Web入门指南

引言

欢迎诸位访问这份文档！或许你们在网络世界中听过"Web"这个词，但它究竟意味着什么，却仍是个未解之谜。别着急，你们来对地方了。在本文中，我将为大家揭开Web的神秘面纱，为你们深入浅出地解释这个领域的内涵。

"Web"指南，正式启程！

介绍一下Web

web专注于寻找并利用Web应用程序中的漏洞，以获取未经授权的访问或控制权。不过，它远不只是技术，更是对创造力、分析能力和逆向思维的考验。

源自黑客文化，Web漏洞挖掘最初是为了探索技术并挑战系统而兴起。它起初可能只是用来发现Web应用程序中的弱点，然后逐渐发展成一项实践，专注于发现问题并向开发者展示如何修复。

在CTF比赛中，你将亲身体验到Web漏洞挖掘的神奇之处。比赛为你提供虚拟的Web应用程序，隐藏着各种类型的漏洞。你的任务是理解应用程序的运行方式，找出潜在的漏洞，然后设计攻击以验证它们的存在。这可能包括构造特定的输入、绕过访问控制，甚至是利用漏洞来实现控制权。

你可以将Web漏洞挖掘比作数字时代的"寻宝冒险"。在这个冒险中，你通过寻找和解决漏洞来揭示隐藏的“宝藏”，即攻击目标或称为flag的关键信息。这是一个令人兴奋且有趣的技能，它不仅帮助你理解应用程序的脆弱性，还提高了你的网络安全意识和防御技能。

怎么学

1. 如何获取知识

   ctf知识的学习与课内一板一眼式的教书不同，如果你想要获得成长的能力，那么你**必须**获取**自主获取知识**的能力。

   - 学会使用搜索引擎
     - 优先选择google和bing
   - 人工智能chatGPT

        - 人工智能不怕累、不怕麻烦，值得重复问一些简单问题
    - GitHub等开源社区
    - 向学长学姐们寻求帮助，学长学姐们都很友善的
2. 如何练习
    - 一些靶场
        - DVWA
        - pikachu
    - 一些练习场
        - Xctf
        - buuoj
3. 学会看题解write up（wp）

    在平时的练习中，肯定会遇到不会的题，千万不要死磕，不会就看wp，下一道更好！ 在搜索引擎或者开源社区查找wp，在看wp的过程中，补充并且掌握自己的不会的知识点
4. 保持记笔记，写心得的习惯。及时记录下来学习的内容以及遇到的问题，回头再看的时候也是一种很好的资源。
    - 建议学习一个markdown语法
    - 推荐一个好用的工具，obsidian，可以作为自己的知识库来使用
    - 和obsidian类似的软件，Typora。这里其实不一定得这个，只要能记录你学习过程的都可以（写心得之类的），记录很重要，它不仅能在后期帮你快速回忆与许久未用的已学知识点，同时也记录你学习的过程十分有意义

前置知识

---

1. 配置环境

    一定要有耐心！ 一套环境不是十分钟二十分钟就能配完的，对于新手而言，几天甚至一两周都有可能，反复地确认自己的步骤、教程的日期、教程使用的系统版本是否正确；

    尽量选择官方网站的配置方式：寻找document字样去看文档，这是最稳的方法，但是比较费力；可以去看私人的文章，但不一定能成功

    可以尝试自己配一套LAMP环境、一台虚拟机
2. 语言

    当提到计算机，不可避免地需要了解编程，事实上，已经存在相当多主流的编程语言，有一些适用于提供和处理web服务，例如python, java, php, golang, rust，你需要具备对于这些代码最少有审计能力（看得懂在做什么）

精通一门语言，搓脚本用

3. 工具
   - 会魔法很重要
   - Burpsuite
   - Hackbar
   - sqlmap

   其他工具用得上再补充~

   相信到时候你们已经有能力自己找到相关工具并且使用了
4. 计网知识
   - 标准的OSI七层模型，重点了解TCP
   - 了解“协议”，如：http，https，ftp，gopher，php伪协议等等
5. 服务框架

   有现成的网络框架用于高效并发处理请求，所以你需要了解函数是干嘛用的，怎么处理请求的
   - python：Flask , Django , Tomado
   - java：spring , Boot
6. 用户凭证

   http是无状态协议，因此需要储存处理用户信息，你需要了解：
   - cookie
   - session
   - jwt

   有时会涉及到用户信息伪造，例如flask框架下的session伪造，通过获取（或者弱口令爆破）secret_key来伪造

   一个session，通常需要自己写脚本（或者获取GitHub现成的脚本改一改使用）
7. 数据库管理系统（DBMS）

   你需要知道去哪儿了解不同DBMS的sql语法，以便完成相应的挑战：
   - sql injection注入：查询脚本由于过滤不严导致查询语句可控，用户得以访问数据库
     - 有回显
     - 盲注
   - 文件读写：通过数据库进行文件的读写，可以配合起来getshell

   （sql注入可以尝试sqlmap一把梭，前提是你找对了注入点）

其他

https://ctf-wiki.org/web/introduction/

结语

祝你能玩得愉快，学得愉快