Web安全入门指南

基础知识

我觉得学习Web安全至少得大概了解下关于Web的基础知识，比如Web服务器，前后端，HTTP协议等；linux的基础操作；了解一些常见的安全术语，如payload，exp，反弹shell等；还有必须学编程，否则很多漏洞不能理解，不会变通，只能成为脚本小子。另外在研究某个具体漏洞的时候也需要学习相关知识，比如研究SQL注入那肯定需要学习SQl语句以及后端语言对数据库的操作，研究XXE需要学习XML，等等。所以，当你发现某篇文章晦涩难懂的话那多半就是基础知识不够，这时建议凡是遇见不会的点就去搜资料，所有点都清楚之后再看问题就透彻很多。

可能你现在看到上面那一段话就已经云里雾里了😅，完全不明白那些名词是什么。当然我的意思不是必须学完这些所有基础才能进一步学习安全，很多时候都是在研究具体某个安全问题的时候才会临时去学习相关的知识。以下列一些应该学习的内容，当然不必在一开始就全部深入学习，可以大概了解，在以后遇到的时候在再一步深入

HTML和JavaScript

入门不需要太深入学习，能看懂，会简单的代码编写就行（比如写个表单提交），Ajax要学下，css需要了解下
HTML教程 (https://www.runoob.com/html/html-tutorial.html)
JavaScript教程 (https://www.runoob.com/js/js-tutorial.html)
Ajax教程 (https://www.runoob.com/php/php-ajax-intro.html)

HTTP协议

可以在网上搜下相关资料，了解下就行，得知道HTTP的构成和不同的请求方法，极力推荐一本书《图解HTTP》，有空可以看看，漫画风还是挺有意思的
HTTP协议 (https://www.runoob.com/http/http-tutorial.html)

MySQL

要理解SQL注入是必须要学SQL语句和某一门后端语言的，其实本质就是数据变成了指令。
SQL语句 (https://www.runoob.com/sql/sql-syntax.html)
MySQL教程 (https://www.runoob.com/mysql/mysql-tutorial.html)
（会用SQL增删改查就行，高级用法以后在具体题目中慢慢学吧）

PHP

为什么编程语言要把PHP单独提出来，因为PHP是挺方便的，而且简单，也有很多安全问题值得研究，刚开始大概学学便是，基础语法能看懂，能写简单代码，前后端的交互（get，post，cookie，header）,数据库的操作

PHP教程 (https://www.runoob.com/php/php-tutorial.html)
教程中的环境搭建有点麻烦，建议安装PHPstudy(web服务器，mysql都集成了)，具体用法可以网上搜搜
PHPstudey (http://phpstudy.php.cn/download.html)

Linux基础

由于此指南是针对入门Web安全的同学，Linux一开始也不建议用太多时间，能够Linux的日常操作就行，可以去图书馆借本linux的书（越薄越好 😂），最好是自己买台Linux服务器，我比较习惯ubuntu系统（阿里云学生机10元/月感觉不错）。然后自己装个apache，php，mysql，搭建个小网站（别用宝塔一类的自动部署，尽量自己动手）
（参考链接我是随便在网上搜的，要是觉得讲的不够详细就自己再搜搜，不必严格按照该文章做，主要目的就是熟悉linux，会搭建web服务器）
Ubuntu 18.04下使用Apache搭建一个web服务器
(https://blog.csdn.net/weixin_39212776/article/details/81192847)

好了基础就少写点，我怕太多吓走新人 😶

Web安全漏洞

其实一开始学习Web安全就是在学习各种漏洞，调试各种漏洞
下面给的各种漏洞我没办法完完整整提供所有学习资料，得靠各位自己网上搜索了，其实搜索能力也是学安全的必备技能，有些参考链接我也是临时搜的，不能完全保证质量，各位自己甄别了
另外，勤动手，每个paylaod必须亲自调试！！！ 😕/认真脸/
自己测试的时候要懂变通，比如某个地方改下测试还能不能执行，要有发散思维，切莫跟着教程学死技巧，学的不仅是技巧本身，还有思考问题的思维，举个例子，网上常见的后台万能密码 `' or '1'='1` 为什么在某情况下可以是万能密码，原理是什么？可以换成什么形式？ `' or 1='1` 可以吗？ `' or '1` 可以吗？

