XCTF攻防世界Web新手入门题WP

原创

A1andNS 于 2019-11-09 15:53:04 发布 473 收藏 3

分类专栏： WP 文章标签： 网络安全 CTF

本文链接：https://blog.csdn.net/qq_26139045/article/details/102987903

攻防世界Web新手入门题(1-6)WP兼学习笔记

第一题：view_source

这一题从题目开始就在进行暗示，view_source意为观看源代码，这就是在明确说要去看网页源代码。

打开网页就是熟悉的flag不在这里，但是flag应该就在source里，所以使用F12进行源码查看，轻松找到了flag：cyberpeace{cc134ff06c517674b100366d6f6e4466}

```
<html lang="en"> event
  <head> ··· </head>
  <body>
    <script> ··· </script>
    <h1>FLAG is not here</h1>
    <!--cyberpeace{cc134ff06c517674b100366d6f6e4466}-->
  </body>
</html>
```

考察点

在网页源代码里通过注释的方式隐藏内容

观察和思考

在工作中，确实存在一些程序员为了方便或者提醒自己，会用这种极其不安全的手段来记录某些信息，这将带来严重的安全隐患。在工作生活中编写前端html代码时也要注意在网页发布时，去除开发过程中的注释，以免重要的信息泄露。据我的观察，也会有一些公司故意利用这种特性来进行自我宣传和广告，大多时科技公司，例如百度网页的源代码，近期就是校招的广告。在源代码里做宣传，一般也就是科技公司所为了，除了IT工作者，还有谁会无聊到去看源代码呢。

第二题：get_post

这一题，看到题目就联想到了post类型的请求。打开网页提示我们用get方式传入一个参数a=1，所以直接在url后面添加`?a=1`即可。之后又提示要我们用post传入一个b=2，所以使用hackbar工具，传入一个post请求类型的b=2，得到我们想要的flag:cyberpeace{2c088170d7c39c5ab26ca88b5af60216}

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{2c088170d7c39c5ab26ca88b5af60216}

考点

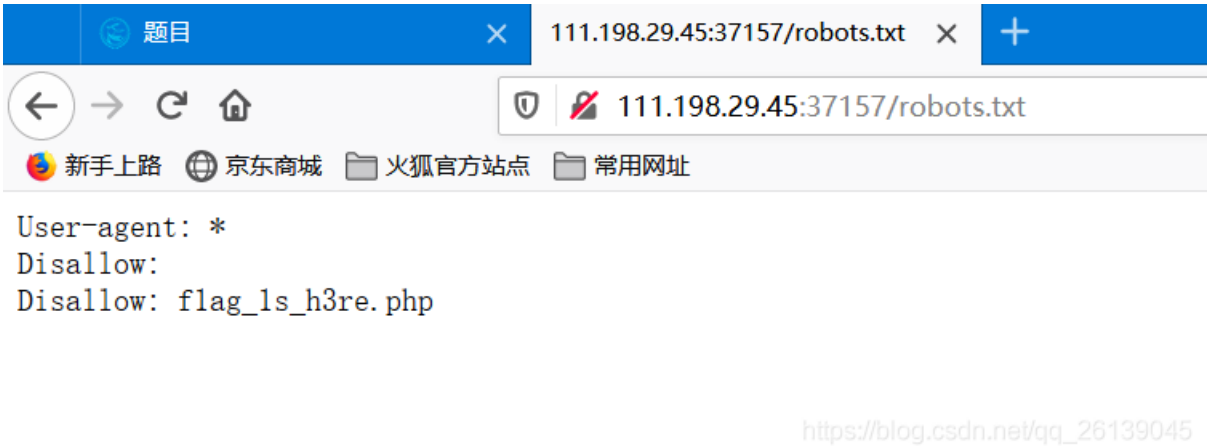
考察对http请求中的post类型和get类型请求的理解和应用。

观察与思考

HTTP协议里，对于请求类型的定义远不止于GET和POST类型，但是大多数使用的是这二者。例如还有OPTION（请求一些选项的信息）、HEAD（请求读取由URL所标志的信息的首部）、PUT（在指明的URL下储存一个文档）、DELETE（删除指明的URI所标志的资源）、TRACE（用来进行环回测试的请求报文）、CONNECT（用于代理服务器）。但这些请求方式相比本题中的两种风险更大，因为有的涉及到了资源的删除和储存文件。但是GET和POST类型依旧会存在一些风险，这就需要在编写后端代码的时候注意进行过滤，防止黑客而已传入参数。

