实验吧-Once More Writeup

原创

baynk 于 2019-08-23 03:02:33 发布 97 收藏 1

分类专栏： # 实验吧 Writeup 文章标签： 实验吧 CTF Once More

本文链接：https://blog.csdn.net/u014029795/article/details/100027963

过程

- 链接：http://ctf5.shiyanbar.com/web/more.php
- 这次在做题前就给了hint，后面会用到。

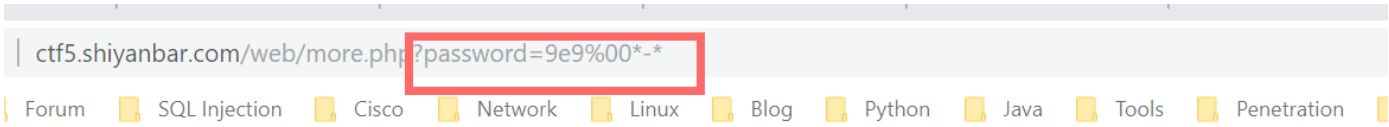
> 啊拉？又是php审计。已经想吐了。
> hint：ereg()函数有漏洞哩；从小老师就说要用科学的方法来算数。
> 格式：CTF{}

- 点到链接里面去，发现要输入一个数值，然后还有一个查看源代码的按钮，GO。

```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>';
        }
}
?>
```

- 首先是ereg函数，一定要在password中找到大小写字母及数字的组成一个或者多个(后面的+)，直白一点就是只能由大小写

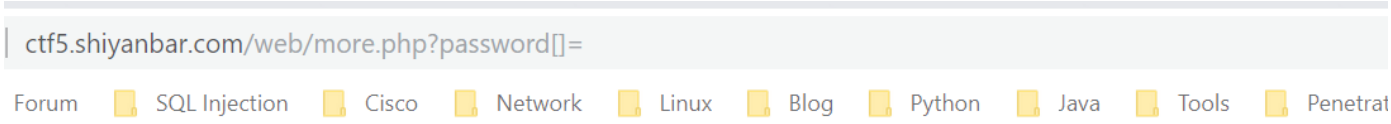
- 首先是ereg函数，一定要在password中找到大小写字母及数字的组成一个或者多个(后面的+)，重点一点就是只能由大小写字母和数字组成，且不能为空。
- 接着，password的长度一定要小于8，并且值一定要大于9999999，从提示就知道这里要用科学计数法来完成。
- 接下来最后一个需求，一定要在passord中找到*-*，但是这个明显和第一条冲突了，所以只能通过hint的提示，ereg有漏洞，通过百度查寻到有%00截断漏洞，于是payload就成功构造，`9e9%00*-*`，这里要注意只能在url中填写，不要直接写在框里面。而且长度有限制要求少于8位的，这里明显超过，能PASS其实是因为%00其实就是空只算一个字符，加起来正好7个，满足条件，最前面的9也可以换别的。



Flag: CTF{Ch3ck_anD_Ch3ck}

总结

- 百度是个好东西~
- 另外还看到了另外一种解法，直接password那里传入数组password。



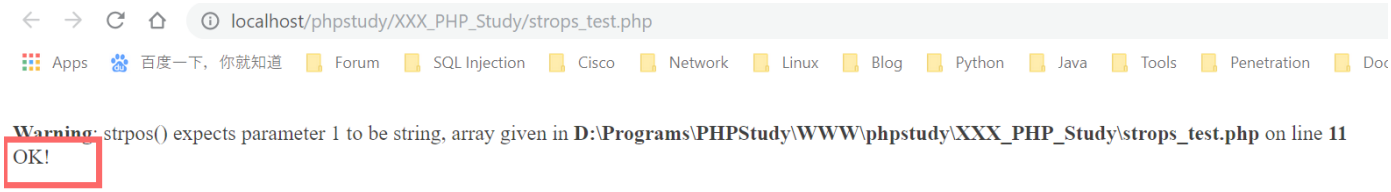
Flag: CTF{Ch3ck_anD_Ch3ck}

- 首先strops去检查数组会出错，===False不成立，成功绕过。但是我自己测试其实是没有成功的，不过这里就不多测试了，就这样吧。

tal error: Uncaught Error: Call to undefined function ereg() in D:\Programs\PHPStudy\WWW\phpstudy\XXX_PHP_Study\strops_test.php:12 Stack
line **12**

- 然后数组长度肯定小于8，然后任意数组是大于任意数字的，所以也能绕过。最关键的是用strpos去检查一个数组也会出错，大概是不等于False，所以才能成功绕过的。

```
$a = array();
if (strpos($a,'1')!==false){
    echo "OK!";
}
```



Warning: strpos() expects parameter 1 to be string, array given in **D:\Programs\PHPStudy\WWW\phpstudy\XXX_PHP_Study\strops_test.php** on line **11**
OK!