                    }
                    die("flag:".$key3."<br>"."支付宝红包口令".$key4);
                }
            }
        }
        else
            die("key1 is error.");
    }
    else
        die("key1 is error.");
}
?>
```

1) 绕过"key1 is error."有三个条件: 1. intval($f)在[0,1]之间; 2. intval($f)小于1; 3. $f等于1，这样就清楚了，'0b1'不等于1，intval(01)不小于1,答案只有0x1

2) 每种语言的整型变量都有长度限制，php中int变量最大值为+2147483647，加一就变成-2147483648，所以l=2147483647，至于原因，在计算机原理这本书中

自己搭的环境正常，云演平台拿不到flag，今天下班，明天继续

接上，原因找到了：PHP_INT_MAX (int)

```
当前 PHP 版本支持的最大整型数字。在 32 位系统中通常为 int(2147483647)，64 位系统中为
int(9223372036854775807)。自 PHP 5.0.5 起可用。
```

3) 最后key3和key4比较，问题出在"$check"上，'='的优先级在'and'之上，正确语句应该是"$check = (is_numeric($key3) and is_numeric($key4));"，所以key3为真，key4为假即可绕过

最终payload为"?f=0x1&l=92233720368547758 07&a=1&g=&source=" # 建议做这种代码审计类的题目时自己搭建环境，方便调试

标签: none