ctf web5 练习_攻防世界（Ctf-Web 新手练习区 Writeup）

原创

大坨坨儿 于 2021-01-12 10:01:50 发布
文章标签： ctf web5 练习

在打着暑假工赚零花钱之余，我将这些题利用空余时间刷了一遍，感觉内心还是比较满足的！

题目：view_source

这道题没啥好说的，在url的前面加上个 “view-source: ”就看到flag了

flag：cyberpeace{e07dcafaeeb31df23b4d661dd4da56f9}

题目：get_post

这道题我使用的方法是：旧版本火狐+旧版本的hackbar(新版本的hackbar要license)

hackbar勾选Post，load URL内容为：http://111.198.29.45:33495/?a=1，post data内容为：b=2，然后点击Execute即可看到flag了

flag：cyberpeace{c4e43c9c9d0f729358dd9417219a9da0}

题目:robots

这个题考到了Robots协议，也就是爬虫排除标准，于是肯定有个robots.txt文件，直接构造url访问这个文件，看到了禁止爬取：f1ag_1s_h3re.php这个页面，我们直接访问这个页面于是便得到了flag了

flag：cyberpeace{1b59446bc8e566382e01b0c209b899bd}

题目：backup

这道题考察的是备份文件漏洞，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

于是我们知道了备份文件：index.php.bak

下载后便得到flag了

flag：cyberpeace{4376485b1a095581d7fb57b8ab3bb924}

题目：cookie

在burpsuite我抓包发现指向了一个名为：cookie.php的页面，访问后提示我们看消息头，于是刷新后在消息头中进行查看，在响应头中发现flag了

flag：cyberpeace{e865c062128d651191621df4662b3573}

题目：disabled_button

这个题对于前端工作者来说绝对的简单的不能再简单了，直接删除掉disabled属性，就可以点击了

flag：cyberpeace{2e978e2dde5d8acdd7ff76f1c426bb29}

题目:simple_js

这个题真正的密码部分因该是：
\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

先要把这段16进制转换成10进制得到：55,56,54,79,115,69,114,116,107,49,50

然后直接一段python脚本解得flag

s=[55,56,54,79,115,69,114,116,107,49,50]for i ins:print(chr(i),end='')

flag：Cyberpeace{786OsErtk12}

题目：xff_referer

直接刷新一下burp截包，然后添加如下两行内容：

X-Forwarded-For:123.123.123.123

Referer:https://www.google.com

然后就看到flag了

flag：cyberpeace{63657c0c7f88a39a475f0de726ef109a}

题目：weak_auth

打开网页看到标题提示weak auth弱验证，这就没啥好说的了，没看到验证码，burp直接来爆破吧！

抓到包后右键send to intruder，在intruder的positions中选中密码，然后payloads导入字典开始start attack

瞬间就爆出了密码：123456，于是便得到了flag

flag：cyberpeace{04415bd2dac05f0e2cd712bb43c447b2}

题目：webshell

这个没啥好说的，菜刀连接上后发现目录下有个flag.txt，打开就看到了flag了

flag：cyberpeace{74fea3cfddba6bfdc6bfba5b38300b08}

题目：command_execution

打开网页在标题看到command execution 命令执行，那就没啥好说的了，看看目录下有些啥吧!

ping -c 3 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

习惯性的看看home里有什么

ping -c 3 127.0.0.1 | ls /home

flag.txt

ping -c 3 3 127.0.0.1 | cat /home/flag.txt

cyberpeace{39190fc825ce46b116b6829f0c13d625}

于是便得到了flag！

flag：cyberpeace{39190fc825ce46b116b6829f0c13d625}

题目：simple_php

这道题在阅读了PHP代码后，发现，要a==0，但a的值又不能为0，因此让a=0+任意非数字字符，而 b=数字就退出， 于是构造：?a=0a&b=12345A便得到完整的flag

flag：Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

到这儿，新手练习区的web题算是解完了，题目虽然不难，但是非常的经典！