SQL注入

- 这个怕是在Web安全里提到最多的了
  sql-labs前几题走完整流程，先查information_schema数据库找表名列名,接着查具体数据。后面关卡能绕过防御证明SQL注入存在即可，做够前二三十关就行，然后去综合靶场学骚操作

- 推荐靶场
  sql-labs和下方我推荐的靶场中自己找题

- 一些资料
  sql—labs搭建 (https://www.cnblogs.com/peterpan0707007/p/7501575.html)
  一篇文章带你深入理解 SQL 盲注 (https://www.anquanke.com/post/id/170626?from=timeline)
  绕waf等等技巧可以以后进阶再学，目前入门重点是理解漏洞本身

（如果新人在学习到这里并且是认认真真跟着做时，想必会发现要学SQL注入得先搭环境，需要安装PHPstudy，然后得配置数据库，才可以将靶场跑起来，然后你得会PHP,这样才能看懂代码，才能发掘漏洞，然后得会SQL语句，这样才能利用漏洞，有时候是盲注，手动不大现实，需要自己写脚本，那么python就是不二之选。然后就根据这条链一步步学习便是，后面所有漏洞学习都同理，就不再重复了）

命令执行/代码执行

- 其实这个本质也是把数据作为了指令，学习这个漏洞无非就是学习Linux的命令，一些特性，代码的书写，绕过等。代码执行就先学PHP相关的吧

- 推荐靶场
  DVWA中命令执行部分和下方我推荐的靶场中自己找题，windows上和linux上很多东西是不同的，建议分别在linux和windows搭建环境测试，除了找方法绕过靶场本身的防御外，自己要网上收集绕过方法，测试是否可行

- 一些资料
  《代码审计》-代码执行和命令执行部分总结的
  Web渗透测试中命令执行漏洞详解 (https://www.0dayhack.com/post-834.html)
  命令执行、代码执行漏洞 (https://www.cnblogs.com/drkang/p/8688481.html)
  LD_PRELOAD & putenv() 绕过 disable_functions & open_basedir
  (https://www.cnblogs.com/leixiao-/p/10612798.html)

XSS

- 学这个得先会javascrip，了解下同源策略，CSP（Content Security Policy），然后还是看书吧《xss跨站脚本 攻击剖析与防御》，其中flash XSS部分过时了不必看，还有其中很多paylaod不一定可用，一定要自己测试。
  还有XSS的实际利用，比如怎么盗cookie，这个过程要很清楚且能自己编写paylaod，自己动手，至少完成一次完整攻击（可以拿室友实验😃，别网上随便找个网站就日，违法犯罪的事可不是我教唆的😂）

- 推荐靶场
  下方我推荐的靶场

- 一些资料
  我的CSP绕过思路及总结 (https://xz.aliyun.com/t/5084)
  【干货分享】XSS攻击进阶篇——那些年我们看不懂的XSS (http://blog.nsfocus.net/xss-advance/)

文件上传

- 一开始还是主要学PHP的文件上传漏洞，把upload-labs这个靶场做完，建议是先黑盒测试，做不出来再白盒审代码，再做不出来才看WP。得注意下出现各种安全问题的前提条件哦，面试肯定要被问到😊

还有记不清这靶场有没考过分布式配置文件，自己去了解下.htaccess和.user.ini
很多时候，只有文件上传功能，但并不能绕过上传webshell，所以还要配合文件包含漏洞，这点留给你们先思考下

- 推荐靶场
  upload-labs (https://github.com/c0ny1/upload-labs)
  （接触到github了，不知道这个的同学就可以去了解下什么是github，然后学习下git）

- 一些资料
  Upload-labs通关手册 (https://xz.aliyun.com/t/2435)

文件包含

- 也是先学PHP相关的（所以我在基础知识里提到要学PHP，如果这个漏洞看不懂的话再去好好学学PHP吧）

- 推荐靶场：
  DVWA好像有来着，还有下方我推荐的靶场找题

- 一些资料：
  php文件包含漏洞
  (https://chybeta.github.io/2017/10/08/php%E6%96%87%E4%BB%B6%E5%8C%85%E5%90%AB%E6%BC%8F%E6%B4%9E/)

CSRF

- 现在在框架里也就开启一项配置就可以解决该问题，但是原理思路还是有必要学习的，还得知道CSRF与XSS的关系和区别

- 推荐靶场
  这个不需要靶场吧，就自己搭环境测试，可以学学工具了，burpsuite（有自动生成CSRF功能，当然还有其他很多功能，这个工具最是常用，一定要学）

