XCTF攻防世界WEB新手练习篇

原创

夜车星繁 于 2019-11-15 21:13:40 发布 1264 收藏 7
分类专栏： ctf

本文链接：https://blog.csdn.net/weixin_44740377/article/details/95796615

做了很多题，web方向：

攻防世界web

*来到齐学长推荐的攻防世界：*https://adworld.xctf.org.cn/task

第一道题略过；

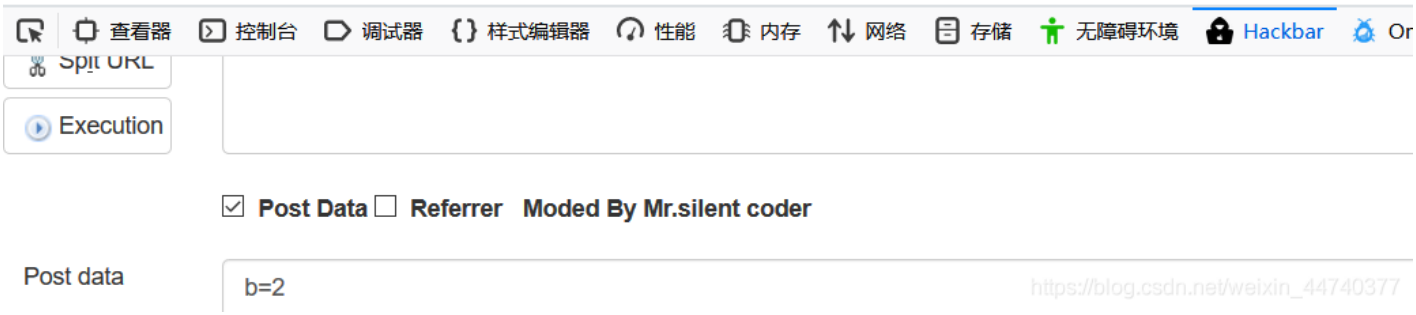
2.get_post

比较简单，按照提示两步即可得到flag

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{28b6acf28d0fa0a5542f721a867682d2}



HTTP协议中共定义了八种方法或者叫“动作”来表明对Request-URI指定的资源的不同操作方式，具体介绍如下：

- GET：向特定的资源发出请求。
- POST：向指定资源提交数据进行处理请求（例如提交表单或者上传文件）。数据被包含在请求体中。POST请求可能会导致新的资源的创建和/或已有资源的修改。
- OPTIONS：返回服务器针对特定资源所支持的HTTP请求方法。也可以利用向Web服务器发送'*'的请求来测试服务器的功能性。
- HEAD：向服务器索要与GET请求相一致的响应，只不过响应体将不会被返回。这一方法可以在不必传输整个响应内容的情况下，就可以获取包含在响应消息头中的元信息。
- PUT：向指定资源位置上传其最新内容。
- DELETE：请求服务器删除Request-URI所标识的资源。
- TRACE：回显服务器收到的请求，主要用于测试或诊断。
- CONNECT：HTTP/1.1协议中预留给能够将连接改为管道方式的代理服务器。

