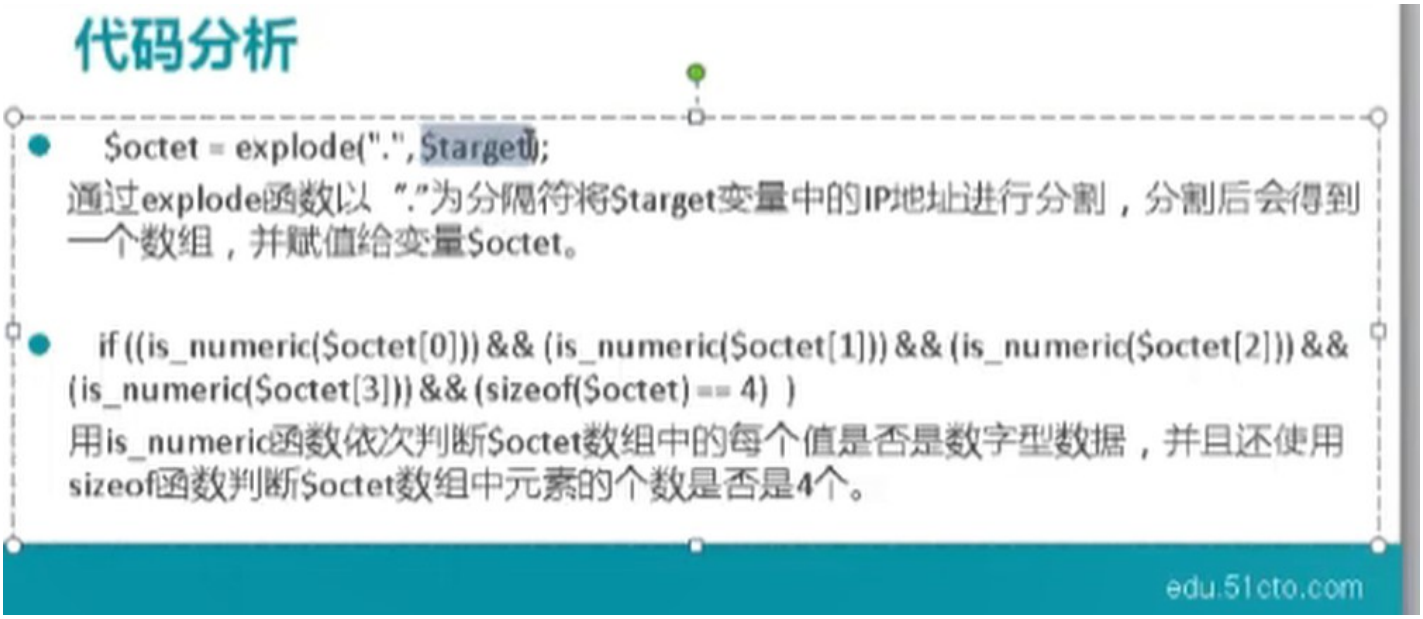
中级命令注入

Command Execution Source

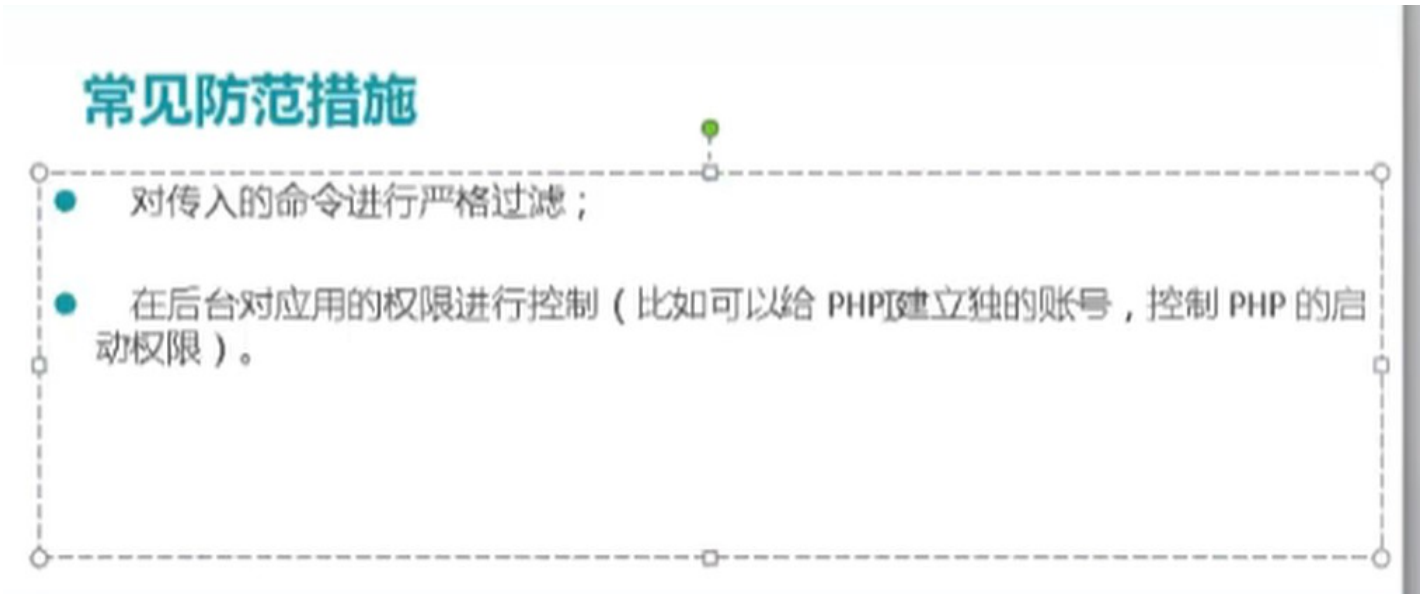
```
<?php

if( isset( $_POST[ 'submit'] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Remove any of the charactars in the array (blacklist).
    $substitutions = array(
#         '&&' => '',  //'&&'是变量的key，后面是变量的值(这里的值为空)!
        ';' => '',//这个变量是分号;
    );//这是php里面的数组!

    $target = str_replace( array_keys( $substitutions ), $substitutions, $target );//$

    // Determine OS and execute the ping command.
    if (stristr(php_uname('s'), 'Windows NT')) {

        $cmd = shell_exec( 'ping  ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping  -c 3 ' . $target );
        echo '<pre>'.$cmd.'</pre>';

    }
}

?>
```

高级命令注入

```php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST["ip"];

    $target = stripslashes( $target );//去掉魔法引号!


    // Split the IP into 4 octects
#     $octet = explode(".", $target);//看下面的一个图 ！就是把target里面的ip地址用.分割,而后

    // Check IF each octet is an integer
    if ((is_numeric($octet[0])) && (is_numeric($octet[1])) && (is_numeric($octet[2]))
    //(is_numeric($octet[0])判断第一个数值是不是数字；(sizeof($octet) == 4) 表示数值的个数为4

    // If all 4 octets are int's put the IP back together.
    $target = $octet[0].'.'.$octet[1].'.'.$octet[2].'.'.$octet[3];


        // Determine OS and execute the ping command.
        if (stristr(php_uname('s'), 'Windows NT')) {

            $cmd = shell_exec( 'ping  ' . $target );
            echo '<pre>'.$cmd.'</pre>';

        } else {

            $cmd = shell_exec( 'ping  -c 3 ' . $target );
            echo '<pre>'.$cmd.'</pre>';

        }

    }

    else {
        echo '<pre>ERROR: You have entered an invalid IP</pre>';
    }


}

?>

