

Web安全工程师

想成为Web安全工程师？不知道该如何入门？不要着急，本计划分五个阶段，包含最基本的Web漏洞检测、理论基础、原理分析及安全防护，帮助你成为优秀的Web安全工程师！

195节课程

43小时

519086已学

* 概念基础
* 技术基础
* 入侵防范
* Web安全漏洞分析与防御
* 渗透实战
* 安全开发

已学完学习中未学习即将上线

概念基础

几堂课快速了解白帽黑客的工作范畴、方式及法律约束，一起带上一顶白帽，仗剑走天涯！

|  |  |  |
| --- | --- | --- |
| **黑客是如何工作的？** |  |  |
| [1.  如何在虚拟机中配置Linux操作系统](http://www.ichunqiu.com/career/105/50979) | [2.  你必须要知道的漏洞测试工具](http://www.ichunqiu.com/career/105/50981) | [3.  带你感受MSF控制台的力量](http://www.ichunqiu.com/career/105/50983) |
| [4.  初次使用MSF应该注意哪些？](http://www.ichunqiu.com/career/105/50985) | [5.  远程管理工具-RATS](http://www.ichunqiu.com/career/105/50987) | [6.  如何在虚拟机中正常运行](http://www.ichunqiu.com/career/105/50989) |
| [7.  远程访问计算机，就这么简单！](http://www.ichunqiu.com/career/105/50991) |  |  |
| **白帽黑客的法律约束** |  |  |
| [1.  白帽子法律行为及相关的法律规定](http://www.ichunqiu.com/career/105/50967) | [2.  白帽子法律咨询与答疑](http://www.ichunqiu.com/career/105/51081) | [3.  白帽子如何通过法律保护自己](http://www.ichunqiu.com/career/105/51085) |
| **网络安全概念基础** |  |  |
| [1.  白帽黑客一直在重复做的事情](http://www.ichunqiu.com/career/105/50659) | [2.  场景环境设置的重要性及必要性](http://www.ichunqiu.com/career/105/50657) | [3.  白帽黑客特定的原则和底线](http://www.ichunqiu.com/career/105/50665) |
| [4.  白帽黑客的优势](http://www.ichunqiu.com/career/105/50663) | [5.  白帽黑客软件、硬件配置建议](http://www.ichunqiu.com/career/105/50661) | [6.  密码学概念简单介绍](http://www.ichunqiu.com/career/105/50667) |
| [7.  什么是密码破解](http://www.ichunqiu.com/career/105/51547) | [8.  攻击概述](http://www.ichunqiu.com/career/105/51475) | [9.  什么是病毒](http://www.ichunqiu.com/career/105/51557) |
| [10.  什么是后门程序](http://www.ichunqiu.com/career/105/51555) | [11.  什么是拒绝服务攻击](http://www.ichunqiu.com/career/105/51799) | [12.  什么是网络嗅探](http://www.ichunqiu.com/career/105/51797) |
| [13.  什么是会话劫持](http://www.ichunqiu.com/career/105/51563) | [14.  白帽黑客的密码加密学](http://www.ichunqiu.com/career/105/51087) | [15.  什么是物理安全](http://www.ichunqiu.com/career/105/52613) |

