SQLMAP工具详解

https://zhuanlan.zhihu.com/p/377428620

sqli-lab题解

详细sqli-labs（1-65）通关讲解-CSDN博客

https://zhuanlan.zhihu.com/p/631613398

• （DEFCON CTF是CTF界最知名影响最广的比赛，历史也相当悠久，已经举办了22届，相当于CTF的“世界杯”）

5.1、CTF赛题复现平台

- **BUUCTF**

1. 拥有大量比赛的复现环境
2. 国内较早使用动态靶机的CTF复现平台·定期举办各类公开赛
3. 提供平台开源环境·较全的比赛Writeup

- **CTFHub**

1. 各类比赛历年真题
2. 较为体系化的技能树
3. 较全的CTF工具集
4. 较全的赛事日历
5. 较全的比赛WriteUp

- **BugKu**

1. 国内较早的CTF复现平台(在buu和ctfhub还没火的时候bugku很有名)·较为基础的题目
2. 较全的WriteUp

- **Pwnable**

1. 适合Pwn新手入门题目较为友好

5.2、赛事与资讯

- **DEF CON CTF**

1. 国际最顶尖的CTF赛事
2. 主赛事+外卡赛
3. 决赛与DEF CON同期举办

- **CTFTime**

1. 较全的国际CTF赛事信息·
2. 较全的CTF战队信息·
3. 较为权威的CTF战队排名。
4. 各大赛事WriteUp
5. 各大赛事日历

- **BUUCTF**

1. 前面说过不重复讲了

- **XCTF国际联赛**

1. 国内较早的CTF联赛
2. 国内第一个出海办比赛的CTF赛事·
3. 在国际上具有一定知名度
4. 部分学校可以加分甚至保研

各类赛事太多了，这里没法一罗列，大家前期可以刷一些校赛和小比赛，进阶刷i春秋、XCTF,后期直接刷CTFTime各类国际赛

5.3、博客与论坛

- 先知社区：https://xz.aliyun.com。
- 看雪论坛：http://bbs.pediy.com/。
- 安全客：http://anquanke.com/.
- FreeBuf http://freebuf.com/。
- P神博客http://leavesongs.com/。
- 代码审计http://t.zsxq.com/UrJiUBY·
- 漏洞百出http://t.zsxq.com/fEmluBe.
- CTFWP@Nu1 http://Lt.zsxq.com/JluJi23

burpsuite

Burp Suite基本介绍
Burp Suite 是用于攻击web 应用程序的集成平台。它包含了许多工具，并为这些工具设计了许多接口，以促进加快攻击应用程序的过程。
所有的工具都共享一个能处理并显示HTTP 消息，持久性，认证，代理，日志，警报的一个强大的可扩展的框架。
Burp Suite是一个集成化的渗透测试工具，它集合了多种渗透测试组件，使我们自动化地或手工地能更

好的完成对web应用的渗透测试和攻击。在渗透测试中，我们使用Burp Suite将使得测试工作变得更加容易和方便，即使在不需要娴熟的技巧的情况下，只有我们熟悉Burp Suite的使用，也使得渗透测试工作变得轻松和高效。
Burp Suite工具箱
burp suite包括以下几个模块

proxy：代理，默认地址是127.0.0.1，端口是8080
target：站点目标，地图
spider：爬虫
scanner：漏洞扫描
repeater：http请求消息与响应消息修改重放
intruder：暴力破解
sequencer：随机数分析
decoder：各种编码格式和散列转换
comparer：可视化差异对比功能

nmap

考点： nmap -oG 写入文件、 -iL读取扫描文件、 escapeshellarg 绕过

我们团队还是偏向于走Web+Misc的路线，这也和我们之后的职业规划比较符合，可以学习一些网络知识

我们还计划实现一个具有SQLMAP的基本功能的工具，所以，现在我们还需要特别深入的了解一下SQL注入的相关原理，其中SQL注入是指...(ppt),当然，既然是开发工具，我们还需要了解一下SQLMAP的功能特点

Sqlmap是开源的自动化SQL注入工具，由Python写成，具有如下特点：

- 完全支持MySQL、Oracle、PostgreSQL、Microsoft SQL Server、Microsoft Access、IBM DB2、SQLite、Firebird、Sybase、SAP MaxDB、HSQLDB和Informix等多种数据库管理系统。
- 完全支持布尔型盲注、时间型盲注、基于错误信息的注入、联合查询注入和堆查询注入。
- 在数据库证书、IP地址、端口和数据库名等条件允许的情况下支持不通过SQL注入点而直接连接数据库。
- 支持枚举用户、密码、哈希、权限、角色、数据库、数据表和列。
- 支持自动识别密码哈希格式并通过字典破解密码哈希。
- 支持完全地下载某个数据库中的某个表，也可以只下载某个表中的某几列，甚至只下载某一列中的部分数据，这完全取决于用户的选择。
- 支持在数据库管理系统中搜索指定的数据库名、表名或列名
- 当数据库管理系统是MySQL、PostgreSQL或Microsoft SQL Server时支持下载或上传文件。
- 当数据库管理系统是MySQL、PostgreSQL或Microsoft SQL Server时支持执行任意命令并回现标准输出。

，当然为了更加了解sql注入的原理，我们还找到了一个SQLILAB靶场，SQLiLab是一个用于学习和测试SQL注入漏洞的实验室环境。它旨在帮助安全研究人员、开发人员和学生理解SQL注入攻击的原理和危害，并学习如何防范这类攻击。SQL注入是一种常见的网络安全漏洞，攻击者可以利用它来访问或修改数据库中的数据，甚至获取系统权限。读ppt