CTF入门

原创

小叮当不懒 于 2020-04-10 21:22:46 发布 303 收藏

文章标签： 机器学习

本文链接：https://blog.csdn.net/qq_46546793/article/details/105417491

CTF入门指南：https://www.ichunqiu.com/course/57517

入门基础

1.编程语言基础（C语言，汇编语言，脚本语言）
2.数学基础（算法，密码学）
3.脑洞大开(天马行空的想象，推理解密）
4.体力耐力（各种通宵熬夜不睡觉）

如何入门

1.恶补基础知识（有基础的跳过此步）
2.尝试从脑洞开始（hackgame）
3.从基础题目出发
4.学习信息安全专业知识
5.锻炼体力耐力

学习之前的思考

CTF分为五个部分：WEB MISC RE 密码学 PWN
如何学习：1.分析赛题情况
2.分析自身能力
3.选择更适合的入手

1.分析赛题情况
PWN、Reverse偏重对汇编、逆向的理解。
Crypto偏重对数学、算法的深入学习。
Web偏重对技巧沉淀、快速搜索能力的挑战。
Misc则更为复杂，所有与计算机安全挑战有关的都算在其中。
2.分析自身的能力（兴趣）
自己对哪一方面比较擅长，比较感兴趣。
3.选择更适合的入手
分析自己的兴趣与特长，然后根据题目的不同特点来选择适合自己的类型。

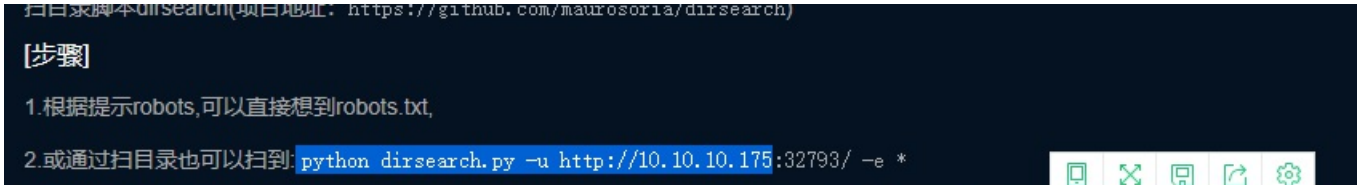
实例

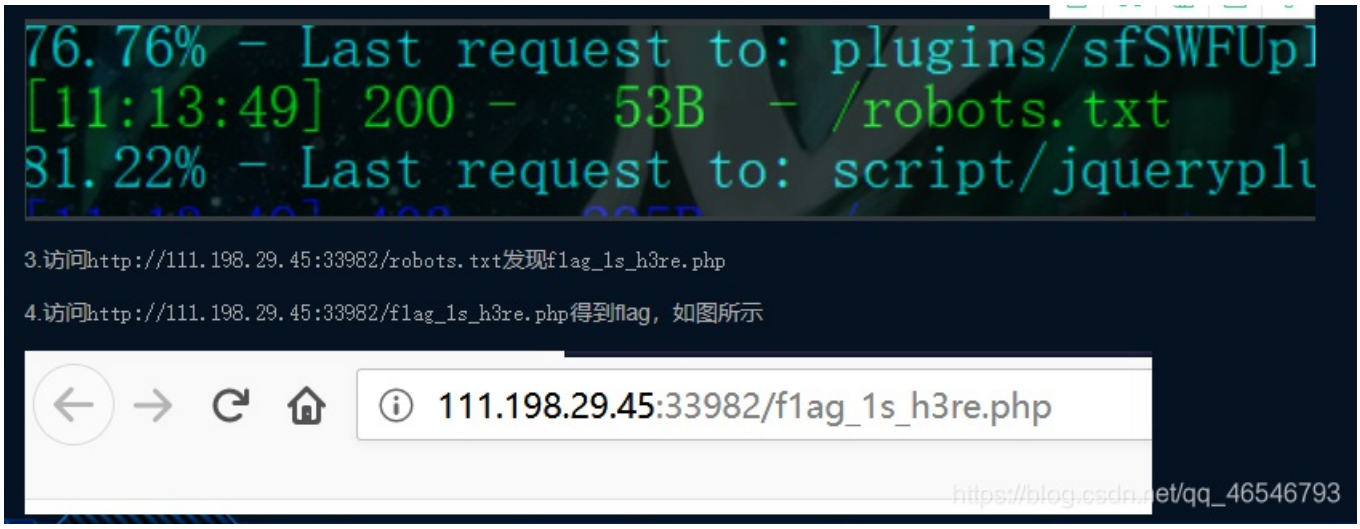
这是属于web类的新手题，分析了一下，web好像是查看网页的源代码。除了鼠标右键以外，Ctrl+u也是查看源码的快捷键。而这一题，由于右键无效，所以只能以Ctrl+u进入源码界面，而flag就在源码的注释里。

```
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Where is the FLAG</title>
</head>
<body>
<script>
document.oncontextmenu=new Function("return false")
document.onselectstart=new Function("return false")
</script>


<h1>FLAG is not here</h1>


<!-- cyberpeace{b8ab5071aa3b000b92c8af865c9321b4} -->

</body>
</html>
```


机器人协议。

发现并不是所有的题目都是这么简单的，方法也非常多，学的还很多，要杂。这个题目就完全没有方法，然后看了答案，理解一半一半。




76.76% - Last request to: plugins/sfSWFUpl
[11:13:49] 200 - 53B - /robots.txt
81.22% - Last request to: script/jqueryplu
3.访问http://111.198.29.45:33982/robots.txt发现f1ag_1s_h3re.php
4.访问http://111.198.29.45:33982/f1ag_1s_h3re.php得到flag，如图所示
111.198.29.45:33982/f1ag_1s_h3re.php
https://blog.csdn.net/qq_46546793