技术基础

学会几招简单的安全工具，初步体会安全问题，高手都是从简单一点点积累得来的！

|  |  |  |
| --- | --- | --- |
| **漏洞扫描工具：AWVS** |  |  |
| [1.  AWVS：简介](http://www.ichunqiu.com/career/105/50759) | [2.  AWVS：安装](http://www.ichunqiu.com/career/105/50761) | [3.  AWVS：站点扫描](http://www.ichunqiu.com/career/105/50763) |
| [4.  AWVS：扫描结果分析](http://www.ichunqiu.com/career/105/50765) | [5.  AWVS：Site Crawler& HTTP Editor](http://www.ichunqiu.com/career/105/50767) | [6.  AWVS：Target Finder & Subdomain Scanner](http://www.ichunqiu.com/career/105/50769) |
| [7.  AWVS：Authentication Tester](http://www.ichunqiu.com/career/105/50771) | [8.  AWVS：HTTP Sniffer](http://www.ichunqiu.com/career/105/50773) | [9.  AWVS：HTTP Fuzzer](http://www.ichunqiu.com/career/105/50775) |
| **网络安全审计工具：Nmap** |  |  |
| [1.  安装与初次使用](http://www.ichunqiu.com/career/105/1223) | [2.  扫描多个目标](http://www.ichunqiu.com/career/105/1225) | [3.  扫描网络并排除特定的目标](http://www.ichunqiu.com/career/105/1227) |
| [4.  扫描开放网络端口](http://www.ichunqiu.com/career/105/1229) | [5.  使用可选包扫描网络 第一部分](http://www.ichunqiu.com/career/105/1231) | [6.  使用可选包扫描网络 第二部分](http://www.ichunqiu.com/career/105/1233) |
| [7.  先进的扫描技术](http://www.ichunqiu.com/career/105/1235) | [8.  端口扫描选项](http://www.ichunqiu.com/career/105/1237) | [9.  系统检测](http://www.ichunqiu.com/career/105/1239) |
| [10.  时间选项 Part1](http://www.ichunqiu.com/career/105/1241) | [11.  时间选项 Part2](http://www.ichunqiu.com/career/105/1243) | [12.  和防火墙的乐趣！](http://www.ichunqiu.com/career/105/1245) |
| [13.  如何输出文件](http://www.ichunqiu.com/career/105/1247) | [14.  如何使用排错选项](http://www.ichunqiu.com/career/105/1249) | [15.  Nmap的脚本引擎](http://www.ichunqiu.com/career/105/1251) |
| [16.  Zenmap的内部结构](http://www.ichunqiu.com/career/105/1253) | [17.  如何解读Zenmap的输出信息](http://www.ichunqiu.com/career/105/1255) | [18.  NDiff 和技巧！](http://www.ichunqiu.com/career/105/1257) |
| **Web安全基础入门** |  |  |
| [1.  什么是ASP木马](http://www.ichunqiu.com/career/105/483) | [2.  数据库的安全风险](http://www.ichunqiu.com/career/105/485) | [3.  网站配置的安全风险](http://www.ichunqiu.com/career/105/487) |
| [4.  PHP安全初探：什么是PHP木马](http://www.ichunqiu.com/career/105/895) | [5.  PHP安全初探：简述PHP常见漏洞](http://www.ichunqiu.com/career/105/897) | [6.  PHP安全初探：APACHE解析漏洞](http://www.ichunqiu.com/career/105/899) |

入侵防范

学会“防范 - 检测 - 溯源 - 验证”的全方位防御规范，让你的系统时刻保持高警戒。

|  |  |  |
| --- | --- | --- |
| **社工情报侦察神器：Maltego** |  |  |
| [1.  什么是Maltego](http://www.ichunqiu.com/career/105/905) | [2.  添加链接与选择](http://www.ichunqiu.com/career/105/907) | [3.  管理Mangage选项卡](http://www.ichunqiu.com/career/105/909) |
| [4.  视图选项](http://www.ichunqiu.com/career/105/911) | [5.  增加实体（entities）](http://www.ichunqiu.com/career/105/913) | [6.  基本图形界面介绍](http://www.ichunqiu.com/career/105/915) |
| **社会工程学工具：SET** |  |  |
| [1.  Social-Engineer Toolkit的更新和网站的克隆](http://www.ichunqiu.com/career/105/50861) | [2.  Social-Engineer Toolkit的社交攻击](http://www.ichunqiu.com/career/105/50863) | [3.  Social-Engineer Toolkit的端口转发](http://www.ichunqiu.com/career/105/50865) |
| [4.  Social-Engineer Toolkit的DNS欺骗](http://www.ichunqiu.com/career/105/50867) |  |  |
| **入侵痕迹追踪溯源** |  |  |
| [1.  基于入侵检测的告警分析-外网](http://www.ichunqiu.com/career/105/338) | [2.  基于入侵检测的告警分析-内网](http://www.ichunqiu.com/career/105/339) |  |