```

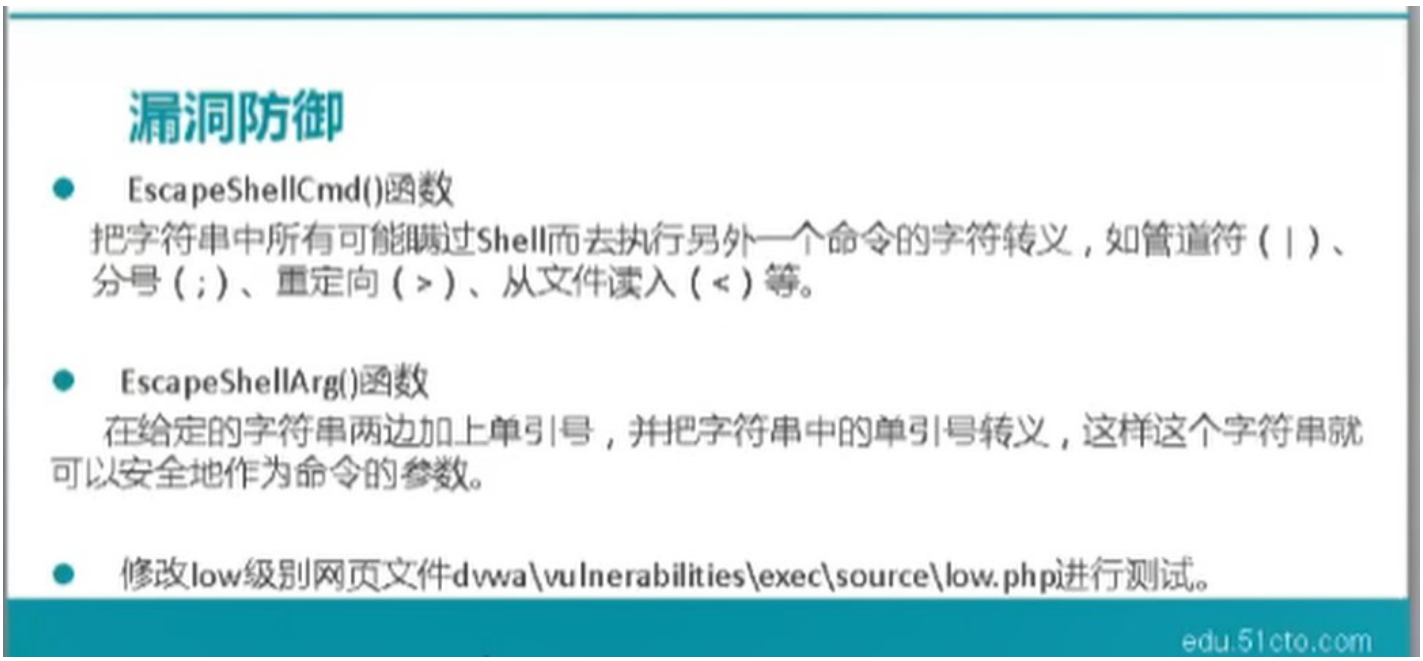


防范措施



1.对传入的命令进行严格过滤

2.在后台对应用的权限进行控制;



1.EscapeShellCmd()函数；(最好记忆！！！)

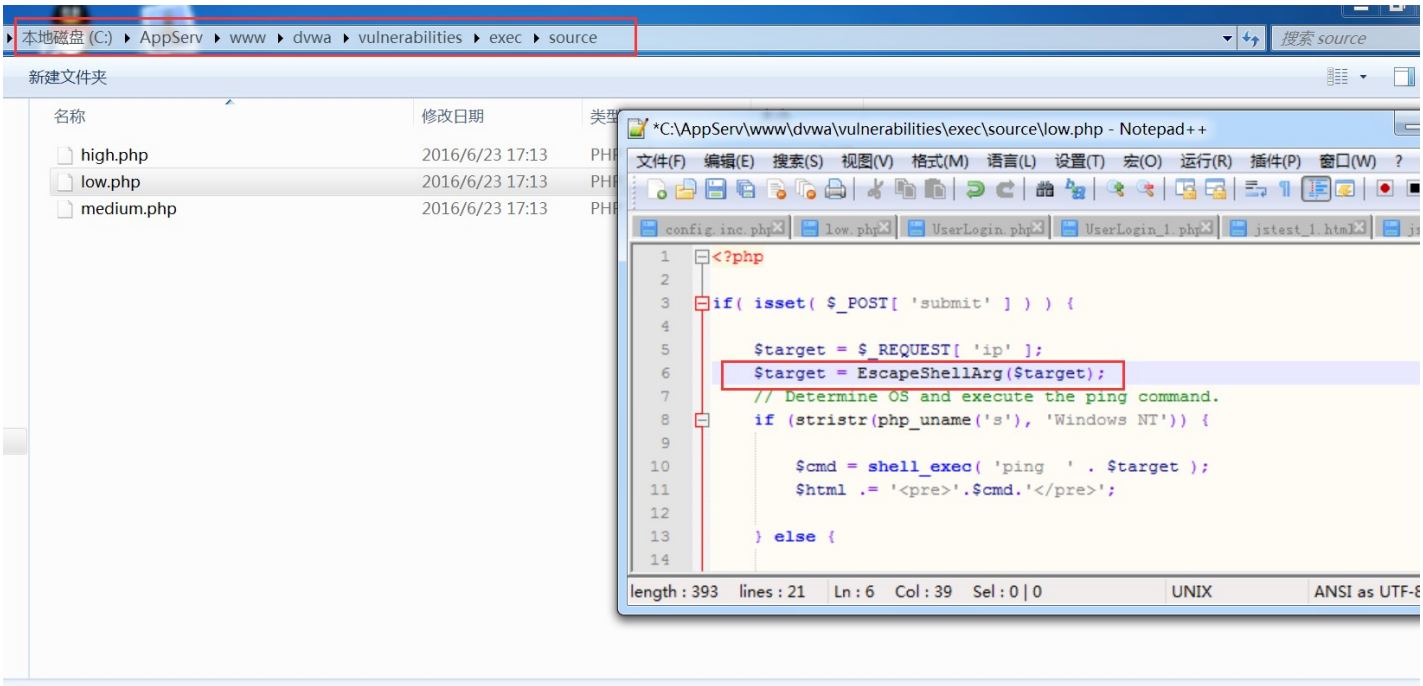
把字符串里面所有可能瞒过shell而去执行另外一个命令的字符转义,如管道符(|),分号(;),重定向(>);从文件读入(<)等；