- 一些资料
  Web安全 — CSRF漏洞 (https://www.freebuf.com/column/155800.html)

XXE

- 这个漏洞多数情况下是可以任意读文件，然后还可造成SSRF，特殊情况下也可执行任意命令，需要先学习下XML，这个建议先在WebGoat靶场（java环境）练习，然后自己动手搭建PHP版本的漏洞环境进行测试，在各种不同配置下测试

- 推荐靶场
  WebGoat XXE部分，自己动手写代码搭建PHP下测试环境

- 一些资料
  一篇文章带你理解漏洞之 XXE 漏洞
  (https://www.k0rz3n.com/2018/11/19/%E4%B8%80%E7%AF%87%E6%96%87%E7%AB%A0%E5%B8%A6%E4%BD%A0%E6%B7%B1%E5%85%A5%E7%90%86%E8%A7%A3%20XXE%20%E6%BC%8F%E6%B4%9E/)
  浅谈XXE漏洞攻击与防御 (https://thief.one/2017/06/20/1/)
  第二届强网杯Web Writeup (https://www.cnblogs.com/iamstudy/articles/2th_qiangwangbei_ctf_writeup.html)
  教育机构那道题

SSRF

- 服务端请求伪造，攻击是发生在后端服务器，注意区分CSRF，要了解gopher协议

- 推荐靶场
  在下方推荐的CTF综合靶场中找找吧,我也记不清哪有了😑
  Vulhub_Weblogic SSRF漏洞 (https://vulhub.org/#/environments/weblogic/ssrf/)

- 一些资料
  猪猪侠 2016 年wooyun 大会议题（自己在网上搜搜吧）
  SSRF漏洞的利用与学习
  (https://uknowsec.cn/posts/notes/SSRF%E6%BC%8F%E6%B4%9E%E7%9A%84%E5%88%A9%E7%94%A8%E4%B8%8E%E5%AD%A6%E4%B9%A0.html)
  【Blackhat】SSRF的新纪元：在编程语言中利用URL解析器
  (https://www.anquanke.com/post/id/86527)
  从一道CTF题目看Gopher攻击MySql (https://www.freebuf.com/articles/web/159342.html)

反序列化

- 每种语言的反序列机制都不同，造成的问题和paylaod构造方式也差异很大，一开还是建议学习PHP反序列化，后面可以学习Python以及Java反序列化安全问题。
  对于PHP反序列化，重点是掌握pop链的构造

- 推荐靶场
  emmm，下面靶场自己找题

- 一些资料
  一篇文章带你深入理解漏洞之 PHP 反序列化漏洞
  (https://www.k0rz3n.com/2018/11/19/%E4%B8%80%E7%AF%87%E6%96%87%E7%AB%A0%E5%B8%A6%E4%BD%A0%E6%B7%B1%E5%85%A5%E7%90%86%E8%A7%A3PHP%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E6%BC%8F%E6%B4%9E/)
  浅谈php反序列化漏洞
  (https://chybeta.github.io/2017/06/17/%E6%B5%85%E8%B0%88php%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E6%BC%8F%E6%B4%9E/)
  PHP反序列化漏洞 (https://www.anquanke.com/post/id/86452)
  一篇文章带你理解漏洞之 Python 反序列化漏洞

(https://www.k0rz3n.com/2018/11/12/%E4%B8%80%E7%AF%87%E6%96%87%E7%AB%A0%E5%B8%A6%E4%BD%A0%E7%90%86%E8%A7%A3%E6%BC%8F%E6%B4%9E%E4%B9%8BPython%20%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E6%BC%8F%E6%B4%9E/)

变量覆盖

- 对于PHP来说，变量覆盖也就是一些函数用法不当造成的问题，先理解漏洞，然后最好自己写代码搭建靶场并测试
- 推荐靶场
  记得bugku中有道白盒审计就是变量覆盖来着
  自己写代码搭建测试
- 一些资料
  代码审计|变量覆盖漏洞 (https://www.freebuf.com/column/150731.html)
  《代码审计》-变量覆盖部分总结

SSTI

- 服务端模板注入
- 推荐靶场
  下面找找吧
- 一些资料
  一篇文章带你理解漏洞之 SSTI 漏洞
  (https://www.k0rz3n.com/2018/11/12/%E4%B8%80%E7%AF%87%E6%96%87%E7%AB%A0%E5%B8%A6%E4%BD%A0%E7%90%86%E8%A7%A3%E6%BC%8F%E6%B4%9E%E4%B9%8BSSTI%E6%BC%8F%E6%B4%9E/)