Web安全漏洞分析与防御

不能只知道如何防范，同时还得知道各种漏洞是如何发生的！从原理上的理解才是真正的明白。

|  |  |  |
| --- | --- | --- |
| **弱口令** |  |  |
| [1.  默认型弱口令](http://www.ichunqiu.com/career/105/50385) | [2.  社工型弱口令](http://www.ichunqiu.com/career/105/50387) | [3.  弱口令之weblogic弱口令](http://www.ichunqiu.com/career/105/50393) |
| [4.  验证码安全](http://www.ichunqiu.com/career/105/50395) | [5.  如何防止弱口令](http://www.ichunqiu.com/career/105/50971) |  |
| **SQL注入** |  |  |
| [1.  您也可以做专家—“啊D”注入测试工具](http://www.ichunqiu.com/career/105/39) | [2.  您也可以做专家—“SQLmap”网站注入测试工具](http://www.ichunqiu.com/career/105/40) | [3.  做好防御还被黑?—绕过防注入脚本的“Tamper”工具](http://www.ichunqiu.com/career/105/38) |
| [4.  专家教您利用安全狗防御SQL注入](http://www.ichunqiu.com/career/105/101) |  |  |
| **非法上传** |  |  |
| [1.  再现杰奇网站漏洞环境](http://www.ichunqiu.com/career/105/43) | [2.  警惕您站上的MIME类型绕过漏洞](http://www.ichunqiu.com/career/105/44) | [3.  警惕您站上的文件扩展名绕过漏洞](http://www.ichunqiu.com/career/105/45) |
| [4.  警惕您站上的文件内容检测绕过类上传漏洞](http://www.ichunqiu.com/career/105/46) | [5.  警惕您站上的空字节截断目录路径检测绕过类上传漏洞](http://www.ichunqiu.com/career/105/47) | [6.  警惕IIS6.0站上的目录路径检测解析绕过上传漏洞](http://www.ichunqiu.com/career/105/48) |
| [7.  警惕IIS6.0站上的解析缺陷绕过上传漏洞](http://www.ichunqiu.com/career/105/49) | [8.  警惕Apache站上的解析缺陷绕过上传漏洞](http://www.ichunqiu.com/career/105/50) | [9.  警惕您站上的htaccess文件上传解析漏洞](http://www.ichunqiu.com/career/105/51) |
| [10.  通过案例学安全—“FCK编辑器”版本识别及信息收集技术演示](http://www.ichunqiu.com/career/105/52) | [11.  警惕您站上的“FCK编辑器”解析漏洞突破检测上传后门漏洞](http://www.ichunqiu.com/career/105/53) |  |
| **跨站脚本XSS** |  |  |
| [1.  认识XSS](http://www.ichunqiu.com/career/105/50115) | [2.  XSS的分类](http://www.ichunqiu.com/career/105/50117) | [3.  XSS的构造剖析上](http://www.ichunqiu.com/career/105/50119) |
| [4.  XSS的构造剖析中](http://www.ichunqiu.com/career/105/50121) | [5.  XSS的构造剖析下](http://www.ichunqiu.com/career/105/50123) | [6.  Shellcode的调用](http://www.ichunqiu.com/career/105/50125) |
| [7.  XSS测试和工具剖析](http://www.ichunqiu.com/career/105/50127) |  |  |
| **Web漏洞分析技术** |  |  |
| [1.  Discuz 全版本存储型 DOM XSS](http://www.ichunqiu.com/career/105/330) | [2.  TurboMail 存储型XSS漏洞](http://www.ichunqiu.com/career/105/449) | [3.  DedeCMS 5.7 反射型XSS漏洞](http://www.ichunqiu.com/career/105/447) |
| [4.  PHPCMS2008 SQL注入漏洞](http://www.ichunqiu.com/career/105/405) | [5.  BlueCMS 1.6 SQL 注入漏洞](http://www.ichunqiu.com/career/105/406) | [6.  D-link 路由器 CSRF漏洞](http://www.ichunqiu.com/career/105/440) |
| [7.  Bash 4.3 远程命令执行漏洞](http://www.ichunqiu.com/career/105/432) | [8.  PHPYun XML 注入漏洞](http://www.ichunqiu.com/career/105/430) | [9.  WeBid 1.1.1 文件上传漏洞](http://www.ichunqiu.com/career/105/437) |
| [10.  KPPW 2.2 任意文件下载漏洞](http://www.ichunqiu.com/career/105/436) | [11.  PHPCMS 2008 命令执行漏洞](http://www.ichunqiu.com/career/105/433) | [12.  CmsEasy 5.5 代码执行漏洞](http://www.ichunqiu.com/career/105/434) |
| [13.  AKCMS 6.0 登录绕过漏洞](http://www.ichunqiu.com/career/105/438) | [14.  AspCms 2.2.9 登录绕过漏洞](http://www.ichunqiu.com/career/105/439) | [15.  DedeCMS 5.7 远程文件包含漏洞](http://www.ichunqiu.com/career/105/51575) |

