攻防世界web新手区合集

原创

阿波次的鹅佛鸽 于 2019-08-07 15:31:49 发布 2789 收藏 15

分类专栏： web 文章标签： 攻防世界*（xctf）

本文链接：https://blog.csdn.net/CNXBDSa/article/details/98749664

攻防世界（xctf）做题合集-get_post- robots-backup-cookie-disabled_button-simple_php-weak_auth-xff_referer-simple_js-command_execution

注意有些题需要直接实践-不去实践永远别想进步

1.view_source

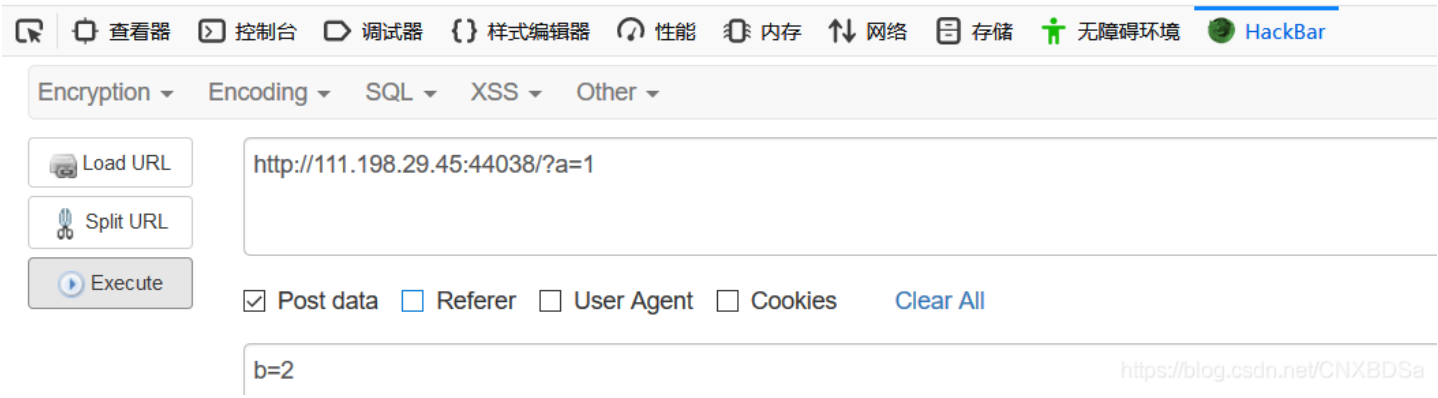
打开 然后查看源代码就找到flag了

```
cyberpeace{32b6a4b19085ce515ea82154233616e0}
```

2.get_post

出现请用GET方式提交一个名为a,值为1的变量那你就按照他说的去做呗 然后出现请再以POST方式随便提交一个名为b,值为2的变量你就继续按照他说的然后出现flag

cyberpeace{ced7d20233b4ef1547fd07d45d4c40ee}




```
cyberpeace{ced7d20233b4ef1547fd07d45d4c40ee}
```

3.robots

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 Exclusion Protocol），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 所以你就尝试去robots爬取网页的文件，尝试robots.txt 到一串f1ag_1s_h3re.php别高兴太早，这只是php文件，然后在刚刚那个ip后面加上这个就行了
http://111.198.29.45:48199/f1ag_1s_h3re.php然后得到flag

```
cyberpeace{2bf41890ddea15bde874d727a9982c0a}
```

4.Backup
备份文件(Backup File）,拷贝到存储介质上的文件，可以帮助您保护数据，以防其在系统硬件或存储介质出现故障时受到破坏 备份文件漏洞，产生该类漏洞的方式一般又三个：1.编辑器自动备份2.版本控制系统备份3.开发者主动备份 打开问我们你真的index.php文件吗？这就是备份文件所以我们构造index.php.bak完整的是http://111.198.29.45:54596/index.php.bak然后让我下载一个文件里面就有flag

```
cyberpeace{21a6b7b4d9d10bd134b64241be1b17a8}
```

5.cookie

cookie （储存在用户本地终端上的数据）打开后出现你知道什么是cookie吗？然后就构造cookie.php出现See the http response 首先想到的是抓包你可以通过Burpsuite去查看他的反应得到flag 你也可以在火狐浏览器里面F12查看他的网络找到的response找到flag

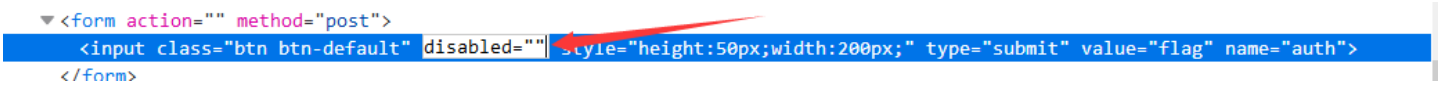

```
cyberpeace{2915b99a54efcc0670203d53c07122f9}
```

