云演CTF: 009.php_for_fun

转载

wangguixiu 于 2021-06-10 08:50:22 发布 182 收藏

云演CTF: 009.php_for_fun

- 作者: admin
- 时间: 2021-05-31
- 分类: 云演CTF

在首页的返回头中获得hint文件名，内容是"Please input a parameter as number!!"

尝试传入参数"number"，返回"Please input a parameter as number!!"，同时返回头中包含hint2，内容是"$req['number']==strval(intval($req['number']))"，根据返回体猜测代码中使用了"is_numberic"判断"number"是否是数值

hint2的作用是"number"值取整后转为字符依然等于"number"，这种判断一般用%20和%00绕过

尝试"number=%001"，返回"nice! 1 is a palindrome number!"，同时返回头中找到hint4，内容是"palindrome"

再次传入"number=%0012"，返回"no, this is not a palindrome number!"，并找到hint3，"intval($number) == intval(strrev($number))?"

找不到更多提示和要求后，百度搜索提示内容，找到源码

```php
<?php
$info = "";
$req = [];
$flag="xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx";
ini_set("display_error", false); //为一个配置选项设置值
error_reporting(0); //关闭所有PHP错误报告
if(!isset($_GET['number'])){
   header("hint:26966dc52e85af40f59b4fe73d8c323a.txt"); //HTTP头显示hint 26966dc52e85af40f59b4fe73d8c323a.txt
   die("have a fun!!"); //die — 等同于 exit()
}
foreach([$_GET, $_POST] as $global_var) {  //foreach 语法结构提供了遍历数组的简单方式
    foreach($global_var as $key => $value) {
        $value = trim($value);  //trim — 去除字符串首尾处的空格字符（或者其他字符）
        is_string($value) && $req[$key] = addslashes($value); // is_string — 检测变量是否是字符串，addslashes — 使用反斜线引用字符串
    } //存入数组req中value
}
function is_palindrome_number($number) {
    $number = strval($number); //strval — 获取变量的字符串值
    $i = 0;
    $j = strlen($number) - 1; //strlen — 获取字符串长度
    while($i < $j) {
        if($number[$i] !== $number[$j]) {
            return false;
        }
        $i++;
        $j--;
    }
    return true;
}
if(is_numeric($_REQUEST['number'])) //is_numeric — 检测变量是否为数字或数字字符串
{
   $info="sorry, you cann't input a number!";
}
elseif($req['number']!=strval(intval($req['number']))) //intval — 获取变量的整数值. 这里要做的是使得elseif False。空白字符绕过
{
     $info = "number must be equal to it's integer!! ";
}
else
{
     $value1 = intval($req["number"]);
     $value2 = intval(strrev($req["number"]));//strrev 反转字符串
     if($value1!=$value2){
          $info="no, this is not a palindrome number!";
     }
     else
     {
          if(is_palindrome_number($req["number"])){
              $info = "nice! {$value1} is a palindrome number!";
          }
          else
          {
             $info=$flag;
          }
     }
}
echo $info;
```

52行"$info=$flag"是想要的结果，目前通过"number=%001"到达48行的"nice..."，而要得到flag需要经过最后两个if：42行是取整后比较，47行是逐字比较，满足42行条件但不满足47行条件。因为13的trim和34的条件，这里需要一个能绕过trim并且取整后会消失的字符，用burp跑出%0c

所以最终payload为：number=%00%0c1(复现php版本是5.5.9，版本不对代码报错)

标签: none