渗透实战

“工欲善其事,必先利其器”，掌握更强大的安全工具，才能更好地帮助我们进行渗透。

|  |  |  |
| --- | --- | --- |
| **Kali渗透测试教程** |  |  |
| [1.  虚拟机介绍及Kali系统的安装](http://www.ichunqiu.com/career/105/1357) | [2.  虚拟机配置及Kali系统配置](http://www.ichunqiu.com/career/105/1359) | [3.  Windows过渡到基本的Linux操作](http://www.ichunqiu.com/career/105/1361) |
| [4.  玩转Windows美化（不是更换主题）](http://www.ichunqiu.com/career/105/1363) | [5.  局域网断网攻击](http://www.ichunqiu.com/career/105/1365) | [6.  实战-获取内网妹子的QQ相册](http://www.ichunqiu.com/career/105/1367) |
| [7.  综合应用之HTTP账号密码获取](http://www.ichunqiu.com/career/105/1369) | [8.  综合应用之HTTPS账号密码获取](http://www.ichunqiu.com/career/105/1371) | [9.  会话劫持-登录别人的百度贴吧](http://www.ichunqiu.com/career/105/1373) |
| [10.  会话劫持-一键劫持会话](http://www.ichunqiu.com/career/105/1375) | [11.  SQLMAP介绍及ASP网站渗透](http://www.ichunqiu.com/career/105/1377) | [12.  SQLMAP介绍之PHP网站渗透](http://www.ichunqiu.com/career/105/1379) |
| [13.  SQLMAP介绍之Cookie注入](http://www.ichunqiu.com/career/105/1381) | [14.  Metasploit新手知识补全](http://www.ichunqiu.com/career/105/1383) | [15.  Metasploit之我的远程控制软件](http://www.ichunqiu.com/career/105/1385) |
| [16.  Metasloit之木马文件操作功能](http://www.ichunqiu.com/career/105/1387) | [17.  Metasploit之木马的系统操作功能](http://www.ichunqiu.com/career/105/1389) | [18.  Metasploit之木马的用户操作及摄像头操作](http://www.ichunqiu.com/career/105/1391) |
| [19.  Metasploit之渗透安卓实战](http://www.ichunqiu.com/career/105/1393) | [20.  Metasploit之服务器蓝屏攻击](http://www.ichunqiu.com/career/105/1395) | [21.  Metasploit之生成webshell及应用](http://www.ichunqiu.com/career/105/1397) |
| [22.  自己的学习方法&新年贺岁](http://www.ichunqiu.com/career/105/1399) |  |  |
| **漏洞检测工具：Metasploit** |  |  |
| [1.  Metasploit框架介绍](http://www.ichunqiu.com/career/105/1595) | [2.  Metasploit升级更新](http://www.ichunqiu.com/career/105/1597) | [3.  Metasploit端口扫描](http://www.ichunqiu.com/career/105/1599) |
| [4.  Metasploit SMB 获取系统信息](http://www.ichunqiu.com/career/105/1601) | [5.  Metasploit 服务识别](http://www.ichunqiu.com/career/105/1603) | [6.  Metasploit 密码嗅探](http://www.ichunqiu.com/career/105/1605) |
| [7.  Metasploit SNMP 扫描](http://www.ichunqiu.com/career/105/1607) | [8.  Metasploit SMB登陆验证](http://www.ichunqiu.com/career/105/1609) | [9.  Metasploit VNC身份识别](http://www.ichunqiu.com/career/105/1611) |
| [10.  Metasploit WMAP Web扫描](http://www.ichunqiu.com/career/105/1613) | [11.  Metasploit之远程代码执行](http://www.ichunqiu.com/career/105/50209) | [12.  Metasploit之MIDI文件解析远程代码执行](http://www.ichunqiu.com/career/105/50211) |
| [13.  Metasploit之口令安全](http://www.ichunqiu.com/career/105/50213) | [14.  Metasploit之Hash值传递渗透](http://www.ichunqiu.com/career/105/50215) | [15.  Metasploit之NDProxy内核提权](http://www.ichunqiu.com/career/105/50217) |
| [16.  Metasploit之多种后门生成](http://www.ichunqiu.com/career/105/50219) | [17.  Metasploit之内网渗透](http://www.ichunqiu.com/career/105/50221) | [18.  Metasploit之反反病毒](http://www.ichunqiu.com/career/105/50223) |
| [19.  Metasploit之玩转不一样的XSS](http://www.ichunqiu.com/career/105/50225) | [20.  Metasploit之维持访问](http://www.ichunqiu.com/career/105/50227) |  |
| **集成平台：Burpsuite** |  |  |
| [1.  burpsuite应用场景](http://www.ichunqiu.com/career/105/51245) | [2.  burpsuite安装和简介](http://www.ichunqiu.com/career/105/51247) | [3.  Proxy代理模块详解](http://www.ichunqiu.com/career/105/51251) |
| [4.  burpsuite代理监听设置](http://www.ichunqiu.com/career/105/51253) | [5.  burpsuite代理的其他设置](http://www.ichunqiu.com/career/105/51261) | [6.  burpsuite重放](http://www.ichunqiu.com/career/105/51263) |
| [7.  burpsuite攻击](http://www.ichunqiu.com/career/105/51265) | [8.  burpsuite攻击类型选择](http://www.ichunqiu.com/career/105/51269) | [9.  burpsuite攻击payload](http://www.ichunqiu.com/career/105/51271) |
| [10.  burpsuite攻击设置](http://www.ichunqiu.com/career/105/51275) | [11.  burpsuite扫描模块](http://www.ichunqiu.com/career/105/51277) | [12.  burpsuite设置1](http://www.ichunqiu.com/career/105/51281) |
| [13.  burpsuite设置2](http://www.ichunqiu.com/career/105/51285) | [14.  burpsuite其他模块介绍](http://www.ichunqiu.com/career/105/51287) |  |
| **渗透工具：SQLMap** |  |  |
| [1.  sqlmap安装和介绍](http://www.ichunqiu.com/career/105/50781) | [2.  access数据库注入](http://www.ichunqiu.com/career/105/50783) | [3.  MySql数据库注入（上）](http://www.ichunqiu.com/career/105/50785) |
| [4.  MsSql数据库注入（下）](http://www.ichunqiu.com/career/105/50787) | [5.  cookie中转注入](http://www.ichunqiu.com/career/105/50789) | [6.  利用google批量搜索注入](http://www.ichunqiu.com/career/105/50791) |
| [7.  tamper插件使用](http://www.ichunqiu.com/career/105/50793) | [8.  file参数使用](http://www.ichunqiu.com/career/105/50795) | [9.  post提交方式注入](http://www.ichunqiu.com/career/105/50797) |
| [10.  os参数注入讲解](http://www.ichunqiu.com/career/105/50799) |  |  |