6.disabled_button

disabled 属性规定禁用按钮。

被禁用的按钮既不可用，也不可点击。

可以设置 disabled 属性，直到满足某些条件（比如选择一个复选框），才恢复用户对该按钮的使用。然后，可以使用 JavaScript 来清除 disabled 属性，以使文本区变为可用状态。所以本题的解题思路就是吧这个disabled标签改掉F12找到disabled



然后给他删掉 你就会发现那个flag的input输出标签可以点开，最后找到flag

```
cyberpeace{d8199b969d8c294edf6f18d458ef86a0}
```

7.simple_js

在题目上得到提示是关于js的所以进去f12找到源代码，点开找到 \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转化为字符串得到一串数字http://www.bejson.com/convert/ox2str/

55,56,54,79,115,69,114,116,107,49,50

然后在转化为字符串得到flag

```
cyberpeace{786OsErtk12}
```

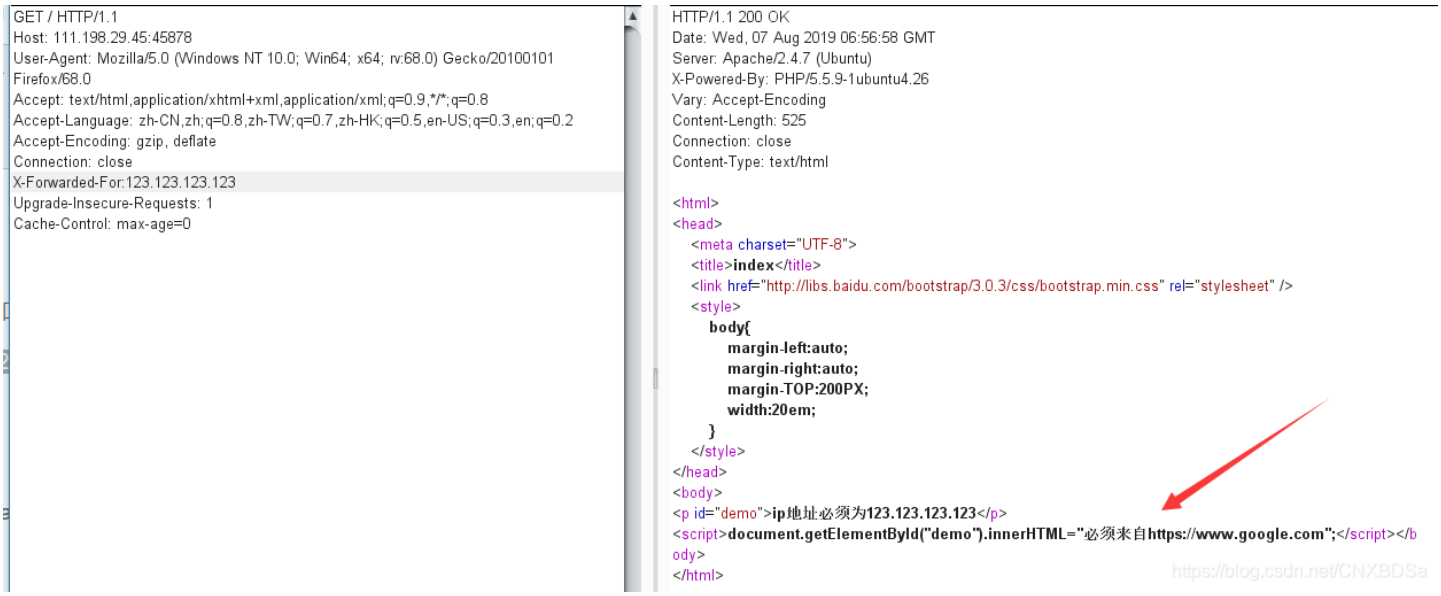
8.xff_referer

X-Forwarded-For 是一个 HTTP 扩展头部，主要是为了让 Web 服务器获取访问用户的真实 IP 地址

在一些大型网站中，来自用户的HTTP请求会经过反向代理服务器的转发，此时，服务器收到的Remote Address地址就是反向代理服务器的地址。在这样的情况下，用户的真实IP地址将被丢失，因此有了HTTP扩展头部X-Forward-For。当反向代理服务器转发用户的HTTP请求时，需要将用户的真实IP地址写入到X-Forward-For中，以便后端服务能够使用。由于X-Forward-For是可修改的，所以X-Forward-For中的地址在某种程度上不可信

