XCTF web新手练习区_1-12

转载

H4ppyD0g 于 2019-07-15 09:13:30 发布 1956 收藏 13

分类专栏： CTF

CTF 专栏收录该内容

45 篇文章 0 订阅

订阅专栏

1 view_source

查看网页源码的方法：

(1) F12(如果只按F12没反应，就功能键+F12)可以查看网页源码。

(2) 网页源码的url以view-source: 开头。在本网页的url前面加上这个可以获取。

(3) 通过python的requests.get()可以获取网页源码。

---

2 get_post

用到了火狐的插件， hackbar。添加完后是在F12的检查里面。

hackbar的第一个框是填url的，在后面添加?a=1作为get请求。

run一下就到了下一个页面，再在下面输入b=2再run一下，爆出flag。

知识点：通过url使用get传参格式：网址?参数名=值&参数名=值。有时需要在?前面加个/

---

3 robots

知识点：通常在网页的url后面加/robots.txt就可以转到该页面的robots协议。爬虫的话需要遵守这个规定，否则可能会承担法律风险。

方法一：

直接在url后面添加/robots.txt，发现有一个不允许访问的php文件，在原有url后边添加这个php文件路径，访问它爆出flag。

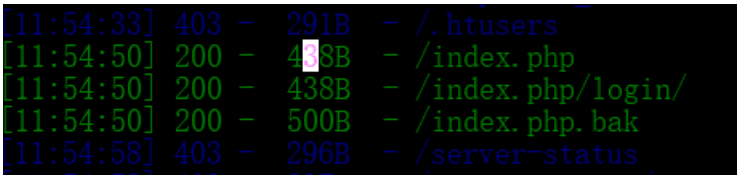
方法二：用burp抓包，发送到spider后，去target界面，找到爬取的文件，发现这个url路径下有几个文件，找到f1ag_1s_h3re.php，把它放在url后面，爆出flag。

---

4 backup

知识点：常见的备份文件后缀名有: .git .svn .swp .svn .~ .bak .bash_history

使用网上的扫描后台的py脚本。
命令：py dirsearch.py -u http://111.198.29.45:50543 -e *



访问index.php.bak下载文件，得到flag.

---

5 cookie

知识点：Cookie，有时也用其复数形式 Cookies，指某些网站为了辨别用户身份、进行 session 跟踪而储存在用户本地终端上的数据（通常经过加密）。

F12后看这个网页的响应，找到cookie.php，访问后提示查看response，在响应头里找到flag。

---

6 disabled_button

F12，查看网页源码，把按钮属性 disabled="" 删掉，就可以点击按钮了，也是在源码中爆出flag。
注意自己修改完网页源码后不能刷新。

---

7 simple_js

知识点：url编码是一种浏览器用来打包表单输入的格式。浏览器从表单中获取所有的name和其中的值，将它们以name/value参数编码（移去那些不能传送的字符，将数据排行等等）作为URL的一部分或者分离地发给服务器。URL编码遵循下列规则：每对name/value由&；符分开；每对来自表单的name/value由=符分开。如果用户没有输入值给这个name，那么这个name还是出现，只是无值。任何特殊的字符（就是那些不是简单的七位ASCII，如汉字）将以百分符%用十六进制编码，当然也包括象 =,&；，和 % 这些特殊的字符。其实url编码就是一个字符ascii码的十六进制。不过稍微有些变动，需要在前面加上“%”。

将字符串转换为URL编码
%35%35%2c%35%36%2c%35%34%2c%37%39%2c%31%31%35%2c%36%39%2c%31%31%34%2c%31%31%36%2c%31%30%37%2c%34%39%2c%35%30
解码得：55,56,54,79,115,69,114,116,107,49,50
输出ascii码对应的字符，得到flag括号里的字符串。

---

8 xff_referer

知识点：
X-Forwarded-For:简称XFF头，它代表客户端，也就是HTTP的请求端真实的IP，只有在通过了HTTP 代理或者负载均衡服务器时才会添加该项
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，告诉服务器我是从哪个页面链接过来的，服务器基此可以获得一些信息用于处理

修改X-Forwarded-For可以用火狐浏览器插件X-Forwarded-For Header。
直接修改成123.123.123.123就可以了，然后页面显示必须来自谷歌url，
bp抓包发送到repeater， 添加Referer 值为需要的url，go一下爆出flag。

---

9 weak_auth

知识点：弱口令(weak password) 没有严格和准确的定义，通常认为容易被别人（他们有可能对你很了解）猜测到或被破解工具破解的口令均为弱口令。弱口令指的是仅包含简单数字和字母的口令，例如“123”、“abc”等，因为这样的口令很容易被别人破解，从而使用户的计算机面临风险，因此不推荐用户使用。

暴力破解可以用bp抓包，发送到intruder，然后添加自己的字典，start attack进行爆破。

随便输入账号和密码，提示用admin登录，那么就暴力admin的密码就可以了，在爆破的结果中看到一个长度不一样的，点开response，可以看到flag。

---

10 webshell

shell=print_r(scandir(getcwd())); 得到网页路径下的目录，页面信息改变，看到里面有flag.txt
shell=print_r(show_source(“flag.txt”));爆出flag。

知识点：
getcwd()会将当前工作目录的绝对路径复制到参数buffer所指的内存空间中,参数maxlen为buffer的空间大小。成功则返回当前工作目录，失败返回 FALSE。可以无参调用这个函数。
scandir() 函数返回指定目录中的文件和目录的数组。
print_r() 函数用于打印变量，以更容易理解的形式展示。
show_source() 函数对文件进行语法高亮显示。
当使用这个函数时，整个文件都会被显示，包括密码和其他敏感信息。

---

11 command_execution

知识点
Web应用防护系统（也称为：网站应用级入侵防御系统。英文：Web Application Firewall，简称： WAF）。
WAF对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站站点进行有效防护。

windows或linux下shell执行顺序：
command1 && command2 先执行command1后执行command2
command1 | command2 只执行command2
command1 & command2 先执行command2后执行command1

ls命令用于显示指定工作目录下之内容（列出目前工作目录所含之文件及子目录)
cat 命令用于连接文件并打印到标准输出设备上。

需要用到hackbar，以post方式提交数据
target=127.0.0.1 | ls …/…/…/home显示home文件下的文件目录
target=127.0.0.1 | cat …/…/…/home/flag.txt显示flag.txt文件内容
不知道为啥得是target。

---

12 simple_php

知识点：
php弱类型，==作用是将两个变量转换成相同类型再比较。而 ===必须是两个变量类型相同值也相同才会返回真。
is_numeric($num)表示如果num是数字或数字字符串则返回true，否则返回false。
如果num是字符串类型，则会从前读到第一个非数字后停止，只截取前面的数字字符部分。

构造get请求：http://111.198.29.45:54873/?a=0x&b=1235x 爆出flag。