**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](http://www.sec-wiki.com/news/)上搜索，例如：[Brup的教程](http://www.sec-wiki.com/news/search?wd=burp)、[sqlmap](http://www.sec-wiki.com/news/search?wd=sqlmap)；
  4. 待常用的这几个软件都学会了可以安装[音速启动](http://www.3lsoft.com/)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](http://netsec.ccert.edu.cn/hacking/files/2011/07/PTES_MindMap_CN1.pdf)；
  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](http://www.owasp.org.cn/OWASP_Training/Upload_Attack_Framework.pdf)；
  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](http://www.sec-wiki.com/news/search?wd=XSS)；
  7. 研究Windows/Linux提权的方法和具体使用，可以参考：[提权](http://www.sec-wiki.com/news/search?wd=%E6%8F%90%E6%9D%83)；
  8. 可以参考: [开源渗透测试脆弱系统](http://www.sec-wiki.com/topic/17)；
* 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](http://www.sec-wiki.com/)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](http://www.sec-wiki.com/opml/index)；
  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](http://www.exploit-db.com/)、[CVE中文库](http://cve.scap.org.cn/)、[Wooyun](http://www.wooyun.org/)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](http://www.sec-wiki.com/news/index?tag=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](http://www.sec-wiki.com/news/search?wd=Kali),《Web Penetration Testing with Kali Linux》、《Hacking with Kali》等；
  4. 熟悉metasploit工具，可以参考[SecWiki](http://www.sec-wiki.com/news/search?wd=Metasploit)、《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](http://www.sec-wiki.com/news/search?wd=%E9%85%8D%E7%BD%AE)；
  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](http://www.sec-wiki.com/news/search?wd=%E9%85%8D%E7%BD%AE)；
  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](http://www.sec-wiki.com/news/search?wd=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](http://www.wampserver.com/en/)和[XAMPP](https://www.apachefriends.org/index.html)，IDE强烈推荐[Sublime](http://www.sublimetext.com/)，一些Sublime的技巧：[SecWiki-Sublime](http://www.sec-wiki.com/news/search?wd=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](http://www.sec-wiki.com/news/search?wd=%E7%88%AC%E8%99%AB)、[视频](http://www.icoolxue.com/album/show/113)；
  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](http://www.verycd.com/topics/2843130/)；
  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](http://www.sec-wiki.com/news/search?wd=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](http://www.sec-wiki.com/news/search?wd=%E5%AE%A1%E8%AE%A1)；
  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](http://www.sec-wiki.com/news/search?wd=%E4%BB%A3%E7%A0%81%E5%AE%A1%E8%AE%A1)、[高级PHP应用程序漏洞审核技术](https://code.google.com/p/pasc2at/wiki/SimplifiedChinese)；
  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~