**简历**

学校：吉林大学

专业：软件工程

姓名：肖子健

年级：2018级本科生

**擅长：**

1. web安全漏洞原理与修复。包括sql注入，xss，文件上传，文件包含，ssrf，csrf，xxe，逻辑漏洞
2. python编程，了解python运行机制。GIL锁，多线程多进程。
3. 熟悉网络协议
4. 擅长自学，有抓重点的能力。可以在有限时间内掌握一件事情的基本样貌。大二上学期之后的全部课程都是自学的。
5. 擅长数学，高考数学140分，大学高数A基本95分(高数1,2,3，组合数学，概率论，计算方法，离散数学1,2，线性代数)。有较强逻辑思维，对于事物和事物之间的关系敏感，擅长举一反三

**了解：**

1. Linux内网渗透，权限提升
2. 网站csp绕过,waf绕过,同源策略,cors,jsonp
3. 信息搜集，子域名挖掘，端口探测，敏感信息探测。使用nmap,sqlmap,metasploit等工具。
4. Apache,iis,nginx这几个中间件的安全漏洞
5. 网络设备，会配置路由器交换机防火墙(华为设备)
6. 了解jvm，java/php/python反序列化
7. 常见的数据结构
8. 设计模式
9. 32位汇编
10. 用python进行简单的数据分析
11. 了解几个常见的数据库和使用，关系型的MySql,Oracle,非关系型的redis
12. 了解c/c++/java/php/shell
13. 具备Mac/Linux开发能力，了解常见的目录结构
14. 了解git，docker原理并使用过

**项目经历：**

1. 补天提交过src(web)
2. 了解基础的运维知识，用虚拟机搭建过渗透网络环境(网关Ubuntu，内网WinXP，dmz区域是Ubuntu运行web，Win03运行网站后台)，并且可以相互通信
3. 熟悉常见的漏洞靶场sqli-labs,upload-labs,dvwa,pikachu都做过练习并且阅读源码
4. python写过爬虫爬取图片，了解反爬虫机制
5. python写过小工具，目录爆破，子域名爆破，win03pop3缓冲区溢出代码，syn/ack/udp/dns/snmp协议的dos攻击，分别用syn/tcp/udp进行端口探测，系统探测(根据ttl)，同网段存活主机探测(都在github下的network-security项目里,主要用socket和scapy包)
6. 参加过两次全国数学建模比赛，获得省三等奖
7. 参加过学校ctf和中科大ctf比赛名次中等
8. 领导过5人的团队开发网站使用PHP/html/MySql和JSF/JPA/EJB/oracle
9. 用c/c++开发过小项目，主要是小游戏(自动扫雷，智能贪吃蛇，智能六子棋下法)也有模拟微信通信
10. 用c实现过数据结构和算法(二叉树，二叉查找数，链表，左堆，最小生成树，队列，AVL树，kpm算法，深度广度优先，快排，堆排，合并排，冒泡排，动态规划，贪心算法，归并等)

**其他：**

1. 有个人博客https://blog.csdn.net/superprintf，喜欢分享技术文章，或者记录个人学习历程
2. 自己的github：[https://github.com/x-j-j/](https://github.com/x-j-j/TeamWork-JLU_info_sys)
3. 为人谦和，喜欢发现不足提升自己，坚持长跑，参加马拉松。坚持每日阅读半小时课外书籍。坚持早睡早起9:30入睡5:30-6:00起床
4. 擅长绘画，音乐，参加过社团，业余活动丰富。