

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

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侧重对汇编、逆向的理解。

Crypto侧重对数学、算法的深入学习。

Web侧重对技巧沉淀、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



题目描述: X老师让小宁同学查看一个网页的源代码, 但小宁同学发现鼠标右键好像不管用了。

题目场景:  http://159.138.137.79:50560

[删除场景](#)

倒计时: 03:56:28 [延时](#)

题目附件: 暂无

https://blog.csdn.net/qq_46546793

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>
```

https://blog.csdn.net/qq_46546793


robots

 51 最佳Writeup由MOLLMY提供

难度系数:  1.0

题目来源: [Cyberpeace-n3k0](#)

题目描述: X老师上课讲了Robots协议, 小宁同学却上课打了瞌睡, 赶紧来教教小宁Robots协议是什么吧。

题目场景:  http://159.138.137.79:59505

[删除场景](#)

倒计时: 03:56:18 [延时](#)

题目附件: 暂无

https://blog.csdn.net/qq_46546793

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。

扫目录脚本dirsearch(项目地址: <https://github.com/maurosoria/dirsearch>)

[步骤]

1. 根据提示robots, 可以直接想到robots.txt,

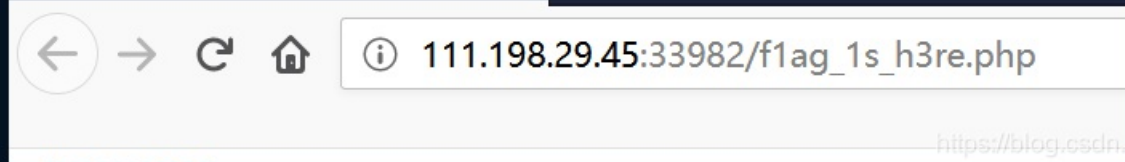
2. 或通过扫目录也可以扫到: `python dirsearch.py -u http://10.10.10.175:32793/ -e *`



```
76.76% - Last request to: plugins/sfSWFUp]
[11:13:49] 200 - 53B - /robots.txt
81.22% - Last request to: script/jqueryplu
[11:13:49] 200 - 205B - /
```

3.访问<http://111.198.29.45:33982/robots.txt>发现flag_1s_h3re.php

4.访问http://111.198.29.45:33982/f1ag_1s_h3re.php得到flag, 如图所示



https://blog.csdn.net/qq_46546793