交易所安全审计指南

零时科技安全团队《交易所安全测试》这一系列的文章已经结束了，为了方便广大安全人员查阅，我们将这十期文章做了一个总结，希望在安全人员们测试或各大交易所想要检查自家交易所安全问题时，能够提供便利。

一、信息收集

信息收集对于安全测试来说，是非常重要且必要的第一步。有时一次非常全面完善的信息收集甚至会占到一次渗透测试总工程量的的70%到80%，为后续的工作提供大量便利。

Checklist

> - 域名 Whois及备案信息采集
> - 服务器真实 IP 发现
> - 服务器指纹识别
> - 目标子域探测
> - 邮件服务探测
> - 证书信息采集
> - Web服务组件指纹采集
> - Web网站目录探测
> - API接口信息泄露
> - 端口服务组件指纹采集
> - 旁服信息采集
> - C 段服务采集
> - GitHub/SVN源码泄露发现
> - DNS记录分析搜索引擎公开信息采集（google，shodan，zoomeye）
> - 企业信息采集（员工信息，组织框架，企业法人，企业综合信息）
> - 敏感文件发现

二、信息收集进阶篇（社会工程学）

社会工程学是信息收集技术的延伸和升级，是更高级的信息利用手段。社会工程学利用系统中最大的漏洞——人来收集更高级，更隐秘的情报，是最直接，最有效的攻击手段之一。

Checklist

> - 身份信息采集
>   - 姓名，绰号，性别发现
>   - 学籍履历发现
>   - 曾、现用手机号发现
> - 关系网络梳理
>   - 工作关系网络梳理
>   - 生活关系网络梳理
> - 社交信息发现
>   - 朋友圈，QQ空间等遗留信息发现
>   - 其他交友APP信息发现
> - 水坑攻击

- 钓鱼攻击
    - 邮件钓鱼
    - 网页钓鱼
- 口令猜解

三、业务逻辑

业务逻辑漏洞独立于其他服务却又受其他安全问题牵扰。业务逻辑漏洞通常和正常业务流程中程序的固有不足，逻辑设计缺陷相关，甚至绕过已有的安全防护措施，一般防护手段及安全设备无法防御检测，可谓防不胜防。

Checklist

- 越权操作测试
    - 订单越权发起、查看、编辑、删除
    - 地址越权添加、删除
    - 用户信息越权查看、编辑
- 工作流程绕过测试
- KYC认证缺陷测试
    - 接口识别
    - 人工识别
- OTC逻辑缺陷测试
- 数值精度测试
- 资产安全测试
    - 充值
    - 提现
- 二次验证绕过测试
    - Google验证器
    - 手机及邮箱验证吗
- 盘口价格设置缺陷测试
- 假充值测试
- 短地址攻击测试
- 数值精度测试

四、信息泄露

交易所工作人员如果有所疏忽，就有可能产生信息泄露问题。零时科技安全团队在审计大量交易所后发现，信息泄露问题一般集中于交易所的账户体系、OTC交易系统、用户订单、邀请列表和网站源代码等地。总的来说信息泄露就是对私密的，不应外露的信息保护不当引发的问题。

Checklist

- KYC信息泄露
    - 登录注册
    - 忘记密码
    - 邀请列表
    - OTC交易系统

    - 用户订单
- 前端源码信息泄露
    - 测试数据泄露
    - 敏感信息泄露
    - API接口泄露
- Github信息泄露
    - 数据库文件/连接凭据
    - 敏感信息泄露
- 敏感文件信息泄露
    - robots.txt
    - crossdomain.xml
    - sitemap.xml
    - .git/.svn/.bak

五、输入输出安全

输入输出的安全问题来源于部分开发人员编码过程中的粗心大意以及应有的安全意识的缺失，如部分开发人员对用户的输入不做任何处理等。这些安全问题对于网站来说是非常严峻的，利用手法繁多且对数据库，网站管理权限，内网都有巨大威胁。

