北京阿拉丁未来科技有限责任公司

阿拉丁统计服务器
安全测试结论

版本：v1.0

日期：2017/4/28

第三方公司测试结果：

测试公司：斗象科技

使用产品：漏洞盒子

测试结果：

测试名称	检查状态
SQL 注入攻击	通过
反射式跨站脚本攻击	通过
存储式跨站脚本攻击	通过
DOM 跨站脚本攻击	通过
会话固定	通过
HTTP 头安全配置	通过
HTTP 方法	通过
服务器版本信息	通过
会话生命周期	通过
水平权限溢出	通过
纵向权限溢出	通过
默认凭证	通过
弱密码规则测试	通过
账户锁定测试	通过
安全问题测试	通过
密码修改测试	通过
目录遍历	通过
文件包含	通过

授权绕过	通过
权限溢出	通过
不安全对象直接引用	通过
Cookie 属性	通过
会话管理	通过
登出测试	通过
会话超时测试	通过
账户恶意锁定	通过
用户账户唯一性测试	通过
Session 随机性与唯一性测试	通过
CRLF 注入测试	通过
LDAP 注入测试	通过
XML 注入测试	通过
ORM 注入测试	通过
Xpath 注入测试	通过
本地文件包含	通过
远程文件包含	通过
命令执行	通过
缓冲区溢出	通过
堆溢出	通过
栈溢出	通过
格式化字符串测试	通过
HTTP Split 测试	通过
代码异常处理	通过
栈异常跟踪	通过
SSL/TLS 加密算法测试	通过
PaddingOracle 测试	通过
敏感信息泄露	通过
上传文件测试	通过
事务完整性测试	通过
HTML 注入	通过
URL 重定向攻击	通过

CSS 注入攻击	通过
Blind 注入测试	通过
点击劫持测试	通过
WebSocket 测试	通过
本地存储测试	通过
Web Messaging 测试	通过
IMAP/SMTP 注入测试	通过
代码注入测试	通过
处理响应时间测试	通过
可用性测试	通过
CORS 测试	通过
FlashSWF 测试	通过
恶意文件上传测试	通过
暴力破解	通过
传输层常见安全测试	通过
错误代码分析	通过
失效验证测试	通过
使用已知不安全组件测试	通过
未验证重定向与转发	通过
不安全对象失效间接引用	通过
默认配置安全测试	通过

阿拉丁安全说明：

1. 阿拉丁统计日志服务器
    a) 接口采用 HTTPS 协议，经过抓包以及嗅探，无法获取真实数据。
    b) 日志服务器都经过第三方服务器安全测试，确定暂无服务器漏洞。
2. 阿拉丁运算服务器
    a) 阿拉丁运算服务器都是使用私有网络。通过私有网络中的核心数据库进行交换数据，外网无法直接访问。

b) 阿拉丁运算服务器通过证书验证且每台服务器证书不一样并定期更换，服务器本身设置了高强度的密码防止黑客通过其他手段记性破解。

3. 服务器管理

a) 服务器安全秘钥专人管理。其他工作人员无法登陆相关服务器。并与服务器管理人员签订了相关保密协议。