ping cat.flag.php,关于2020年强网杯-强网先锋-主动的赛题解析

转载

O超哥 于 2021-03-26 20:40:58 发布 308 收藏 1
文章标签： ping cat.flag.php
原标题：关于2020年强网杯-强网先锋-主动的赛题解析

一、基本信息(总概述)

本题涉及知识点：

命令执行

正则匹配

linux命令绕过

二、基本环境和工具

Linux系统

PHP+Apache

Firefox

Index.php

Flag.php

三、Writeup

1、根据题目要求还原实验环境

首先在Linux虚拟机上安装Apache

Yum install httpd

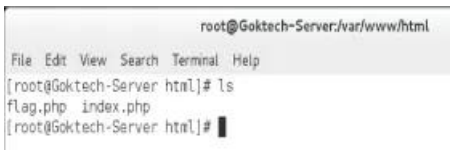
```
[root@Goktech-Server Desktop]# yum install httpd
Loaded plugins: langpacks, product-id, subscription-manager
This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.
Resolving Dependencies
--> Running transaction check
---> Package httpd.x86_64 0:2.4.6-93.el7.centos will be installed
--> Processing Dependency: httpd-tools = 2.4.6-93.el7.centos for package: httpd-2.4.6-93.el7.centos.x86_64
--> Running transaction check
---> Package httpd-tools.x86_64 0:2.4.6-93.el7.centos will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package              Arch              Version                  Repository  Size
================================================================================
Installing:
 httpd                x86_64            2.4.6-93.el7.centos      base       2.7 M
Installing for dependencies:
 httpd-tools          x86_64            2.4.6-93.el7.centos      base        92 k

Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 2.8 M
Installed size: 9.5 M
Is this ok [y/d/N]: y
Downloading packages:
(1/2): httpd-tools-2.4.6-93.el7.centos.x86_64.rpm          |  92 kB  00:00:00
(2/2): httpd-2.4.6-93.el7.centos.x86_64.rpm                | 2.7 MB  00:00:01
--------------------------------------------------------------------------------
Total                                       2.4 MB/s | 2.8 MB  00:00:01
Running transaction check
```

安装PHP环境

Yum install php

```
[root@Goktech-Server Desktop]# yum install php
Loaded plugins: langpacks, product-id, subscription-manager
This system is not registered to Red Hat Subscription Management. You can use subscription-manager to register.
Resolving Dependencies
--> Running transaction check
---> Package php.x86_64 0:5.4.16-48.el7 will be installed
--> Processing Dependency: php-common(x86-64) = 5.4.16-48.el7 for package: php-5.4.16-48.el7.x86_64
--> Processing Dependency: php-cli(x86-64) = 5.4.16-48.el7 for package: php-5.4.16-48.el7.x86_64
--> Running transaction check
---> Package php-cli.x86_64 0:5.4.16-48.el7 will be installed
---> Package php-common.x86_64 0:5.4.16-48.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch              Version                 Repository
                                                                           Size
================================================================================
Installing:
 php                    x86_64            5.4.16-48.el7           base
                                                                          1.4 M
Installing for dependencies:
 php-cli                x86_64            5.4.16-48.el7           base
                                                                          2.7 M
 php-common             x86_64            5.4.16-48.el7           base
                                                                          565 k

Transaction Summary
================================================================================
Install  1 Package (+2 Dependent packages)

Total download size: 4.7 M
Installed size: 17 M
Is this ok [y/d/N]: y
Downloading packages:
```

