XCTF web新手题（全）

原创

软大彭少 于 2020-09-22 23:49:39 发布 376 收藏 1
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/qq_46485934/article/details/108742396
版权

一.view source

无法右键查看源代码

- 方法一：ctrl +u
- 方法二：burp 抓包

二.get post

- 请用GET方式提交一个名为a,值为1的变量
  直接在url后面加上?a=1
- 请再以POST方式随便提交一个名为b,值为2的变量
  可以使用hackbar post传入b=2

三.robots

- robots协议
  Robots协议（也称为爬虫协议、机器人协议等）的全称是“网络爬虫排除标准”（Robots ExclusionProtocol），网站通过Robots协议告诉搜索引擎哪些页面可以抓取，哪些页面不能抓取.根据协议，网站管理员可以在网站域名的根目录下放一个robots.txt 文本文件，里面可以指定不同的网络爬虫能访问的页面和禁止访问的页面，指定的页面由正则表达式表示。网络爬虫在采集这个网站之前，首先获取到这个文件，然后解析到其中的规则，然后根据规则来采集网站的数据。

注意，这个协议的存在更多的是需要网络爬虫去遵守，而起不到防止爬虫的功能。


```
User-agent: *
Disallow:
Disallow: f1ag_1s_h3re.php
```

cyberpeace{62c8b2d4600db2153a0a354638da5866}

四.backup

- 如果网站存在备份文件，常见的备份文件后缀名有：“.git” 、“.svn”、“ .swp”“.~”、“.bak”、“.bash_history”、“.bkf” 尝试在URL后面，依次输入常见的文件备份扩展名。

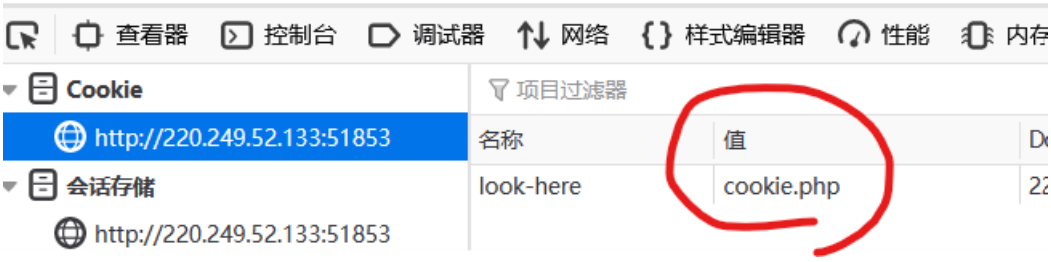
加上index.php后缀网页没反应
加上index.php.bak时提示下载文件，用txt打开得到flag

```
<?php
$flag="Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}"
?>
</body>
</html>
```

