# WEB DOC



# CTF和web

- 什么是CTF?
- CTF的详细介绍
- CTF中的web安全?

# 关于X1cT34m

- 我们是一个什么神秘的组织？
  - A student group of hackers
- 我们在做什么？

- 共同学习Web安全
- Hack for fun

# 加入我们

---

- WEB方向需要的是乐于**分享分享分享交流交流交流**技术的、能独立思考并解决技术难题的、能**主动主动主动**分担团队责任的小伙伴。
- 大一、大二的小伙伴们，如果你觉得自己已经有了足够的实力，我们随时欢迎你的加入申请，同时WEB方向会在且仅在每年3-4月份进行一次**正式**的招新考核，考核对于每个人都是公平的。

# 阅读入门DOC前，以下内容你必须知道

---

1. 明确自己打CTF是为了娱乐，还是为了以后的工作发展
2. 如果是为了工作，那么需要一颗非常有毅力的心
3. 做好放弃周末休息时间的准备
4. 你的**绝大多数**学习资料会来源于搜索引擎（百度，Google），也就是自学

# 入门DOC

---

## 你需要掌握的技能(编程、人际交流、思维模式、学习能力、学习方法等等方面)

- 入门DOC的正确使用方法：
    a. WEB组的小伙伴们提供了方向，提供了关键词，你们恰巧可以利用**搜索引擎**来查找相关内容，自主学习
    b. 但凡是各大CTF平台已经有的题目，用搜索引擎都能搜到“【题目名称】-wp”
    c. 初期遇见的东西**绝大多数**都是**没听说过**的，只有不停的**搜索**，不停的**学习**，有智慧和礼貌的**提问**才能成长
- 你需要学习语言的顺序：PHP->Python->Java

## 你应该充分利用起来的资源

- 【学习】Github
- 【靶场】BUUOJ
- 【靶场】南邮0xCTF
- 【靶场】南邮CGCTF(可能访问不了，但是题目适合入门)
- 【靶场】CTF.show萌新计划
- 【靶场】CTFhub技能树
- 【靶场】BugKuCTF

- 【靶场】攻防世界
- 【学习】CTF-Wiki-Web
- 【学习】dalao们的博客，这里推荐几个wp详细或者干货比较多的：k0rz3n ,smi1e,sky,y1ng,p牛
- 【学习】各大技术分享平台：先知社区，freebuf，安全客
- 【学习】一些入门可以看的web安全相关书籍
    a. 《白帽子讲web安全》：可以通过这本书建立对WEB安全基本的整体概念（阅读需一定基础）
    b. 《web安全攻防渗透测试安全指南》：干货较多（与第一本相比，侧重点为攻击手法），可以拿来填充自己的知识储备库
    c. 《web安全深度剖析》：张炳帅著，各种漏洞都有介绍，个人感觉更适合新手
    d. 《内网安全攻防渗透测试安全指南》：内网渗透从入门到起飞，是《web安全攻防渗透测试安全指南》的姊妹篇（推荐后期购买）

## 你该从哪些基础漏洞开始

- 首先，搭建一个本地网站，推荐使用phpstudy
  ps：不一定都要自己本地搭建环境，一般是刷CTF题目的时候遇见了就去学，边打边学，以赛代练
- 入门漏洞环境DVWA

## sql-injection

- sql注入靶场
- sqliabs-wp
- PayloadsAllthetThings
- MySQL注入常见姿势总结（讲的比较全）

## 文件上传

- 文件上传漏洞靶场
- uploadlabs-wp
- 文件上传漏洞小结

## XSS

- xss-labs
- xsslabs-wp
- 那些年我们一起学xss
- prompt 1 to win

## SSRF

- ssrf学习记录

## PHP相关漏洞

php是世界上最好（la ji）的语言，漏洞层出不穷，作为一名安全人员，熟练掌握PHP基本语法和相关漏洞是必要的，以下漏洞都需要PHP基础

- PHP基础学习：B站
- 弱类型语言漏洞
- 变量覆盖漏洞
- 文件包含漏洞
- 反序列化漏洞
- RCE漏洞
- ……

## Python相关漏洞

- flask之ssti模版注入从零到入门
- flask SSTI常见绕过姿势
- pickle反序列化初探
- Python pickle 反序列化实例分析
- ……

## XXE

- 一篇文章带你深入理解漏洞之XXE漏洞
- xxe-lab

## Java相关漏洞

- Java反序列化漏洞从入门到深入
- Java反序列化漏洞原理解析

## Javascript相关漏洞

- Node.js 常见漏洞学习与总结
- Nodejs安全从入门到入土

……

# 你将会用到的工具

## 虚拟机

- vm中安装kali的教程VMware是比较常用的虚拟机软件，安装kali的过程中会有关于vm的配置问题，这里挂的是vm15的kali教程
- kali首先大部分所需要的工具Kali已经是集成好了的。不建议过度依赖工具，但是可以按需求使用。同时kali也是你熟悉Linux操作,或者简单渗透的一个大好机会

## 抓包工具

- BurpSuit使用手册（bp到52pojie.cn找）

## 网站目录扫描工具

- dirsearch
- 御剑 自己找吧（我也不知道在哪下的😄）
- ctfwscan-为ctf而生的扫描器

## 网站后门管理工具

- AntSword
- Behinder

## SQL注入工具

- 尽量不要使用工具，手注更灵活、高效
- Sqlmap
- 当然到了后面都是需要自己用python根据实际情况编写注入脚本

## XSS接收面板（可以自己搭）

- BlueLotus_XSSReceiver
- XSS小结

## 服务器管理相关工具

选择自己喜欢的：

- Termius真的超好用。用github学生包直接免费领取。
- Xshell
- putty
- Xftp
- FileZilla

## 你该如何判断自己已经度过了萌新阶段

1. 攻防世界高手区第一页
2. 0xCTF刷到600分
3. ……

## 后续

1. 跟着队伍多打比赛，保持活跃度
2. 刷XCTF分站赛，看CTF WEB热点、趋势
3. 多关注博客
4. 准备校赛

- 往届校赛NCTF2018
- 往届校赛NCTF2019的web题目
    - BUUOJ上面已有四道，Github也有源码
    - easyphp
    - flask_website
    - backdoor
- 0xGame新生赛(预计2020.10月)
- NCTF2020(预计2020.11月下旬)

## 联系方式

- 2020南邮CTF招新群 QQ1147289478
- 钟敏睿 QQ1643239341
- 陈励勤 QQ912309920
- 柯劳芸 QQ598743446
- 万力桐 QQ1367114100
- 滕育林 QQ1010433224
- 童程 QQ2448552437
- 桑行立 QQ1803700972