在red hat的网站目录下创建如下两个文件



两个文件中内容如下

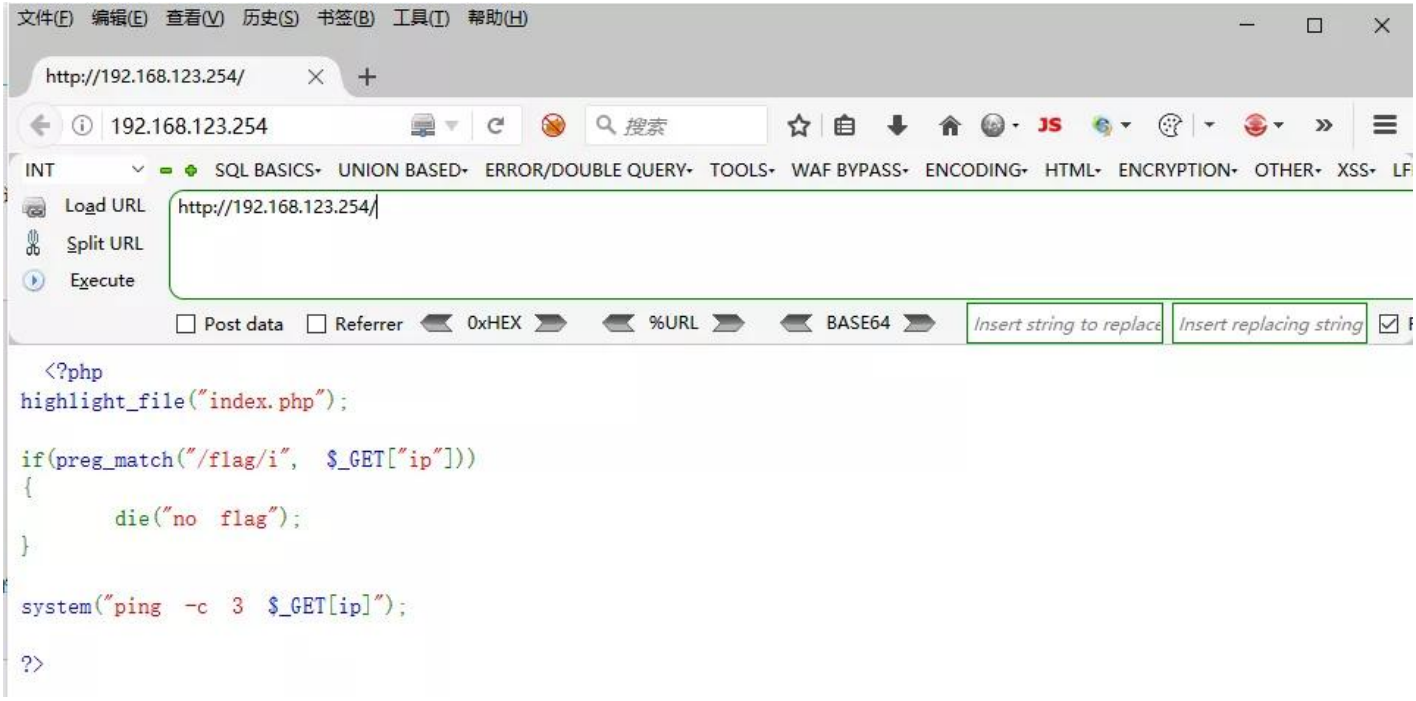
开启HTTP服务

systemctl start httpd

为了方便在主机实验可以临时关闭防火墙

systemctl stop firewalld

2、在浏览器中输入虚拟机IP(192.168.123.254)进行访问



system("ping -c 3 $_GET[ip]");这一条语句明显表明可以进行命令执行

3、尝试构造命令观察当前文件目录下是否有flag相关文件

如图，发现有falg.php文件，但题目中对flag进行了过滤

如果直接cat flag.php显示如下

这是由于preg_match 函数用于执行一个正则表达式匹配。

题目中的preg_match("/flag/i",$_GET["ip"])，其正则表达式为：/flag/i，该函数表示从我们构造的ip的值中匹配flag字符串，所以我们在构造ip的值为"8.8.8.8;cat flag.php"时输出了no flag(die函数输出一条消息，并退出当前脚本。)，因为他匹配的了flag字符串

正则表达式中"/"是表达式开始和结束的标记(即匹配了flag)且其后的"i"标记这是一个大小写不敏感的搜索即flag中字母的大写和小写的组合都会被匹配到

本题中的正则表达式未涉及许多的正则表达式的元字符，例如还有一些其他常见的类型题目如正则表达式(/^\w+$/)在表达式开始和结束的标记中间的

^匹配输入字行首；

\w 匹配包括下划线的任何单词字符；

+匹配前面的子表达式一次或多次(大于等于1次)；

$匹配输入行尾

总体意义就是限定一个任意长字符串，全部由字母数字下划线组成，前面中间后面都不能有空格、标点等非\w字符

关于正则表达式的更多内容可以参考百度百科中给出的详细介绍

https://baike.baidu.com/item/%E6%AD%A3%E5%88%99%E8%A1%A8%E8%BE%BE%E5%BC%8F/1700215?fr=aladdin