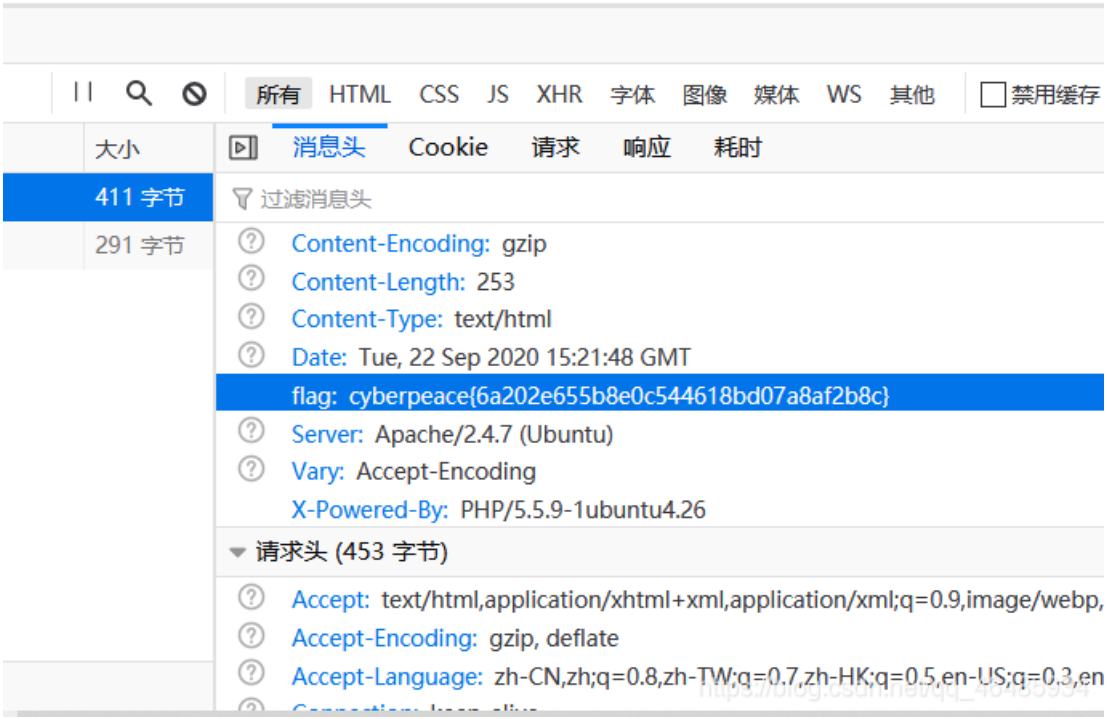
https://blog.csdn.net/qq_46485934

五.cookie

此题用浏览器的开发者工具即可解出



于是访问http://220.249.52.133:51853/cookie.php



* 关于cookie

Cookie（复数形态Cookies），又称为“小甜饼”。类型为“小型文本文件”[1]，指某些网站为了辨别用户身份而储存在用户本地终端（Client Side）上的数据（通常经过加密）。由网景公司的前雇员卢·蒙特利在1993年3月发明[2]。最初定义于RFC 2109。当前使用最广泛的 Cookie标准却不是RFC中定义的任何一个，而是在网景公司制定的标准上进行扩展后的产物。

简单的说，cookie就是服务端为了让用户不在每次访问需要登录的页面都要登录一次，而生成的一种证明身份的数据。服务器可以设置或读取Cookies中包含信息，借此维护用户跟服务器会话中的状态。

cookie中常常包含了一些敏感消息：用户名、计算机名、使用的浏览器和曾经访问的网站等，当得到没有过期的cookie时就能绕过登录甚至做更多的事。

六.disabled button

https://blog.csdn.net/qq_46485934

考察web前端知识

用开发者工具查看页面源代码

```
<html>
 <head> ... </head>
 <body>
  <h3>一个不能按的按钮</h3>
  <form action="" method="post">
   <input class="btn btn-default" disabled="" style="height:50px;width:200px;" type="submit" value="flag" name="auth">
  </form>
 </body>
</html>
```

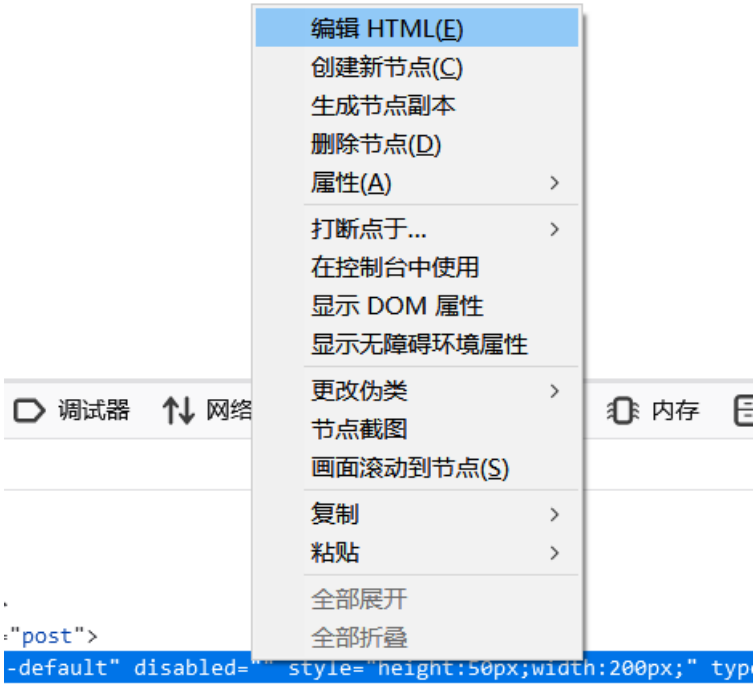
定义和用法

disabled 属性规定应该禁用 input 元素。

被禁用的 input 元素既不可用，也不可点击。可以设置 disabled 属性，直到满足某些其他的条件为止（比如选择了一个复选框等等）。然后，就需要通过 JavaScript 来删除 disabled 值，将 input 元素的值切换为可用。