这题就是这样的提示ip地址必须是123.123.123.123所以你burpsuite抓包构造

X-Forwarded-For:123.123.123.123他会出现



然后构造Referer:https://www.google.com

```
<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><s
cript>document.getElementById("demo").innerHTML="cyberpeace{3a5812cd288300af2aaf6175ea7ff30b}
";</script></body>
</html>
```

具体的是将

X-Forwarded-For:123.123.123.123

Referer:https://www.google.com

添加到反应头中

出现flag

```
cyberpeace{3a5812cd288300af2aaf6175ea7ff30b}
```

9.weak_auth

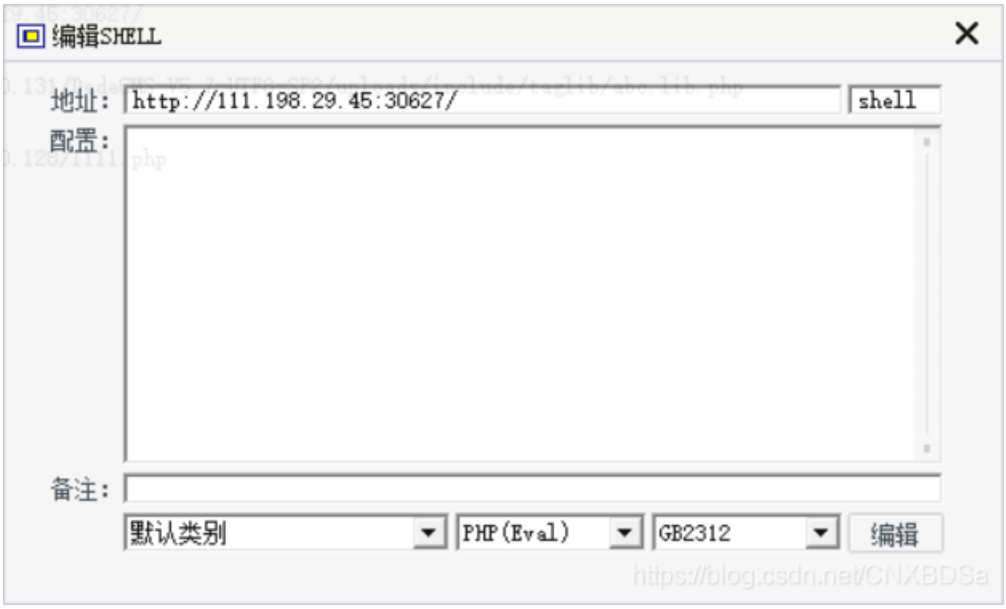
这题进去是一个登陆页面随手输入admin一管理员方式运行在输入密码不对然后爆破直接找到密码123456登陆找到

```
cyberpeace{5b130a17794b669202e27c4151447cb3}
```

10.webshell

简称后门，废话少说上工具中国菜刀，来呀，干一架啊，哈哈开玩笑的

进去后找到一个txt文件夹就是答案了




```
cyberpeace{f357a4904499b6346caefe7383cd696e}
```

11.command_execution
点上面标题可以去详细看一下命令执行、代码执行漏洞
这题我也没有搞太懂，后面搞懂了再来解释，请教大佬后也做出来了
首先ping
127.0.0.1 | ls …/…/…/
出现下面一大串
ping -c 3 127.0.0.1 | ls …/…/…/
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
run.sh
sbin
srv
sys
tmp
usr
var
然后在进入查看home文件
127.0.0.1 | ls …/…/…/home
出现ping -c 3 127.0.0.1 | ls …/…/…/home
flag.txt
然后进入flag文件中
127.0.0.1 | cat …/…/…/home/flag.txt找到flag

```
cyberpeace{9078bc16ef3b0be53fd5c657476d73e9}
```

又偷偷和大佬学习了一波（详情点击大佬两个字进去看大佬的博客）
127.0.0.1| find / -name "flag*"直接去找到flag更强
127.0.0.1|cat /home/flag.txt

12.simple_php

看代码先是显示两个函数输入a和b 然后是判断语句a=0并且a的值又不能为0 这是一个矛盾 所以构造?a=0A在后面加上一个A让a在等于0的同时加上一个非数字这个时候得到一半flag 继续向下看 第二个if语句 is_numeric函数 — 检测变量是否为数字或数字字符串，bool is_numeric (mixed $var)。如果 var 是数字和数字字符串则返回 TRUE，否则返回 FALSE 意思b要是数字就退出所以b不能是数字所以构造b=A 第三b要大于1234才出现flag 所以最终构造
http://111.198.29.45:35506/?a=0A&&b=123456A 然后出现flag

```
Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}
```