1、知识点

知识点	说明
session_start()	创建新会话或重用现有会话的内置函数
mt_srand()	播种 Mersenne Twister 随机数生成器
microtime()	返回当前Unix时间戳的微秒数

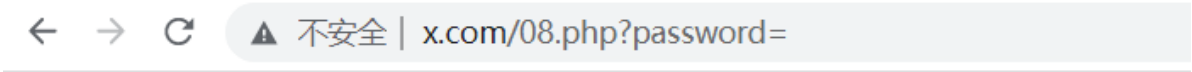
2、源码

```
<?php

$flag = "flag";

session_start();
if (isset ($_GET['password'])) {
    if ($_GET['password'] == $_SESSION['password'])
        die ('Flag: '.$flag);
    else
        print '<p>Wrong guess.</p>';
}
mt_srand((microtime() ^ rand(1, 10000)) % rand(1, 10000) + rand(1, 10000));
?>
```

3、分析

1）程序接收GET方法传入的password值，并使用password和SESSION中的password进行比较，相等即返回flag。

2）这里也是用了比较，那么让GET中password的值和SESSION中password的值都为空，也能让判断成立，得到flag。



(!) Notice: Undefined index: password in F:\Range\PhpStudy2018

Call Stack

#	Time	Memory	Function
1	0.0007	132368	{main}( )

Flag: flag

4、利用

```
?password=
```