实验吧——(web)Once More writeup

原创

嗯哼哈嘿 于 2019-05-01 23:37:27 发布 81 收藏

分类专栏： CTF 文章标签： 实验吧 web ereg漏洞 php函数漏洞


```php
<?php
if (isset ($_GET['password'])) {
 if (ereg ("^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
 {
  echo '<p>You password must be alphanumeric</p>';
 }
 else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
 {
  if (strpos ($_GET['password'], '*-*') !== FALSE)
  {
   die('Flag: ' . $flag);
  }
  else
  {
   echo('<p>*-* have not been found</p>');
  }
 }
 else
 {
  echo '<p>Invalid password</p>';
 }
}
?>
```

读代码时，需要知道以下几点：

1. **ereg()函数**用指定的模式搜索一个字符串中指定的字符串,如果匹配成功返回true,否则,则返回false。搜索字母的字符是大小写敏感的。题中ereg()正则限制了password的形式，只能是一个或者多个数字、大小写字母。
2. **strpos() 函数**查找字符串在另一字符串中第一次出现的位置。
3. %00 是URL的终止符

ereg函数存在**NULL截断漏洞**，导致了正则过滤被绕过,所以可以**使用%00截断正则匹配**。（即ereg读到%00的时候，就截止了）
ereg()只能处理字符串的，遇到**数组做参数返回NULL**，判断用的是 **===**，要求类型也相同，而NULL跟FALSE类型是不同的,strpos()的参数同样不能为数组，否则**返回NULL**，而判断用的是 **!==**，所以这里的条件成立，也能得到flag.
所以只要在地址栏里，在传递参数时传递数组参数就行。
如：
http://ctf5.shiyanbar.com/web/more.php?password[]=1--
或
http://ctf5.shiyanbar.com/web/more.php?password[]=2
即可得到Flag

另：

strlen()限制了**长度**小于8并且大小必须大于9999999,**1e8=100000000 > 9999999**
（这个思路是我最开始想的思路，但没想到用e来让数字变大）
strpos()对password进行匹配，**必须含有'-'**，最终才输出flag
所以构造 1e8%00*-* (1e9%00*-*也行)
（ereg函数读到%00就会截断，不会再看后面的内容，所以满足字符和数字组成的字符串）
http://ctf5.shiyanbar.com/web/more.php?password=1e8

Flag: CTF{Ch3ck_anD_Ch3ck}

参考：
https://www.jianshu.com/p/7b732d4b8eac
https://www.cnblogs.com/liuyimin/p/7668005.html