20200714信息安全实训

笔记本:	我的第一个笔记本		
创建时间:	2020/7/14 8:16	**更新时间:**	2020/7/14 16:32
作者:	820410740@qq.com		
URL:	app://desktop.dingtalk.com/web_content/chatbox.html?isFourColumnMode=fal...		

单双引号的嵌套过滤
网址 非法渗透测试 是真是假 （站长之家 工信部备案系统）备案
命令执行 https://www.cnblogs.com/Qiuzhiyu/p/12533052.html
https://www.jianshu.com/p/720649d2427f

命令执行定义

当应用需要调用一些外部程序去处理内容的情况下，就会用到一些执行系统命令的函数。如PHP中的**system，exec，shell_exec**等，

当用户可以控制命令执行函数中的参数时，将可注入恶意系统命令到正常命令中，造成命令执行攻击。

形成原因

脚本语言优点是简洁，方便，但也伴随着一些问题，如速度慢，无法解除系统底层，如果我们开发的应用需要一些除去web的特殊功能时，就需要调用一些外部程序。带来方便的同时也存在威胁。

漏洞危害

继承Web服务程序的权限去执行系统命令或读写文件
反弹shell
控制整个网站甚至控制服务器

进一步内网渗透

命令执行常用函数

1. System：system函数可以用来执行一个外部的应用程序并将相应的执行结果输出，
函数原型如下：string system(string command, int&return_var)
其中，command是要执行的命令，return_var存放执行命令的执行后的状态值。
2. Exec：exec函数可以用来执行一个外部的应用程序
string exec (string command, array&output, int &return_var)
其中，command是要执行的命令，output是获得执行命令输出的每一行字符串，
return_var存放执行命令后的状态值。
3.Passthru：passthru函数可以用来执行一个UNIX系统命令并显示原始的输出，
当UNIX系统命令的输出是二进制的数据，并且需要直接返回值给浏览器时，
需要使用passthru函数来替代system与exec函数。
Passthru函数原型如下：void passthru (string command, int&return_var)
其中，command是要执行的命令，return_var存放执行命令后的状态值。
4. Shell_exec：执行shell命令并返回输出的字符串，
函数原型如下：string shell_exec (string command)
其中，command是要执行的命令。