Checklist

- 跨站脚本（XSS）
- 模板注入测试
- HTTP头注入测试
- HTTP参数污染测试
- 不安全的HTTP方法测试
- 服务端请求伪造（SSRF）测试
- 任意文件上传
- SQL注入测试
- XXE实体化测试
- 反序列化漏洞测试
- HTTP请求夹带（smuggling）攻击测试
- 代码注入测试
- 本地文件包含测试
- 远程文件包含测试
- 命令执行注入测试
- 缓冲区溢出测试
- 格式化字符串测试

六、配置安全

服务端是一种专门为某一客户端设立的，具有针对性的程序，通常都只具备认证与传输数据功能，但却是网站运行得重要组成部分之一，也是网站的根基。如果服务端配置并不安全，也就意味着根基不牢，危险性可想而知。

Checklist

- 后端服务组件配置测试
- 服务器登录安全测试

- 文件扩展名解析测试
- 备份文件测试
- 测试文件测试
- 测试接口暴露
- HTTP方法测试
- Web前端跨域策略测试
- Web安全响应头部测试
- 弱SSL/TLS加密，不安全数据传输测试
- 非加密信道传输敏感数据测试
- 弱口令及默认口令探测
- 管理后台发现

七、用户认证

用户认证是一种非常古老的问题，古早的“盗号”就属于此类。此类安全问题的危害也显而易——当一个恶意攻击者有办法通过认证进入你的账户并拿走你的钱时，他是绝对没有理由把钱放在那的。

Checklist

- 用户注册过程测试
- 用户登录过程测试
- 找回密码过程测试
- 设备解绑过程测试
- 验证码策略测试
- 帐户权限变化测试
- 帐户枚举测试
- 弱密码策略测试
- 口令信息加密传输测试
- 默认口令测试
- 帐户锁定机制测试
- 认证绕过测试
- 浏览器缓存测试
- 权限提升测试
- 授权绕过测试
- 撞库攻击测试

八、接口安全

接口，即API，“应用程序编程接口”。是一些预先定义的函数，使得应用程序与开发人员基于某软件或硬件可以访问一组例程，而又无需访问源码或理解内部工作机制的细节。由于其快速、有效和安全、可靠的特性，被开发人员广泛的使用。但如果接口本身没有做好安全防护或者调用时没有做好频率限制，都会导致问题的出现。

Checklist

- RPC安全测试
  - RMI远程命令执行
  - CORS
- Web Service安全测试
  - SQL注入

    - 信息泄露
- GraphQL安全测试
    - 未授权访问
    - 信息泄露
    - GraPhQL SQL注入
    - 嵌套查询DOS
- RESTful API安全测试
- 数值精度测试
- 接口频率限制测试
    - 邮箱验证接口
    - 短信验证接口
    - 批量刷单
- 超时检测

九、APP安全

APP现如今已经被使用得越来越频繁，但其安全方面还处在刚刚起步的阶段，与一张白纸相去不远。故此，即使交易所网站这道“城墙”能使恶意攻击者毫无办法，但如若不慎，APP这道小“暗渠”也能要了城里人的命。

Checklist

- App 运行时虚拟机监测
- App 运行时root监测
- App数据备份检测
- 代码反编译检测
- 敏感权限使用
- 敏感信息泄露
- 拒绝服务测试
- 目录穿越安全测试
- App 缓存安全检测
- 接口安全测试
- 弱加密安全测试
- 秘钥硬编码安全检测
- 数据存储安全检测
- 数据传输安全检测
- 日志信息泄露检测
- App组件导出检测
- App组件权限检测
- webview 多项漏洞安全测试
- App Webview DOM 安全测试
- 本地SQL注入安全测试
- SQLite 存储安全审计

以上即零时科技安全团队本期《交易所安全测试》系列文章的总结，敬请期待下一系列文章！

本项目Github地址：https://github.com/NoneAge/BlockchainSecurityTutorial/tree/master/1.CryptocurrenciesExchangePentestTutorial