

**佰通**

工作经历

自我评价

22岁，现居广州 135-0000-0000 11111111@qq.com

求职意向：

渗透测试工程师

1. 拥有多个项目测试经验以及接近3年的测试管理经验，能够根据项目特点制定合适的测试计划、测试策略，分配测试资源并持续优化测试过程。
2. 拥有自动化脚本编写能力（Java+Selenium2.0+PageObject），有多个大型自动化项目实施经验。
3. 掌握Java+SpringMVC+Mybatis开发框架，可开展测试开发相关工作。
4. 熟悉常见的安全漏洞攻击原理、漏洞利用、防御措施以及修复方案，日常主要在“乌云”提交Bug。
5. 掌握常用渗透测试工具Metasploit、KaliLinux2.0、AppScan、WVS、Burpsuite、SqlMap、Hydra、Safe3、Nmap、XSS平台...
6. 熟悉Oracle、MySql、MSSQL等常见数据库，能熟练使用SQL语言。
7. 熟悉JMeter，能对常见场景进行性能及压力测试。熟悉Python脚本语言，可编写python自动化脚本。
8. 具备良好的沟通能力，较强适应能力和学习能力，具有极强团队合作意识。

2017.07 - 2020.10 广州大正锐科信息技术有限公司 测试leader & 渗透测试工程师

测试leader工作：

1. 负责项目的跟踪与整体把控，制定项目计划。解决和协调项目遇到的问题。参与项目功能、自动化、安全测试，跟踪并管理测试过程。
2. 管理测试团队，提升团队战斗力与凝聚力。与开发、UI、产品、运维、运营等交流沟通，保证信息对称。
3. 关注行业动态，学习新方法和新技术。

渗透测试工程师工作：

1. 制定公司产品的安全性测试的计划及安全规范。按照计划对公司产品进行渗透测试，业务逻辑安全测试。
2. 制定和完善安全性漏洞的修复方案。组建和管理安全测试团队，不断学习行业新技术。

测试工程师工作：

1. 对需求进行深入分析，并编写测试用例。独立完成分配的PC、wap、app端测试工作并提交测试报告。
2. 负责自动化代码的编写及维护工作。对系统进行性能、安全性等测试工作。
3. 与开发进行沟通，对进度进行更新及Bug进度跟踪。

2016.03 - 2017.06 信元网络安全技术股份有限公司 渗透测试工程师

1. 对联通网站做渗透测试、漏洞扫描，帮助中国联通发现多种类型的安全漏洞。引导客户进行安全管理规范建设。
2. 参与联通重大节日的网络安全保障，使其重大节日无网络安全事件发生。
3. 对中国联通的业务系统做风险评估，引导客户如何规避风险。

教育背景

项目经验

2018.08 - 2020.06 运营商渗透测试项目

对移动集团、陕西移动、青海联通、新疆移动、甘肃移动等西北多地多个运营商的渗透测试项目进行支撑。

主要工作有：

1. 日常的或周期性的渗透测试。重要检查及演习的渗透测试自测支撑及演习期间的保障。
2. 对客户的包括ctf等基础安全技能进行培训。对突发安全事件的应急响应。
3. 完成多次演习的支撑及自测。支撑多次部委及集团的检查。

2017.08 - 2017.09 DedeCMS站点渗透测试

渗透步骤：

1. 收集整理信息，判断站点功能、对应IP地址，操作系统版本、脚本语言为php、框架版本信息版本等。
2. Nmap扫描对应IP，查看开放的端口。AWVS扫描，发现注入点，手工判断存在注入，sqlmap拖库。
3. 破解用户密码后登录管理后台，上传webshell脚本。
4. 连接后台，查看登录账户发现后台登录账户为应用用户，做简单提权。
5. 使用NC反弹，代理转发后，扫描该网段存活主机，发现有一台开启了3389端口的主机。
6. 使用弱口令爆破，取得服务器控制权。登录该主机，发现该主机是域控服务器。

漏洞汇总：

敏感信息泄露，开源CMS未修改后台默认目录；攻击检测与防范不足，账户登录无验证码，可爆破，可上传木马；发现内网域控服务器存在弱口令，爆破成功就可以控制服务器。

修复方案：

建议修改默认目录名称；建议增加验证码功能；建议增加所有上传文件的服务器MIME校验白名单功能；建议所有后台密码使用复杂性密码。漏洞挖掘及验证。

2016.06 - 2017.06 华数安保驻场测试

主要在乙方驻场负责渗透测试、入侵检测、应急响应等工作内容并且参与公司其他项目的渗透和应急响应工作。日常：安全监测、周报输出、月度扫描、应用上线前安全检测。

重要工作有：

1. 16年6月协助广电总局调查创维色情广告事件，挖的主要后台SQL注入漏洞2个，其中包含总网流量控制系统(EPG内网系统)。
2. 16年7-8月对浙江华数下面的省市公司子公司进行等保式的安全检测。
3. 16年10月参与ICTC展会公司展台筹建工作。
4. 16年11月获得华为私有云月活动第三名。
5. 17年2月春节期间外部应急响应及溯源。
6. 17年2月负责互联网机顶盒安全测试和应急响应。

主要负责渗透测试、入侵检测、应急响应等工作内容。

2012.09 - 2016.06 广东电子信息职业技术学院 信息安全与管理 / 大专