ABCWallet 安全审计报告

项目概述

此次安全审计项目核心目标是为 ABCWallet 进行快速全面的安全审计，检测潜在的威胁点，协助 ABCWallet 提升一个安全维度。协力 ABCWallet 团队一起为客户的资金安全做出最有效的推进，更好的保护广大 ABCWallet 用户的安全。

前言

感谢 ABCWallet 项目方对慢雾科技的认可，感谢相关人员的辛苦与支持。

审计周期：10 个工作日

审计团队：慢雾安全团队

审计时间：2019 年 10 月 10 日 - 2019 年 10 月 20 日

【iOS 文件版本】

文件名：Payload.ipa

版本号：1.0.38

MD5：97bc2a3b6ba7c66923d2dfd715eae6f6

【Android 文件版本】

文件名：app-devtest-release1.0.11_2019-10-15_21-01-56_legu_aligned_signed.apk

版本号：1.0.11

文件 MD5：0b3193c632e3ffbc16bd21642e1a7dbf

文件下载地址：https://www.pgyer.com/Jfhi

项目介绍

ABC 钱包是 BlockABC 团队重磅打造的业界独一无二的区块链应用，支持管理多个主流公链资产、交易所资产和 NFT 资产，提供涵盖行情、交易、理财、 Staking、OTC 等一站式理财服务，功能特性丰富繁多，却拥有极其简单易用的交互体验。

审计结果

（其他未知安全漏洞不包含在本次审计责任范围）

序号	审计大类	审计子类	审计结果
1	开源情报采集	域名 Whois 信息采集	通过
		真实 IP 发现	通过
		子域探测	通过
		邮件服务探测	通过
		证书信息采集	通过
		Web 服务组件指纹采集	通过
		C 段服务采集	通过
		人员组织结构采集	通过
		GitHub 源码泄露发现	通过

		人员隐私泄露发现	通过
2	服务端安全配置审计	CDN 服务探测	通过
		文件扩展名解析测试	通过
		备份 / 未链接文件测试	通过
		HTTP 方法测试	通过
		HTTP 严格传输测试	通过
		Web 前端跨域策略测试	通过
		Web 安全响应头部测试	通过
		弱口令及默认口令探测	通过
		管理后台发现	通过
3	身份鉴别管理审计	角色定义测试	通过
		用户注册过程测试	通过
		帐户权限变化测试	通过
		帐户枚举测试	通过
		弱用户名策略测试	通过
4	认证与授权审计	口令信息加密传输测试	通过
		默认口令测试	通过
		认证绕过测试	通过
		记住密码功能测试	通过

		浏览器缓存测试	通过
		密码策略测试	通过
		密码重置测试	通过
		权限提升测试	通过
		授权绕过测试	通过
		双因素认证绕过测试	通过
		Hash 健壮性测试	通过
5	会话管理审计	会话管理绕过测试	通过
		Cookies 属性测试	通过
		会话固定测试	通过
		会话令牌泄露测试	通过
		跨站点请求伪测试	通过
		登出功能测试	通过
		会话超时测试	通过
		会话令牌重载测试	通过
6	输入安全审计	跨站脚本（XSS）测试	通过
		模板注入测试	通过
		第三方组件漏洞测试	通过

		HTTP 参数污染测试	通过
		SQL 注入测试	通过
		XXE 实体注入测试	通过
		反序列化漏洞测试	通过
		SSRF 漏洞测试	通过
		代码注入测试	通过
		本地文件包含测试	通过
		远程文件包含测试	通过
		命令执行注入测试	通过
7	业务逻辑审计	交易业务逻辑检测	通过
		数据完整性测试	通过
		请求伪造测试	通过
		接口安全测试	通过
		接口频率限制测试	通过
		工作流程绕过测试	通过
		非预期文件类型上传测试	通过
		恶意文件上传测试	通过

8	密码学安全审计	弱 SSL/TLS 加密，不安全的传输层防护测试	通过
		SSL Pinning 安全部署测试	通过
		非加密信道传输敏感数据测试	通过
9	移动端审计	钱包安全	通过
		运行环境安全	通过
		代码禁止反编译	通过
		文件存储安全	通过
		通信加密	通过
		权限安全	通过
		接口安全	通过
		业务安全	通过
		WebKit 安全	通过
		APP 缓存安全	通过
		APP Webview DOM 安全	通过
		APP SQLite 存储安全审计	通过
		APP 代码混淆	通过
综合审计结果			通过

最终评级：优

免责声明

厦门慢雾科技有限公司(下文简称“ 慢雾 ”) 仅就本报告出具前已经发生或存在的事实出具本报告，并就此承担相应责任。对于出具报告以后发生或存在的未知漏洞及安全事件，慢雾无法判断其安全状况，亦不对此承担责任。

本报告所作的安全审计分析及其他内容，仅基于信息提供者截至本报告出具时向慢雾提供的文件和资料(简 称“已提供资料”)。慢雾假设:已提供资料不存在缺失、被篡改、删减或隐瞒的情形。如已提供资料信息缺失、被篡改、删减、隐瞒或反映的情况与实际情况不符的，慢雾对由此而导致的损失和不利影响不承担任何责任。

慢雾科技
slow mist

官方网址

www.slowmist.com

电子邮箱

team@slowmist.com

微信公众号