实验吧WEBWP(二）

原创

Neil-Yale 于 2017-03-20 08:46:58 发布 1354 收藏

文章标签： 源码 WriteUp CTF

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/yalecaltech/article/details/64120772

版权

1.Once More（http://www.shiyanbar.com/ctf/1805）

点击—view the source code

关键码

else if (strlen(_GET['password']) < 8 &&_GET['password'] > 9999999)

{

if (strpos ($_GET['password'], '-') !== FALSE)

{

die('Flag: ' . $flag);

}

看了代码后，大意就是让我们满足以下条件才会出来flag

1.password的字符串长度小于8而password的数值却要大于9999999

2.并且该数中要包含"-"

第一点，只有科学计数法能满足

如1e7,1e8，1e9

第二点，如果我们直接加-，答案为1e9-的话实际上两个条件都不满足了

根据提示ereg()存在漏洞，百度之，知道是截断漏洞，故构造1e8%00*-*

完整的url=http://ctf4.shiyanbar.com/web/more.php?password=1e8%00-

2.Guess Next Session(http://www.shiyanbar.com/ctf/1788)

点击—view the source code

if (

要挑战rand是不可能的

于是我们尝试将两者都修改为0

得到答案

3.FALSE（http://www.shiyanbar.com/ctf/1787）

点击—view the source code