职位描述：

1. 对公司网站、业务系统进行安全评估测试（黑盒、白盒测试）；
2. 对公司各类系统进行安全加固；
3. 对公司安全事件进行响应，清理后门，根据日志分析攻击途径；
4. 安全技术研究，包括安全防范技术，黑客技术等；
5. 跟踪最新漏洞信息，进行业务产品的安全检查。

职位要求：

1. 熟悉主流的 Web 安全技术，包括 SQL 注入、XSS、CSRF、一句话木马等安全风险；
2. 熟悉国内外主流安全产品和工具，如：Nessus、Nmap、AWVS、Burp、Appscan 等；
3. 熟悉 windows、linux 平台渗透测试、后门分析、加固；
4. 至少掌握一门编程语言 C/C++/Perl/Python/PHP/Go/Java 等；
5. 熟悉渗透测试的步骤、方法、流程，具有 Web 安全实战经验；
6. 熟悉常见安全攻防技术，对网络安全、系统安全、应用安全有深入的理解和自己的认识；
7. 对 Web 安全整体有深刻理解，具备代码审计和独立漏洞挖掘能力；
8. 具有较强的团队意识，高度的责任感，文档、方案能力优秀者优先。

学习路线：

- 2 周

Web 安全相关概念
熟悉基本概念（SQL 注入、上传、XSS、CSRF、一句话木马等）。

1. 通过关键字（SQL 注入、上传、XSS、CSRF、一句话木马等）进行 Google/SecWiki；
2. 阅读《精通脚本黑客》，虽然很旧也有错误，但是入门还是可以的；
3. 看一些渗透笔记/视频，了解渗透实战的整个过程，可以 Google（渗透笔记、渗透过程、入侵过程等）；

- 3 周

熟悉渗透相关工具
熟悉 AWVS、sqlmap、Burp、nessus、chopper、nmap、Appscan 等相关工具的使用。

1. 了解该类工具的用途和使用场景，先用软件名字 Google/SecWiki；
2. 下载无后门版的这些软件进行安装；
3. 学习并进行使用，具体教材可以在 SecWiki 上搜索，例如：Brup 的教程、sqlmap；
4. 待常用的这几个软件都学会了可以安装音速启动做一个渗透工具箱；

- 5 周

渗透实战操作
掌握渗透的整个阶段并能够独立渗透小型站点。

1. 网上找渗透视频看并思考其中的思路和原理，关键字（渗透、SQL 注入视频、文件上传入侵、数据库备份、dedecms 漏洞利用等等）；
2. 自己找站点/搭建测试环境进行测试，记住请隐藏好你自己；
3. 思考渗透主要分为几个阶段，每个阶段需要做那些工作，例如这个：PTES 渗透测试执行标准；
4. 研究 SQL 注入的种类、注入原理、手动注入技巧；
5. 研究文件上传的原理，如何进行截断、双重后缀欺骗(IIS、PHP)、解析漏洞利用（IIS、Nignix、Apache）等，参照：上传攻击框架；
6. 研究 XSS 形成的原理和种类，具体学习方法可以 Google/SecWiki，可以参考：XSS；
7. 研究 Windows/Linux 提权的方法和具体使用，可以参考：提权；
8. 可以参考: 开源渗透测试脆弱系统；

- 1 周

关注安全圈动态
关注安全圈的最新漏洞、安全事件与技术文章。

1. 通过 SecWiki 浏览每日的安全技术文章/事件；
2. 通过 Weibo/twitter 关注安全圈的从业人员（遇到大牛的关注或者好友果断关注），天天抽时间刷一下；
3. 通过 feedly/鲜果订阅国内外安全技术博客（不要仅限于国内，平时多注意积累），没有订阅源的可以看一下 SecWiki 的聚合栏目；
4. 养成习惯，每天主动提交安全技术文章链接到 SecWiki 进行积淀；
5. 多关注下最新漏洞列表，推荐几个：exploit-db、CVE 中文库、Wooyun 等，遇到公开的漏洞都去实践下。

6. 关注国内国际上的安全会议的议题或者录像，推荐 SecWiki-Conference。

- 3 周

熟悉 Windows/Kali Linux
学习 Windows/Kali Linux 基本命令、常用工具；

1. 熟悉 Windows 下的常用的 cmd 命令，例如：ipconfig,nslookup,tracert,net,tasklist,taskkill 等；
2. 熟悉 Linux 下的常用命令，例如：ifconfig,ls,cp,mv,vi,wget,service,sudo 等；
3. 熟悉 Kali Linux 系统下的常用工具，可以参考 SecWiki,《Web Penetration Testing with Kali Linux》、《Hacking with Kali》等；
4. 熟悉 metasploit 工具，可以参考 SecWiki、《Metasploit 渗透测试指南》。

- 3 周

服务器安全配置
学习服务器环境配置，并能通过思考发现配置存在的安全问题。

1. Windows2003/2008 环境下的 IIS 配置，特别注意配置安全和运行权限，可以参考：SecWiki-配置；
2. Linux 环境下的 LAMP 的安全配置，主要考虑运行权限、跨目录、文件夹权限等，可以参考：SecWiki-配置；
3. 远程系统加固，限制用户名和口令登陆，通过 iptables 限制端口；
4. 配置软件 Waf 加强系统安全，在服务器配置 mod_security 等系统，参见 SecWiki-ModSecurity；
5. 通过 Nessus 软件对配置环境进行安全检测，发现未知安全威胁。

- 4 周

脚本编程学习
选择脚本语言 Perl/Python/PHP/Go/Java 中的一种，对常用库进行编程学习。

1. 搭建开发环境和选择 IDE，PHP 环境推荐 Wamp 和 XAMPP，IDE 强烈推荐 Sublime，一些 Sublime 的技巧：SecWiki-Sublime；
2. Python 编程学习，学习内容包含：语法、正则、文件、网络、多线程等常用库，推荐《Python 核心编程》，*不要看完*；
3. 用 Python 编写漏洞的 exp，然后写一个简单的网络爬虫，可参见 SecWiki-爬虫、视频；

4. PHP 基本语法学习并书写一个简单的博客系统，参见《PHP 与 MySQL 程序设计（第 4 版）》、视频；
5. 熟悉 MVC 架构，并试着学习一个 PHP 框架或者 Python 框架（可选）；
6. 了解 Bootstrap 的布局或者 CSS，可以参考：SecWiki-Bootstrap;

- 3 周

源码审计与漏洞分析
能独立分析脚本源码程序并发现安全问题。

1. 熟悉源码审计的动态和静态方法，并知道如何去分析程序，参见 SecWiki-审计；
2. 从 Wooyun 上寻找开源程序的漏洞进行分析并试着自己分析；
3. 了解 Web 漏洞的形成原因，然后通过关键字进行查找分析，参见 SecWiki-代码审计、高级 PHP 应用程序漏洞审核技术；
4. 研究 Web 漏洞形成原理和如何从源码层面避免该类漏洞，并整理成 checklist。

- 5 周

安全体系设计与开发
能建立自己的安全体系，并能提出一些安全建议或者系统架构。

1. 开发一些实用的安全小工具并开源，体现个人实力；
2. 建立自己的安全体系，对公司安全有自己的一些认识和见解；
3. 提出或者加入大型安全系统的架构或者开发；
4. 看自己发展咯~