# ctf中php绕过,CTF之PHP黑魔法总结

转载

爆燃·火星 于 2021-03-09 19:42:30 发布 644 收藏 1
文章标签： ctf中php绕过
CTF之PHP黑魔法总结。

一、要求变量原值不同但md5或sha1相同的情况下

1.0e开头的全部相等(==判断)

240610708 和 QNKCDZO md5值类型相似，但并不相同，在”==”相等操作符的运算下，结果返回了true.

Md5和sha1一样

2.利用数组绕过(===判断)

Md5和sha1对一个数组进行加密将返回NULL;而NULL===NULL返回true，所以可绕过判断。

二、S trcmp利用数组绕过

查看php的手册

int strcmp ( string $str1 , string $str2 )

Return Values

Returns < 0 if str1 is less than str2; > 0 if str1 is greater than str2, and 0 if they are equal.

当输入的两个值为不是字符串时就会产生不预期的返回值：

比如

```
$password=$_GET['password'];
if(strcmp('am0s',$password)){
echo 'false!';
}else{
echo 'success!';
}
?>
```

这样一段代码中，输入password[]=1则返回success，成功绕过验证

三、当有两个is_numeric判断并用and连接时，and后面的is_numeric可以绕过

```
$a=$_GET['a'];
$b=$_GET['b'];
$c=is_numeric($a) and is_numeric($b);
var_dump(is_numeric($a));
```

var_dump(is_numeric($b));

var_dump($c); //$b可以不是数字，同样返回true

$test=false and true;

var_dump($test); //返回true

四、NULL,0,”0″,array()使用==和false比较时，都是会返回true的

五、 Eregi匹配

数组绕过

ereg是处理字符串，传入数组之后，ereg是返回NULL

%00截断绕过

http://www.secbox.cn/hacker/1889.html

六、接收参数$a得存在，并且$a==0可用.绕过(非数字都可绕过)

测试代码：

$a=$_GET['a'];

if ($a==0) {

echo "1";

}

if ($a) {

echo "must";

}

七、接收参数中不能出现某一字符，但下面又必须使用可以 php://伪协议绕过

目前遇到的是file_get_contents其他情况具体而定

八、 is_numeric绕过

空格、\t、\n、\r、\v、\f、+、-能够出现在参数开头，“点”能够在参数任何位置，E、e只能出现在参数中间。

九、php5,3,29,这里可以直接用%0b绕过\s(空白字符)的匹配

十、 既是0又是1的情况

$a==1&$test[$a]=t时

php精度(16以上)var_dump(9999999999999999999==1);//true

科学计数法 .1e1 echo $b[‘.1e1’]//输出t

.是字符串所以在数组里面变成0，但在is_numeric中有点则正常输出为数字

十一、 当switch没有break时可以继续往下执行

if (isset ( $_GET ['which'] )) {

```
$which = $_GET ['which'];
switch ($which) {
case 0 :
case 1 :
case 2 :
echo $which . '.php';
break;
default :
echo "1";
break;
}
}
```

$which进入循环时没有break则按顺序