https://blog.csdn.net/qq_46485934

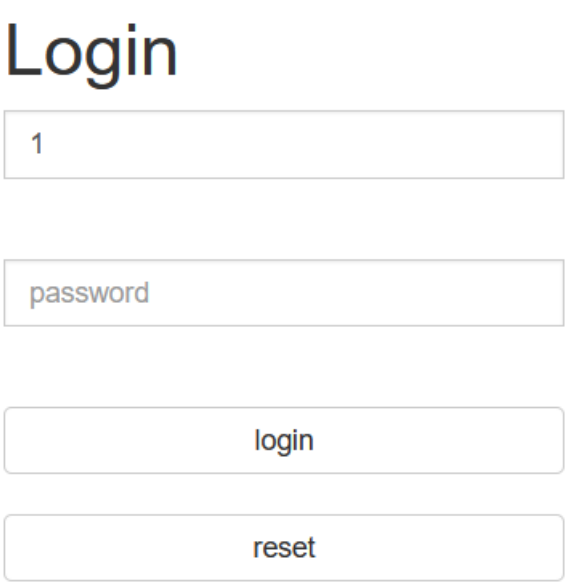
看完这段描述应该就明白了，直接把disabled 属性删掉就可以了



https://blog.csdn.net/qq_46485934

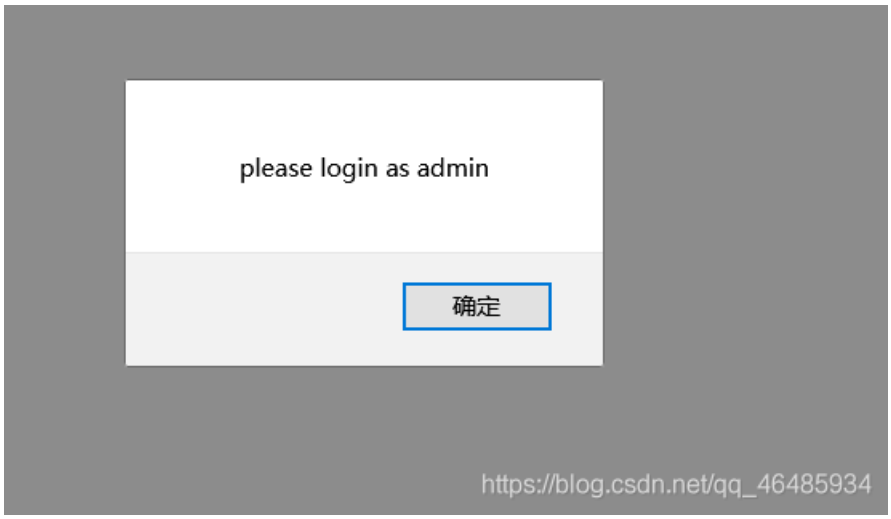
编辑HTML后点击按钮即可

七. weak auth



https://blog.csdn.net/qq_46485934

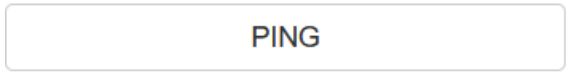
用户名输入1，密码也输入1



说明用户名要用admin
根据此题题意，猜测此题为弱密码
密码先猜admin,123456之类的
123456密码正确

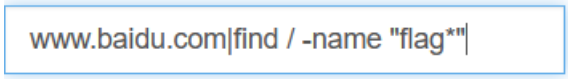
八.command execution

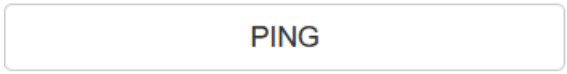
- 本题考的是命令执行漏洞方面的知识
- 命令执行漏洞是什么？
  当应用需要调用一些外部程序去处理内容的情况下，就会用到一些执行系统命令的函数。如PHP中的system，exec，shell_exec等，当用户可以控制命令执行函数中的参数时，将可注入恶意系统命令到正常命令中，造成命令执行攻击。
- 掌握有关命令执行的知识
  windows或linux下：
  command1 & command2 ：不管command1执行成功与否，都会执行command2（将上一个命令的输出作为下一个命令的输入），也就是command1和command2都执行
  command1 && command2 ：先执行command1执行成功后才会执行command2，若command1执行失败，则不执行command2
  command1 | command2 ：只执行command2
  command1 || command2 ：command1执行失败，再执行command2(若command1执行成功，就不再执行command2)
- write up




```
ping -c 3 www.baidu.com
```

https://blog.csdn.net/qq_46485934

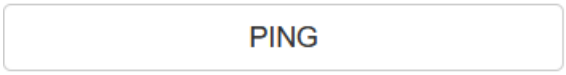





```
ping -c 3 www.baidu.com|find / -name "flag*"
/home/flag.txt
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu0/domain1/flags
```

https://blog.csdn.net/qq_46485934

发现有一个flag.txt文件，最后直接cat就行了




```
ping -c 3 www.baidu.com|cat /home/flag.txt
cyberpeace{a54001150237fee525ec8f6b6c44767b}
```

https://blog.csdn.net/qq_46485934

九. simple php

- 本题考查php的弱类型比较

```php
<?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;
}
?>
```

https://blog.csdn.net/qq_46485934

- 字符串和数字比较使用==时,字符串会先转换为数字类型再比较 php var_dump('a' == 0);//true，这里'a'会被转换数字0 var_dump('123a' == 123);//true，这里'123a'会被转换为123
  所以
  http://220.249.52.133:44940/?a=a&b=1235a