其他

Web安全方面的漏洞当然不止这些，不过目前就入门来说掌握这些应该差不多了，其他的就希望你们在看文章或是做题中遇见并且学习

推荐的书籍

学习的时候，书也是不可少的，往往书中才有比较系统的知识。有些看不懂的话也很正常，配合网上搜索资料，慢慢消化，多动手！切莫只看不动，以为自己理解了，其实动手实践才能真正学到东西

- 《图解HTTP》
- 《Web前端黑客技术与揭秘》
- 《白帽子讲Web安全》
- 《SQL注入攻击与防御》
- 《黑客攻防技术宝典-Web实战篇》

- 《代码审计:企业级Web代码安全架构》

推荐的靶场

其实我觉得我学习进度最快的时候就是在靶场边刷题边学习的时候，一开始可能无从下手，就可以看看别人写的wp(write up，题解，比如直接搜bugku WP)，跟着wp作者的解题方法学习，然后自己思考，测试自己的想法。在学了某个漏洞原理之后也最好去找相应靶场，相应题目，练习巩固

综合在线CTF靶场

- bugku (https://ctf.bugku.com/)
- JarvisOJ
- 实验吧
- 攻防世界 (https://adworld.xctf.org.cn/)

在线XSS靶场

- alert(1) to win (https://alf.nu/alert1)
- prompt(1) to win (http://prompt.ml)

综合本地靶场

- WebGoat
- DVWA
- bwapp
- Vulhub (https://vulhub.org/#/environments/)

需要学习的工具

我就只列几个Web安全中常用的工具吧

- burpsuit
  可以说这个是最最常用的工具，可以在网上找个破解版，前提是安装java环境，这个就网上搜教程吧。主要是学习Proxy，Decoder，Reperter，Intruder这四个模块的功能
- SQlmap
  学习基本的命令，temper的使用，实战中估计用的多，但我经常是比赛，都得自己写脚本，平常这工具就用的较少。
  工具虽然方便，但一定要掌握手工注入的技巧以及脚本编写的能力
- hackbar
  有些版本不能用，就试着换其他版本就行，其实也就是方便发包调试

- dirsearch
  目录扫描工具

写在后面

终于快写完了，写了几个小时还是挺累的😑
学弟学妹们有什么问题也可以直接来问我，Q1729888211

一些提问

统一写几个你们可能有的疑问

- 我需要严格按照上面的顺序学习吗？
  不用，以上只是入门所需知识的大纲，我想到啥就写了，没啥特定顺序，按照自己的学习计划安排就是，最好在1到3个月扎实掌握以上基础知识

- 学完以上这些我就可以成为厉害的大黑阔吗？
  怕是不行，毕竟我自己都还很菜，安全领域涉及的东西很多很多，不过学完以上也算黑客入门了吧，简单渗透几个网站，打打CTF还是没问题。

- 有些文章看不懂怎么办？
  如果在文章中遇见不会的名词，建议暂停当前文章的阅读，先去把不懂的地方弄懂，如果硬着头皮读下去，遇见不会就跳过的话，读完最后就会发现自己确实什么都没弄懂。如果有些确实读不懂，那说明水平确实还不够，暂时放一边吧，切莫好高骛远，从基础一步步走好。

- 感觉学了很久技术不见进步怎么办？
  你得努力学，如果每天只是看几十分钟文章，做几十分钟题，然后其他时间就打游戏刷剧去了，我觉得这样你看的见进步才怪了。当然在掌握正确学习方法条件下也可能出现学了很久，技术没有明显进步，所谓量变产生质变。继续加油吧少年。

一些建议

- 有舍有得
  既然选择了成为一名正义的白帽子，那么有些东西是得舍去的，比如每天要少打游戏，少玩手机，少看剧，花大量时间在学习技术上，选择这条路请坚持走下去，不忘，方得。

- 纸上得终浅，欲知需躬行
  不能光看，一定要动手，一定要动手！！！

- 勤做笔记，利于巩固知识和以后查阅，还有就是自己多总结

- 实在遇见不懂的问题而百度谷歌又查不到的时候就多问，学长学姐其实都比较乐意回答问题的，不过要注意下提问的技巧，比如一个问题你是哪里不理解，做过何种尝试，结果怎么样