安全开发

有良好的开发流程规划和代码开发意识，对开发出安全的应用程序来说绝对是至关重要的！

|  |  |  |
| --- | --- | --- |
| **安全开发设计** |  |  |
| [1.  Java安全开发规范](http://www.ichunqiu.com/career/105/50709) | [2.  安全开发流程](http://www.ichunqiu.com/career/105/50715) | [3.  源代码缺陷审计（上）](http://www.ichunqiu.com/career/105/50719) |
| [4.  源代码缺陷审计（下）](http://www.ichunqiu.com/career/105/52677) | [5.  C/C++安全开发规范（上）](http://www.ichunqiu.com/career/105/50723) |  |
| **PHP代码审计** |  |  |
| [1.  环境搭建](http://www.ichunqiu.com/career/105/1421) | [2.  SQL注入基础](http://www.ichunqiu.com/career/105/1325) | 3.  常用函数问题,header注入,二次注入 |
| 4.  反射型XSS,存储型XSS,DOM型XSS,flash型XSS | 5.  从防御代码中看xss | 6.  本地文件包含，远程文件包含 |
| 7.  GET与POST,Flash CSRF | 8.  通过黑白测试挖掘CSRF+防御手段 | 9.  命令执行(system、exec、shell\_exec)等解释及如何挖掘 |
| 10.  常见的上传防御(黑名单，白名单，文件头部等)及绕过技术 | 11.  thinksaas找回密码 | 12.  Hdwiki 修改密码 |