CTF web安全45天入门学习路线

原创

b1ackc4t 已于 2022-01-26 11:34:09 修改 483 收藏 4
分类专栏： web安全 文章标签： web安全 安全
于 2022-01-23 18:43:02 首次发布

前言

因为最近在准备开发CTF学习平台，先做一个学习路线的整理，顺便也是对想学web的学弟学妹的一些建议。

学习路线

初期

刚刚走进大学，入了web安全的坑，面对诸多漏洞必然是迷茫的，这时的首要任务就是**打好网站开发的基础**，曾有伟人说过-“自己不会做网站，何谈去找网站的漏洞”，在学习漏洞前，了解基本网站架构、基础网站开发原理，基础的前后端知识，能够让你之后的漏洞学习畅通无阻。

html+css+js（2-3天）

前端三要素 html、css、js是被浏览器解析的代码，是构成静态页面的基础。也是前端漏洞如xss、csrf的基础。

重点了解html和js

- 推荐学习资料：
  - https://www.runoob.com/
  - https://www.w3school.com.cn/
- 能力要求：能够写出简单表单，能够通过js获取DOM元素，控制DOM树即可。

apache+php （4-5天）

推荐使用phpstudy来进行傻瓜式安装，可以少走很多弯路。通过apache+php体会一下网站后端的工作，客户端浏览器通过请求apache服务器上的php脚本，php执行后生成的html页面返回给浏览器进行解析。

重点了解php

- 推荐学习资料：
  - https://www.runoob.com/
  - https://www.w3school.com.cn/
- 能力要求：了解基本网站原理，了解php基本语法，开发简单动态页面

mysql （2-3天）

之前已经安装的phpstudy可以轻易的安装mysql。mysql是一款典型的关系型数据库，一般来说，大部分网站都会带有数据库进行数据存储。

重点了解sql语句

- 推荐学习资料：
  - https://www.runoob.com/
  - https://www.w3school.com.cn/
- 能力要求： 能够用sql语句实现增删改查，并且能用php+mysql开发一个增删改查的管理系统（如学生管理系统）

python (2-3天)

虽然 “php是最好的语言”，但它主要还是应用在服务端做网站开发，我们搞安全经常需要写一些脚本或工具来进行诸如密码爆破、目录扫描、攻击自动化等操作，需要一个方便且趁手的编程语言，这里我推荐python

重点学习**requests、BeautifulSoup、re**这三个库

- 推荐学习资料
  - https://www.runoob.com/
  - https://www.w3school.com.cn/
- 能力要求： 了解python基础语法，能够用python爬取网站上的信息（requests+BeautifulSoup+re）

burpsuite （1-2天）

web安全的工具很多，但我觉得必备的渗透工具还得是它

重点学习Proxy、Repeater、Intruder三个模块，分别用于抓包放包、重放包、爆破

初步使用即可，在中期的漏洞学习中去逐渐熟练它

- 推荐学习资料
  - https://www.bilibili.com/video/BV1aq4y1X7oE
  - DVWA之暴力破解
- 能力要求： 能够用burpsuite抓包改包、爆破用户名密码

中期

此时我们对网站已经不再陌生，能够自己动手完成一个简单站点。但我们写出来的代码真的安全吗？进入中期，我们便要开始着眼经典漏洞的学习。

一个漏洞的学习，要搞明白三点（每学完一个漏洞就问自己这三个问题）：

1. 如何利用这个漏洞？
2. 为什么会产生这个漏洞？
3. 如何修复这个漏洞？

SQL注入（7-8天）

我们web狗学习的第一个漏洞一般都是SQL注入，它是web安全经典中的经典，也是在这里被灌输“永远不信任用户的输入”的口号，即使是现在sql注入也依旧存在，并且它还在不断衍生出如nosql注入、ORM注入等，可谓防不胜防。

- 推荐学习资料：
  - sqli-labs 如何使用它网上有很多教学，wp也有很多大佬写了 这里贴一个https://blog.csdn.net/wang_624/article/details/101913584
  - sqlmap sql注入神器，**有余力**可以去看看它的源码，学习一下大佬进行sql注入并把它自动化的思路
  - buuctf 找相关的真题进行练习 wp百度一搜就有
    - [极客大挑战 2019]EasySQL
    - [极客大挑战 2019]LoveSQL
    - [SUCTF 2019]EasySQL
- 能力要求： 能够手工注入出任意表的数据，熟悉三种盲注的手法，能够通过sql注入实现任意文件读取和任意文件写入，能够自己编写一个不含sql注入的查询功能

文件上传（7-8天）

webshell是可以进行代码执行的木马

而文件上传其实就是想办法把webshell上传到目标的服务器上去并成功解析，达到控制目标服务器的目的，这也是web安全的一个重点内容

- 推荐学习资料
  - upload-labs 几乎涵盖所有上传漏洞类型
  - buuctf 找相关的真题进行练习
    - [ACTF2020 新生赛]Upload
  - 趁手的webshell管理工具： 蚁剑
- 能力要求： 会写php的webshell，明白webshell的原理，熟悉常见的文件上传绕过方法（如过后缀检测、过文件头检测、过MIME类型检测），能够自己编写一个不含漏洞的上传功能

其他漏洞（14-15天）

以上两个漏洞是我认为一个初学者最应该掌握也是最典型的漏洞，涵盖了代码执行、文件操作、数据库操作等web应用的主体内容。然而web安全的世界还有很多的漏洞需要你去探索，不过学会了这两种漏洞的你去学其他漏洞定然是游刃有余，不会像刚开始那么困惑了。

以下四个为中期要掌握的漏洞

1. 命令执行（RCE）
    1. php常见的代码执行（eval）、命令执行（system）函数
2. 文件包含
    1. file协议、php伪协议的利用
3. XSS
    1. 通过XSS获取用户cookie
4. CSRF
    1. 通过csrf让用户点击恶意链接就触发敏感操作

后期

此时的你熟悉了web安全几个核心的漏洞，并且有了一些ctf题目的练习经验，已经是一个合格的ctfer了。**恭喜你。成功入门web安全**。后续的学习方法或许该由你自己决定，我在此只给一些建议。

多多参与CTF赛事

参与当下举行的ctf赛事是最好的学习方法之一，即使是初学者也能够找到一些适合自己能力的赛事，比如**极客大挑战、UNCTF、各个大学的新生赛**等等都是不错的选择，在比赛中去发现自己知识的不足，然后去针对的补充这部分知识，是很好的学习循环，**无需迷茫的去到处获取知识，而是在需要时去学习**。

Tips: 或许有人觉得直接刷题是一样的，但完全不是，当下比赛中的题往往更加前沿和流行，你可以找到当下的ctf题目趋势，紧跟技术热点，而且可以多多融入ctf竞技的氛围中，成长的更快。

- ctfhub 可以很方便的查看最近举行的ctf赛事

多多看其他师傅的博客

打完ctf比赛的你肯定是想看writeup（答案）的，一般来说赛后过几天就会有很多师傅发出他的writeup，从**比赛群、百度**等途径都可以找到。多多看看其他师傅的解题思路，关注几个大牛，看看他们发的技术文章，都是很好的学习方法。

总结

web是个大坑，进去容易出去难，入门容易提升难，希望选择web的学弟学妹能够坚持在web安全这条路走下去，不要中途变了心。