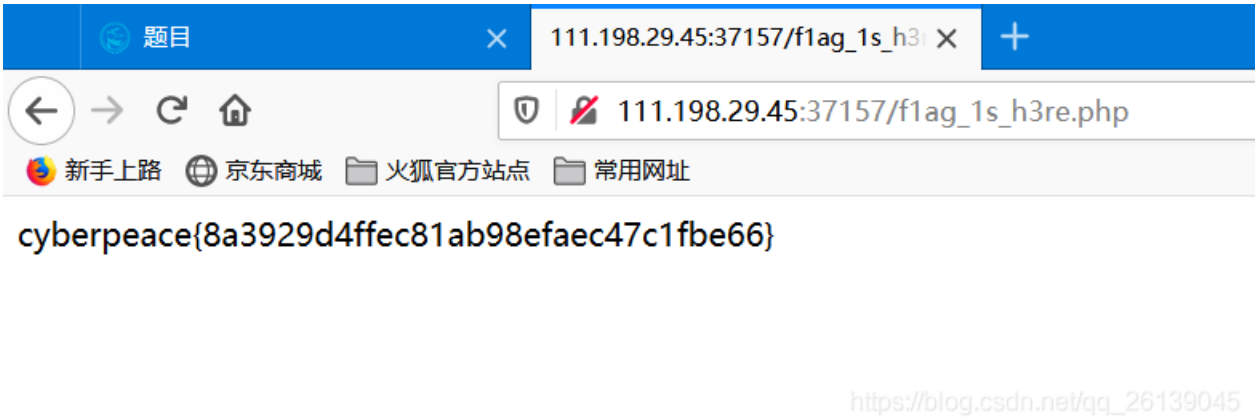
第三题：robots

这题题目和提示都很明显的指向了robots协议，所以在url的结尾加上robots.txt，打开查看txt。



所以可以得到第一提示，它不允许所有的搜索引擎爬过，不被允许的内容是一个flag_1s_h3re.php的网页文件。

所以直接去访问这个网页。



得到了flag： cyberpeace{8a3929d4ffec81ab98efaec47c1fbe66}

考察点

robots协议的相关知识

观察和思考

这题涉及到了robots协议。 robots是网站跟爬虫间的协议，用简单直接的txt格式文本方式告诉对应的爬虫被允许的权限，也就是说robots.txt是搜索引擎中访问网站的时候要查看的第一个文件。 所通过在这个txt文档里添加相关的一些内容来禁止搜索引擎爬取相关的网页和路径。这样搜索引擎就只会爬取未经限制的网页。

每当用户试图访问某个不存在的URL时，服务器都会在日志中记录404错误（无法找到文件）。每当搜索蜘蛛来寻找并不存在的robots.txt文件时，服务器也将在日志中记录一条404错误，所以你应该做网站中添加一个robots.txt。 如果你在robots.txt里面设置了禁止所有搜索引擎爬取，那么就会导致你的网页无法被搜索引擎收录。那就再学习一下robots.txt文件的格式

User-agent:该项的值用于描述搜索引擎robot的名字，如果是*表示的是所有的搜索引擎

Disallow:该项的值用于描述不希望被访问到的一个URL，这个URL可以是一条完整的路径，也可以是部分的，任何以Disallow开头的URL均不会被robot访问到。

