/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

/\* 程序作者：爱的伊苏 \*/

/\* 程序完成时间：2019/1/19 \*/

/\* 有任何问题请联系：740531307@qq.com \*/

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

//@永远得意的笑下去

下面为题目所给源码

<?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>';

}

}

?>

直接开始代码审计

第一层：Isset为确定目标是否被定义

第二层：正则表达式为大小写字母&&数字

第三层：总长度八位以内&&大于9999999 – 以科学记数法表示仅需三位

第四层：密码中必须包含“\*-\*”

综上 密码为 科学记数法 + 过滤第二层筛查 + 必须包含的字符

最后成果图