2.EscapeShellArg()函数；(这个函数也比较重要,最好记忆！！)

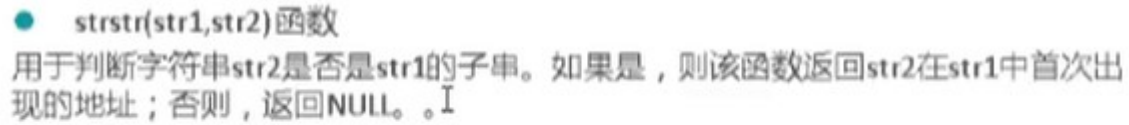
在给定的字符串两边加上单引号,并把字符串中的单引号转义,这样这个字符串就可以安全地作为命令的参数；

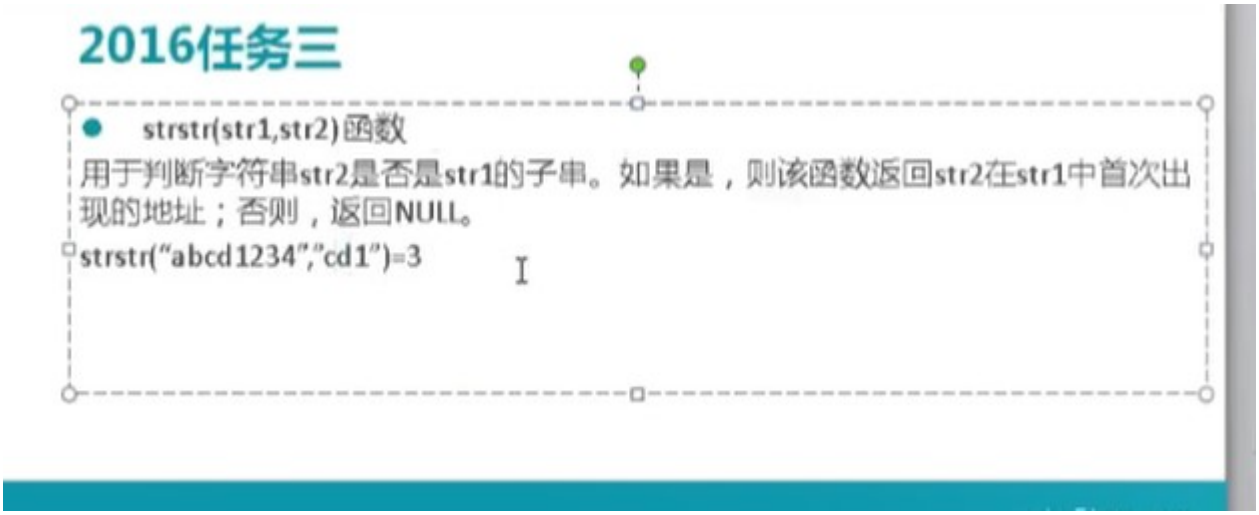
3.修改low级别网页文件 `dvwa\vulnerabilities\exec\source\low.php` 进行测试!

这里举个例子:(修改网页源码！)



这里没有效果了！





strstr()函数的用法如上;