Allow:该项的值用于描述希望被访问的一组URL，与Disallow项相似，这个值可以是一条完整的路径，也可以是路径的前缀，以Allow项的值开头的URL是允许robot访问的。

我们常用的搜索引擎类型有：

google蜘蛛：googlebot

百度蜘蛛：baiduspider

yahoo蜘蛛：slurp

alexa蜘蛛：ia_archiver

msn蜘蛛：msnbot

有一些题目也会把flag藏在某个隐藏目录下

第四题：backup

根据提示他要我去寻找备份文件，进入网页问我们index.php的备份文件。那么我就再url处输入index.php.bak访问，跳出下载框，我下载文件到本地打开它。

得到flag：Cyberpeace{855A1C4B3401294CB6604CCC98BDE334}

考察点

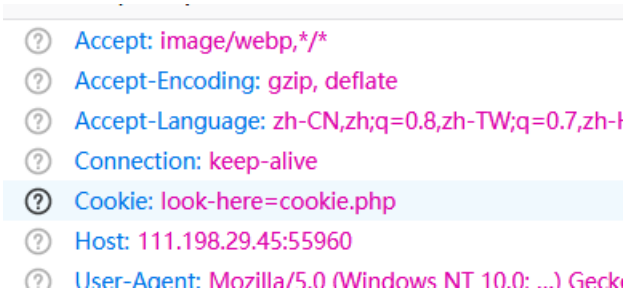
考察对网页文件的备份名称了解，后缀为`.bak`

思考

一些网络管理员再一些目录下，放置了网页备份文件，导致备份文件泄露，这是一种极其不安全的行为，应该要注意这个问题。如果重要的信息被泄露，将会让攻击者有机可乘，造成网站损失。

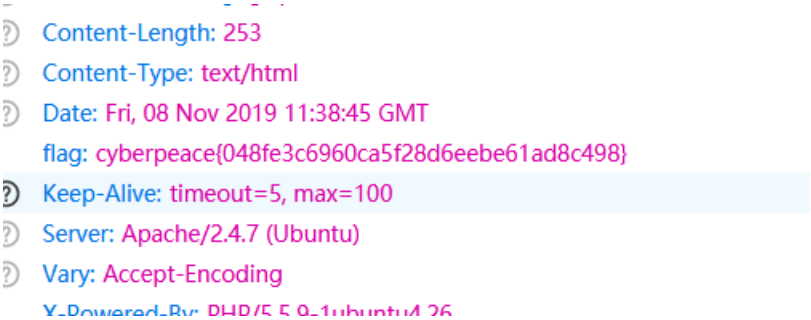
第五题：cookie

看提示就知道适合cookie相关的内容。打开之后问我知不知道cookie，我下意识的去看来一下cookie



看到了一个提示cookie.php所以我就访问了cookie.php

根据网页的提示我看了http的请求头



得到的flag：cyberpeace{048fe3c6960ca5f28d6eebe61ad8c498}

考察点

cookie相关知识，这里是查看网页cookie

观察与反思

Cookie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 。服务器可以利用Cookies包含信息的任意性来筛选并经常性维护这些信息，以判断在HTTP传输中的状态。Cookies最典型的应用是判定注册用户是否已经登录网站，用户可能会得到提示，是否在下一次进入此网站时保留用户信息以便简化登录手续，这些都是Cookies的功用。 所以cookie使用被攻击者利用从而导致重要的信息泄露。所以要重视对cookie的保护。

第六题： disable_button

从题目是不可用的按钮，以及描述里提到的前端知识。就知道是要修改前端代码来让按钮可以点按。

果然一个不能按的按钮，查看前端代码

修改代码把disable改为able即可

点按button得到一个flag

cyberpeace{0f10ea6ef3068a2eedf94be8d546739a}

考察点

前端代码的理解和修改

观察和思考

对前端的一些修改时可以达到一些绕过前端限制的效果，所以很多时候前端限制的效果不好，反而容易被人破解了，所以应该从后端上来进行限制会比较好。