OceanONE 安全审计报告

（2018 年 09 月 05 日）

审计周期：7 天

审计团队：慢雾安全团队

审计时间：2018 年 8 月 20 日 - 2018 年 8 月 27 日

网站地址：https://ocean.one

代码仓库：https://github.com/MixinNetwork/ocean.one

(提交版本：dd82931be41621ccb6cff693ff3f5cdc82921596)

项目介绍：

OceanONE 是一个基于 Mixin Network 构建的去中心化交易所，它几乎是去中心化交易所首次实现与中心化交易所相同的用户体验。

OceanONE 接受 Mixin Network 中的所有资产作为基础货币，唯一支持的报价货币是 Mixin XIN，比特币 BTC 和 Omni USDT。

所有订单和交易数据都在 Mixin Network 快照的 memo 中，编码 memo 是 base64 编码的 MessagePack。

审计结果：

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		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

	认证与授权审计	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	接口安全测试	通过
		请求伪造测试	通过
		完整性测试	通过
		超时检测	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
		交易挂单逻辑测试	通过
		交易吃单逻辑测试	通过
		充值提现逻辑测试	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	Go 源代码审计	解引用 nil 指针	通过
		越界访问	通过
		运行时未捕获的异常	通过
		巨大切片分配请求	通过
		无限递归和循环	通过
		死锁	通过
		多线程数据竞争	通过
		文件目录越权读写	通过
10	开源安全审计工具	Gosec 审计	通过
综合审计结果			通过

最终结论： OceanONE 作为首个在 Mixin Network 上构建的去中心化交所，在审计过程中未发现严重、高危漏洞，项目方快速响应、及时解决发现的任何细节安全问题，团队成员技术扎实。

官方网址

www.slowmist.com

电子邮箱

team@slowmist.com

微信公众号