4、知识储备

百度查询Linux的关键字绕过方法

https://blog.csdn.net/wojiushilsy/article/details/106129503

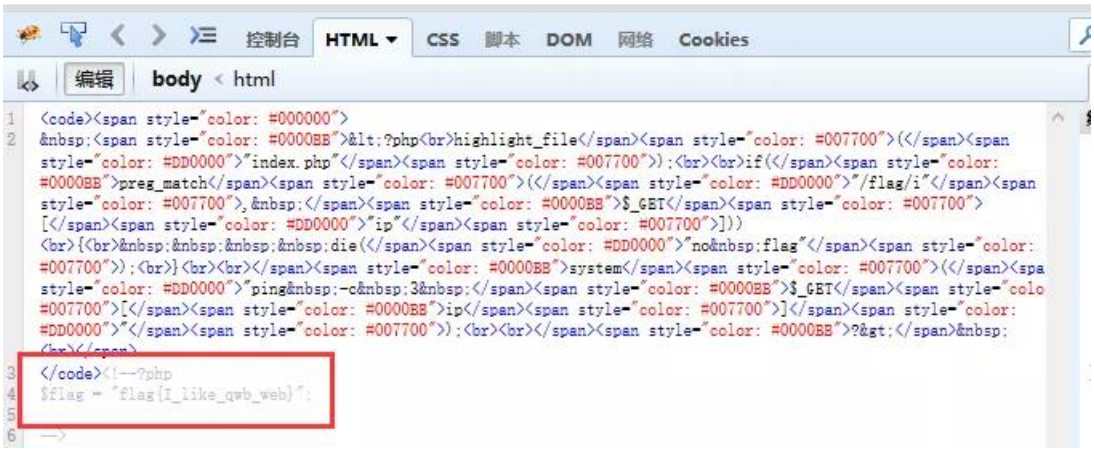
linux中直接查看文件内容的命令

cat、tac、more、less、head、tail、nl、sed、sort、uniq

其中使用tac和sort命令可以直接将falg命令的内容输出到页面上，使用cat就得查看源码找到flag的内容

5、单双引号绕过


```php
<?php
highlight_file("index.php");

if(preg_match("/flag/i",  $_GET["ip"]))
{
        die("no  flag");
}

system("ping  -c  3  $_GET[ip]");

?>
```



