变量覆盖指的是用我们自定义的参数值替换程序原有的变量值，一般变量覆盖漏洞需要结合程序的其它功能来实现完整的攻击。

经常导致变量覆盖漏洞场景有：$$，extract()函数，parse_str()函数，import_request_variables()使用不当，开启了全局变量注册等。

0×01 全局变量覆盖

register_globals的意思就是注册为全局变量，所以当On的时候，传递过来的值会被直接的注册为全局变量直接使用，而Off的时候，我们需要到特定的数组里去得到它。

代码示例1：

```
<?php
//?id=1
echo "Register_globals: ".(int)ini_get("register_globals")."<br/>";
echo '$_GET["id"] :'.$_GET['id']."<br/>";
echo '$id :'.$id;
?>
```

当register_globals=Off的时候，下一个程序接收的时候应该用$_GET['id']来接受传递过来的值；

当register_globals=On的时候，下一个程序可以直接使用id来接受值，也可以用_GET['id']来接受传递过来的值。

tips：如果上面的代码中，已经对变量id赋了初始值，比如id=0，那么即使在URL中有/test.php?id=1，也不会将变量覆盖，id值为0

代码示例2：

```
<?php
echo "Register_globals: ".(int)ini_get("register_globals")."<br/>";
if (ini_get('register_globals')) foreach($_REQUEST as $k=>$v) unset(${$k});
print $a."<br/>";
print $_GET[b];
?>
```

在register_globals=ON时，

提交/test.php?a=1&b=2，变量a未初始化，_GET[b]=2

提交/test.php??GLOBALS[a]=1&b=2,$a = 1$,_GET[b]=2

tips:　从 PHP » 4.2.0 版开始配置文件中 PHP 指令 register_globals 的默认值从 on 改为 off 了,自 PHP 5.3.0 起废弃并将自 PHP 5.4.0 起移除。源自：http://php.net/manual/zh/security.globals.php

0×02 $导致的变量覆盖问题

使用foreach来遍历数组中的值，然后再将获取到的数组键名作为变量，数组中的键值作为变量的值。因此就产生了变量覆盖漏洞。请求?id=1 会将id的值覆盖，id=1。

```
<?php
```

```
foreach (array('_COOKIE','_POST','_GET') as $_request)
{
    foreach ($$_request as $_key=>$_value)
    {
        $$_key=  $_value;
    }
}
$id = isset($id) ? $id : 2;
if($id == 1) {
    echo "flag{xxxxxxxxxx}";
    die();
}
echo $id;
?>
```

0×03 extract()变量覆盖

extract() 函数从数组中将变量导入到当前的符号表。该函数使用数组键名作为变量名，使用数组键值作为变量值。针对数组中的每个元素，将在当前符号表中创建对应的一个变量。源自：http://www.w3school.com.cn/php/func_array_extract.asp

代码示例1：

将键值 "Cat"、"Dog" 和 "Horse" 赋值给变量 $a、b 和 $c：

```
<?php
$a = "Original";
$my_array = array("a" => "Cat","b" => "Dog", "c" => "Horse");
extract($my_array);
echo "\$a = $a; \$b = $b; \$c = $c";
?>
//运行结果: $a = Cat; $b = Dog; $c = Horse
```

代码示例2：

```
<?php
$id=1;
extract($_GET);
echo $id;
?>
//提交: ?id=123
//结果:  123
```

tips: 在调用extract()时使用EXTR_SKIP保证已有变量不会被覆盖 extract($_GET,EXTR_SKIP);

0×04 parse_str()变量覆盖

parse_str() 函数把查询字符串解析到变量中，如果没有array 参数，则由该函数设置的变量将覆盖已存在的同名变量。

用法参考： http://www.w3school.com.cn/php/func_string_parse_str.asp

代码示例一：

```
<?php
parse_str("a=1");
echo $a."<br/>";      //$a=1
parse_str("b=1&c=2",$myArray);
print_r($myArray);   //Array ( [c] => 1 [b] => 2 )
?>
```

tips：parse_str()类似的函数还有mb_parse_str()，用法基本一致。

0×05 import_request_variables变量覆盖

import_request_variables 函数可以在 register_global = off 时，把 GET/POST/Cookie 变量导入全局作用域中。

```
<?php
import_request_variables("g", "get_");
echo $get_id;
?>
//提交：?id=111
//结构：111
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。