moectf2024 web入门指北

xt

一.web是啥

互联网时代，web应用以及涉及到生活中的方方面面，与后端交互的软件呀，浏览器看到的web网页呀。ctf中web一般涉及web网页安全，通过利用网页前后端的漏洞（代码漏洞也好，服务器漏洞也好）获取关键数据flag，一上来首先需要大家自己搭建一个基本的网站，了解网站的基本架构，连网站是怎么运行的都不知道何谈找漏洞呢。

二.学习方法

不懂就搜（善用ai和搜索引擎，小到软件怎么使用，大到某一个庞大的知识点，可以使用多个搜索引擎，推荐google和www.bing），不懂就问（大雪参必备技能---脸皮厚），推荐blog网站：先知社区，freebuf

三.学习路线

配置环境（最难最烦)：你可以去搜教程看文档，在配置期间你可能会遇到各种各种看不懂得错误，要有耐心，环境需要边学边配置，这里简单列举好用的

1.linux操作系统需要学习（先学会简单使用shell）使用vm虚拟机装个linux发行版吧，用多了相信你会喜欢linux

2.浏览器及其插件（hackbar，ProxySwitchyOmega，Wappalyzer）

3.常用工具（BurpSuite，PHPStudy，Antsword，dirsearch）安装使用想必你会自己搜叭

4.杂七杂八（clash，uTools，Everything）还有一些常用的网站（fofa,cmd5,站长之家）等等

路线指南：

基础知识：（目标搭建自己的第一个网站）

1.基本的网络协议（重点**http**）http的请求头请求体请求方法

2.编码与加解密知识，经典的base64，hash等等，需要一点基本的密码知识

可供参考的资料：https://www.cnblogs.com/ruoli-s/p/14206145.html

3.认证方法（**cookie，session，jwt**）

4.前端三要素（**html**，css，**javascript**）css知道就好，粗体为重点

5.后端（先从最简单的**php**开始）开发简单动态网站（使用phpstudy或者手动安装lamp）

6.数据库（先简单学习**Mysql**）能实现增删改查

7.一个趁手的脚本语言（推荐**python**）能够实现简单爬虫7.学会使用重要的工具，刚开始不用陷入学工具，简单学会使用burpsuite就行

信息搜集：

知道一个网站是什么框架等等

初探漏洞：

web漏洞多到数不清，先从top10学起，以下只给部分介绍，可以从php语言来看这些漏洞是如何产生的，又怎样修补避免呢，攻击时怎么绕过某些阻碍

1.sql注入

就是拼接sql语句实现读取数据库信息（信息泄露），篡改，甚至删除数据库信息，有多种注入方式和利用技巧，注入类的漏洞很多但都大差不差，sql注入算是经典中的经典，学习的时候不要只看不操作，可以找靶场玩玩

推荐靶场：sql-libs

2.php的安全问题

php使用不当会容易出现很多漏洞，==，===使用不当导致php弱类型呀啥的，而且php语言太灵活容易被利用

文件包含，主要由函数include()，require()，include_once()，require_once()造成他们包含的文件会被解析成php代码执行

变量覆盖，关键变量能被用户控制从而导致问题

远程代码执行（**rce**），比如eval()中的代码能够让用户控制（eval($_POST['code']);）

等等种种

3.前端安全（xss, csrf等等）

由前端造成的漏洞

xss：用户通过html注入篡改网页前端，一般插入javascript使得别人访问时自动运行，比如评论区啥的很多很多甚至用户名都行，只要没啥过滤，都可以让浏览器渲染执行，ctf中主要是窃取cookie
推荐靶场：xss-libs

Csrf: 攻击者可以使得受害者发送http的请求（如果受害者的token没过期的话，嘿嘿）

4.服务端请求伪造（ssrf)

用户能使服务器发送http请求，一般我们是向服务器发请求，而ssrf是使得服务器计算机发出http请求

5.文件上传

用户在上传文件功能的地方（头像呀什么的）上传可执行脚本获得shell（php一句话木马），在服务器可以执行有害命令

6.其他

各种语言的反序列化，nodejs原型链污染， ssti，xxe，各种cms，组件漏洞啥的

四.练习

靶场推荐

- 攻防世界（有入门靶场）
- Bugku
- Buuctf
- ctfhub
- Nssctf

不会可以查看wp,一定搞清楚原理,可以学完一个漏洞就找相同类型的靶场打一打（瞎jb乱打不是很建议）

最后建议多看书多看博客社区多了解，祝大家可以在ctf中玩的开心

题目：搭个php网站访问即可获得flag（本地搭一个就行）

附件：
链接：https://pan.baidu.com/s/1Fw0QKHL6uOsolvE8NLtx1Q?pwd=0000
提取码：0000