**变量覆盖**

1. 什么是变量覆盖？

用我们传参值替换程序原有的变量值。

1. 常见的漏洞场景：$$使用不当，extract()函数使用不当，parse\_str()函数使用不当，

Import\_request\_variables()使用不当

变量赋该漏洞能使我们直接获取webshell，拿到服务器的权限。

**相关函数的解析**

1. extract（）

将数组进行键值分离，即将数组每一项都拆成一个变量

$my\_array=array(“a”=>”1”,”b”=>”2”);

echo \$a=$a;\$b=$b;(\是转义字符，作用是转换含义，在这句话里代表旁边不是变量

1. parse\_str()

将字符串进行键值分离

parse\_str(‘name=ldz&age=18’);

echo $name;echo age;

例题：

<?Php

$session=0;

parse\_str($\_GET[‘f’]);

if($session==1){

echo’flag’}

?>

如题，有parse\_str函数我们可以直接通过get提交payload‘?f=session=1’即可变量覆盖

1. $$

通常与foreach一起出现，例题：

<?php

$a=1;

foreach(array(‘\_COOKIE’,’\_POST’,’\_GET’)as $\_request){ //分化成cookie，post和get三个值  
foreach($$\_request as $key=$value){ //将$\_get/post/cookie进行键值分离

$$key=addslashes($\_value); //分离后是键等于值

} //addslashes是用来防止sql注入的

}

echo $a //输出结果

?>