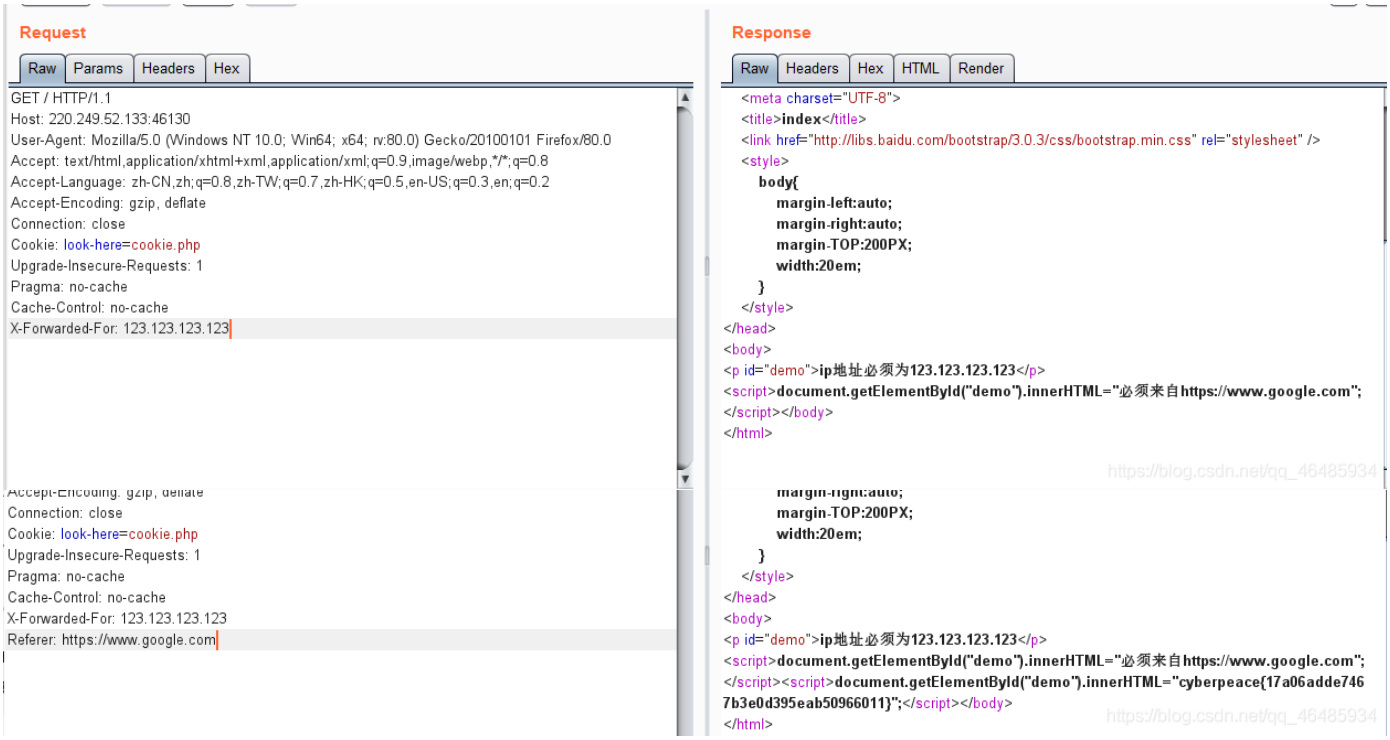
十.xff referer

点开题目，出现如下页面

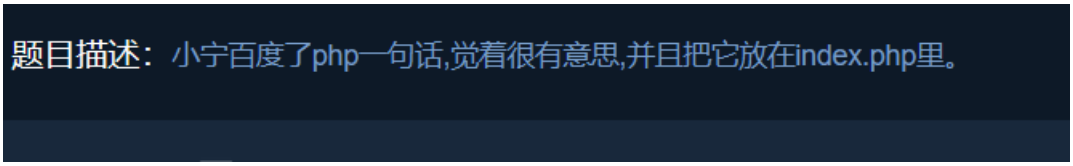
ip地址必须为123.123.123.123

https://blog.csdn.net/qq_46485934

- xff
  X-Forwarded-For（XFF）是用来识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址的HTTP请求头字段。 Squid 缓存代理服务器的开发人员最早引入了这一HTTP头字段，并由IETF在HTTP头字段标准化草案中正式提出。
- referer
  HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器该网页是从哪个页面链接过来的，服务器因此可以获得一些信息用于处理。
- 于是用brup抓包，在http头加一条X-Forwarded-For: 123.123.123.123
  发送请求



十一.webshell

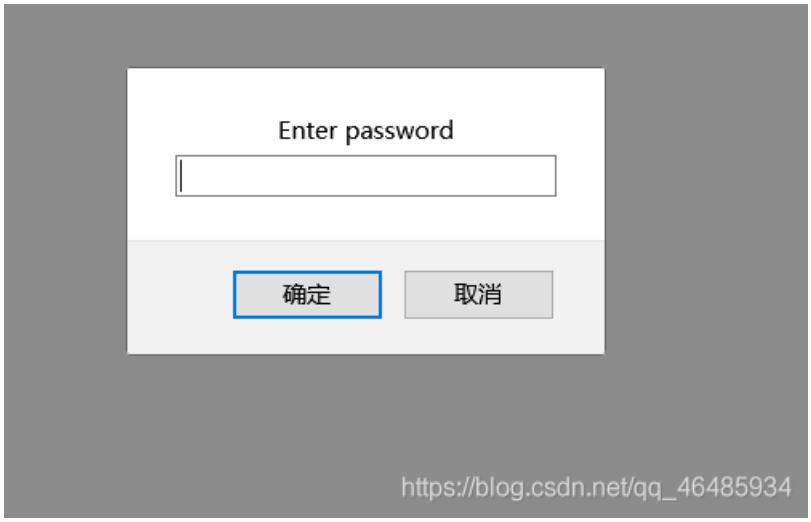


即 220.249.52.133:37476/index.php

https://blog.csdn.net/qq_46485934

密码为 shell,连接蚁剑看到有一个flag.txt,打开即可

十二.simple js



输了几次密码后就直接看源码

js学的太差了，看不懂，好懵，就去网上找了一篇博客

这里有一篇很好的blog大佬的blog

写的很好，佩服佩服！！！