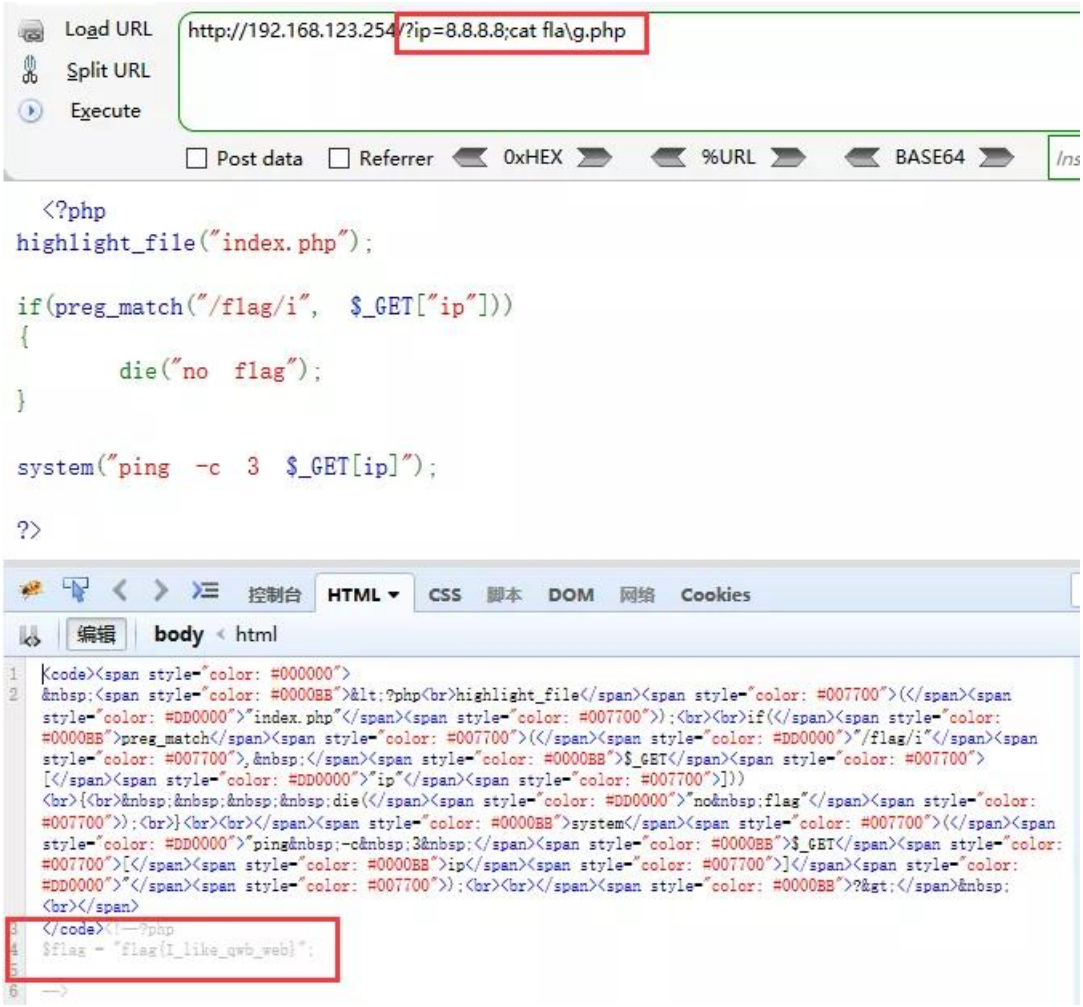

```
<code><span style="color: #000000">
 <span style="color: #0000BB">&lt;?php<br>highlight_file</span><span style="color: #007700">(</span><span
style="color: #DD0000">"index.php"</span><span style="color: #007700">);<br><br>if(</span><span style="color:
#0000BB">preg_match</span><span style="color: #007700">(</span><span style="color: #DD0000">"/flag/i"</span><span
style="color: #007700">, </span><span style="color: #0000BB">$_GET</span><span style="color: #007700">
[</span><span style="color: #DD0000">"ip"</span><span style="color: #007700">]))
<br>{<br>    die(</span><span style="color: #DD0000">"no flag"</span><span style="color:
#007700">);<br>}<br><br></span><span style="color: #0000BB">system</span><span style="color: #007700">(</span><spa
style="color: #DD0000">"ping -c 3 </span><span style="color: #0000BB">$_GET</span><span style="colo
#007700">[</span><span style="color: #0000BB">ip</span><span style="color: #007700">]</span><span style="color:
#DD0000">"</span><span style="color: #007700">);<br><br></span><span style="color: #0000BB">?&gt;</span> 
<br></span>
</code><!--?php
$flag = "flag{I_like_qwb_web}";

-->
```


```php
<?php
highlight_file("index.php");

if(preg_match("/flag/i",  $_GET["ip"]))
{
        die("no  flag");
}

system("ping  -c  3  $_GET[ip]");

?>
```


```
<code><span style="color: #000000">
 <span style="color: #0000BB">&lt;?php<br>highlight_file</span><span style="color: #007700">(</span><span
style="color: #DD0000">"index.php"</span><span style="color: #007700">);<br><br>if(</span><span style="color:
#0000BB">preg_match</span><span style="color: #007700">(</span><span style="color: #DD0000">"/flag/i"</span><span
style="color: #007700">, </span><span style="color: #0000BB">$_GET</span><span style="color: #007700">
[</span><span style="color: #DD0000">"ip"</span><span style="color: #007700">]))
<br>{<br>    die(</span><span style="color: #DD0000">"no flag"</span><span style="color:
#007700">);<br>}<br><br></span><span style="color: #0000BB">system</span><span style="color: #007700">(</span><span
style="color: #DD0000">"ping -c 3 </span><span style="color: #0000BB">$_GET</span><span style="color:
#007700">[</span><span style="color: #0000BB">ip</span><span style="color: #007700">]</span><span style="color:
#DD0000">"</span><span style="color: #007700">);<br><br></span><span style="color: #0000BB">?&gt;</span> 
<br></span>
</code><!--?php
$flag = "flag{I_like_qwb_web}";

-->
```

如上图取得$flag = "flag{I_like_qwb_web}"

6、使用反斜杠绕过



7、利用Shell 特殊变量绕过

如下图使用tac命令可以直接看到flag的内容

8、利用通配符绕过

如下图使用sort命令也可以直接看到flag的内容

绕过方法还有很多这边就列举了几个简单易操作的出来

国科学院学生会是由国科学院指导开展的学员服务型组织，致力于配合国科学院完成日常工作的开展以及强化锻炼学员的自身职业素养与专业技能，下设部门有技术部和综合部。

如果你们也想提升自我，又或者是想认识这些和你们一样优秀的小伙伴，那就赶快联系指导老师并加入我们吧！

学生会信箱：

student@goktech.cn返回搜狐，查看更多

责任编辑：