3.**robots**

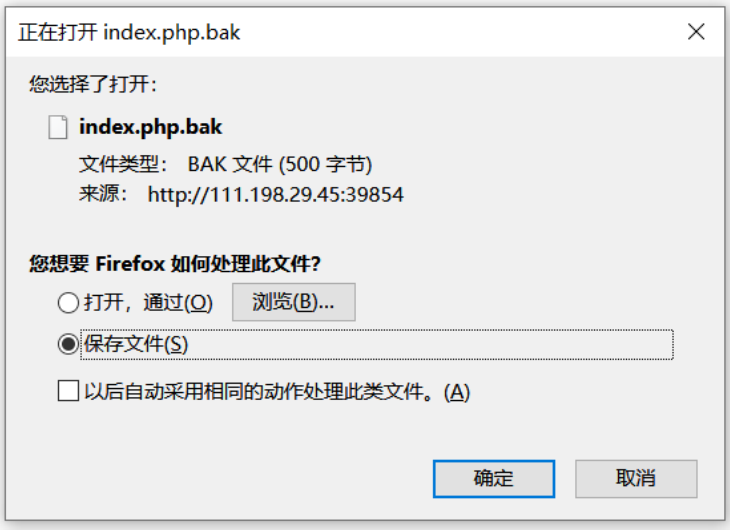
这道题我是用御剑扫描：

发现隐藏文件，构造url即可：


```
User-agent: *
Disallow:
Disallow: flag_1s_h3re.php
```

4.backup

打开即可得到flag：

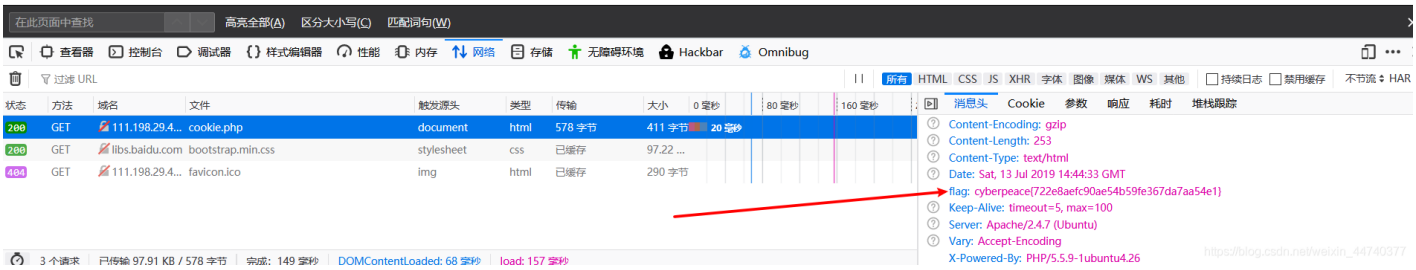


你知道index.php的备份文件名吗?

5.cookie

同上，先构造url，F12查看网络：

See the http response

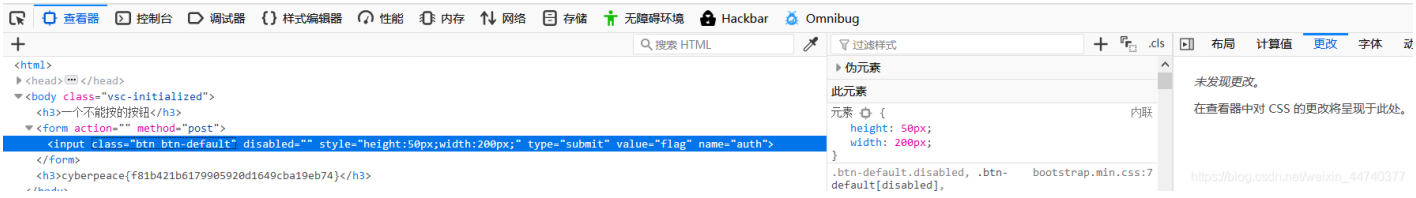


6.

一个不能按的按钮

flag

cyberpeace{f81b421b6179905920d1649cba19eb74}



7.simple js

随便输入，查看源码，在最底下发现一段16进制编码，转化为字符，发现为一段数字，再次转化为字符串，通过源码分析得知即为flag的内容.

8.xff_referer

有关**X-Forwarded-For**和**Referer**的知识

- 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。
- xff 是http的拓展头部，作用是使Web服务器获取访问用户的IP真实地址（可伪造）。由于很多用户通过代理服务器进行访问，服务器只能获取代理服务器的IP地址，而xff的作用在于记录用户的真实IP，以及代理服务器的IP。
- 格式为：X-Forwarded-For: 本机IP, 代理1IP, 代理2IP, 代理2IP
- referer 是http的拓展头部，作用是记录当前请求页面的来源页面的地址。服务器使用referer确认访问来源，如果referer内容不符合要求，服务器可以拦截或者重定向请求。

通过burp截包然后添加X-Forwarded-For: 123.123.123.123与Referer: https://www.google.com

得到flag。

9.weak_auth

burpsuite爆破即可，我burpsuite软件嗝屁了，搁这儿耽误我半小时了。。。

10.webshell

中国菜刀打开即可。

有道：文档：Linux.note
链接：http://note.youdao.com/noteshare?id=a35c6eb1230fefee2b651368688c746c

执笔至此，还有许多作业没有完成。

攻防世界的杂项做了二十多道有点疲劳，博客又懒得写。。。国庆期间我要进阶啊！！