1、知识点

知识点	说明
ereg()	搜索字符串以匹配模式中给出的正则表达式
strpos()	查找字符串首次出现的位置

2、源码

```
<?php

$flag = "flag";

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) //strpos – 查找字符串首次出现的位置
      {
      die('Flag: ' . $flag);
      }
      else
      {
        echo('<p>*-* have not been found</p>');
       }
      }
     else
     {
        echo '<p>Invalid password</p>';
      }
   }
?>
```

3、分析

```
    1) 程序首先进行了两个判断：
        - $_GET需要接收password参数
        - password的值必须为数字或者大小写字母
```

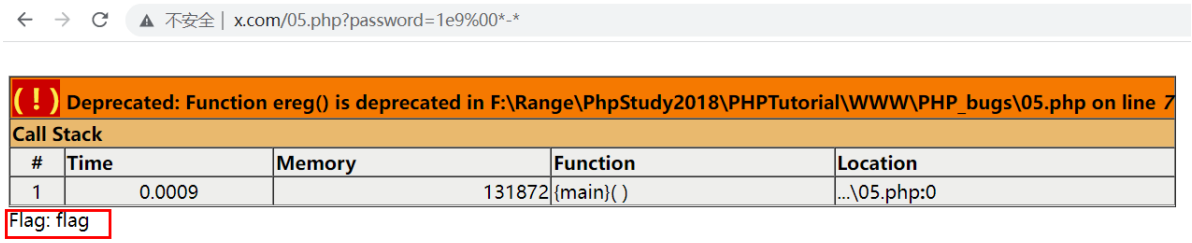
```php
$flag = "flag";

if (isset ($_GET['password']))
{
  if (ereg ( pattern: "^[a-zA-Z0-9]+$", $_GET['password']) === FALSE)
  {
    echo '<p>You password must be alphanumeric</p>';
  }
```

2）随后又进行了两个关键判断：
   - password值的长度需要小于8，值又要大于9999999
   - password值必须匹配到 *-*关键词

```php
else if (strlen($_GET['password']) < 8 && $_GET['password'] > 9999999)
 {
   if (strpos ($_GET['password'], needle: '*-*') !== FALSE) //strpos - 查找字符串首次出现的位置
    {
    die('Flag: ' . $flag);
    }
```

3）总结一下关键点：
   - password值需要大于9999999，并且长度不能大于8
   - password必须以数字或大小写字母组成，又得包含特殊字符 *_*

4）利用思路：
   - 使用科学计数法绕过第1个关键点
   - 使用%00进行截断，然后在后面添加特殊字符*_*



4、利用

```
?password=1e9%00*-*
```