|  |  |
| --- | --- |
| **产品名称Product name** | **密级Confidentiality level** |
| **营销广告分析** | **内部公开** |
| **产品版本Product version** | **Total pages共15页** |
| **BI MAAS 1.0.2.300** |

**营销广告分析安全性测试策略**

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by  拟制 | 金雪松 | Date  日期 | 2015-09-15 |
| Reviewed by  评审人 | 林啸鸣 | Date  日期 | 2015-09-16 |
| Approved by  批准 |  | Date  日期 | yyyy-mm-dd |



Huawei Technologies Co., Ltd.  
华为技术有限公司

All rights reserved  
版权所有 侵权必究

修订记录

| **日期** | **修订版本** | **CR号** | **修改章节** | **修改描述** | **作者** |
| --- | --- | --- | --- | --- | --- |
| 2015-09-15 | V1.0 |  |  | 初稿输出完成 | 金雪松/00165946 |
|  |  |  |  |  |  |

目 录

1 概述 5

2 测试规划 5

2.1 项目分析 5

2.2 分层策略 5

2.3 测试计划 6

2.4 自动化策略 6

2.5 测试工具规划 6

3 安全测试策略 7

3.1 总体测试策略 7

3.2 SDV安全测试策略 8

3.3 SIT安全测试策略（备注：本次测试不安排SIT，此处略） 10

4 参考资料清单 10

4.1 Web安全测试规范 10

**Keywords 关键词**：终端，营销广告分析，安全红线，测试策略

Abstract 摘要：安全测试策略主要用于指导安全测试方案的输出，测试计划的安排，测试风险的识别等工作，作用如下：

* 手工测试、自动化测试的分工策略，（SDV/SIT/SVT）各阶段的测试策略，安全测试工具（如：Nessus、NGS）的资源规划，以及明确工具使用配置/规则或策略；
* 产品历史版本或同类产品的安全问题进行继承性分析，明确产品的基线/增量测试策略；
* 针对现网安全问题用例集进行产品针对性梳理，输出测试范围和重点；
* 识别高风险模块，进行针对性的测试分析，提高测试覆盖范围。

**缩略语清单：**

| 缩略语 | 英文全名 | 中文解释 |
| --- | --- | --- |
| ICSL | Internal Cyber Security Lab | 内部网络安全实验室 |
| EMUI | Emotion User Interface |  |
|  |  |  |
|  |  |  |

# 概述

营销广告分析是为了支撑日常的终端的营销，进行终端营销时选择哪些门户、哪些广告位进行广告的投放，广告投放的效果如何，而设计的一套系统，在跟踪分析终端广告投放的效果。 营销广告分析具有用户录入、查询、维护广告位信息的系统，用户主要为公司内部人员。该系统结构较简单，且后期会进行框架更换。本次测试目的是为了覆盖整个系统，基于最新的网络安全红线2.0，排查安全问题，并进行整改。

# 测试规划

## 产品组网图



**测试模块：**

产品主要部件/模块为MktSystem，BIportal、mysql、邮件服务器等，Mktsystem对用户提供直接的服务。

**测试维度：**

* A1类：合法监听接口、隐私保护、未公开接口
* A2类：访问通道控制、软件完整性保护、敏感数据与加密保护、日志审计

B类：操作系统加固与防病毒、Web安全、产品开发、发布和安装安全、数据库加固、口令安全、敏感数据保护、访问通道控制

**测试重点：**

* 敏感信息/数据存储和传输；
* 用户登录鉴权、用户权限管理；
* WEB安全测试
* 第三方软件安全性测试以及工具(例如APPScan、FUZZ等)扫描；
* 组网安全

产品主要部件/模块为MktSystem，其中第三方软件/模块为mysql、BIportal、邮件服务器，mysql、邮件服务器主要检查敏感数据是否加密存放、传输等，对功能不进行重点检查。

## 分层策略

手工测试策略：

涵盖应用及系统安全，日志检查，权限检查，数据存储检查，这些部分都需要通过手工测试来进行。

自动测试策略：

过程中会用到APPSCAN，敏感信息扫描工具，Nessus，PeachFuzzer，SecureCAT，NMAP以及NGS Squirrel这些工具做自动化的扫描和测试。

版本源代码需进行安全工具扫描。

## 测试计划

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **版本名称** | **测试时间** | | **测试人员** | **测试地点** | **配套测试的配套版本** | |
| **起始时间** | **结束时间** | **产品名称与版本号** | **版本说明** |
| BI MAAS 1.0.2.300 | 2016-01-22 | 2016-01-22 | 张中维 | 南京 | BI MAAS 1.0.2.300 |  |
|  |  |  |  |  |  |  |

## 自动化策略

目前无安全方面的自动化用例，后期再规划、实施。

## 测试工具规划

涵盖所有测试过程中需要用到的工具，在这里列明，并给出获取方式：

|  |  |  |  |
| --- | --- | --- | --- |
| 工具名称 | 作用 | 工具地址账号信息 | 备注 |
| APPSCAN | Web服务器扫描 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| PeachFuzzer | Fuzz模糊测试工具 | https://szxsvn04-ex:3690/svn/TC\_EMUI\_DOC\_SVN/07.安全与测试/02 测试/02 业务测试/05 云安全测试/03 安全工具 | 本地部署，参考附件中的PeachFuzzer测试指导。 |
| Nessus | OS扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| SecureCAT | OS扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| NMAP | 端口扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| NGS Squirrel | 数据库安全扫描工具 | <http://rnd-tcloud.huawei.com:8080/safeui/home/main>  备注：域名登录 | 参照云安全测试平台给定的扫描策略，填入相关服务器信息即可。 |
| Coverity | 代码静态扫描 | 专门服务器提供扫描，无需个人部署。 |  |
| Fortify | 代码静态扫描 | 专门服务器提供扫描，无需个人部署。 |  |
| 防病毒软件（Symantec、Mcafee、Avira AntiVir、卡巴斯基等） | 病毒扫描 | VMP提供自动扫描功能 |  |
| Burpsuit | 网络通信测试工具 | 单机版，归档地址：  https://szxsvn04-ex:3690/svn/TC\_EMUI\_DOC\_SVN/07.安全与测试/02 测试/02 业务测试/05 云安全测试/03 安全工具 |  |
| 敏感信息扫描工具 | 扫描秒干信息 | 单机版，归档地址：  https://szxsvn04-ex:3690/svn/TC\_EMUI\_DOC\_SVN/07.安全与测试/02 测试/02 业务测试/05 云安全测试/03 安全工具 |  |

# 安全测试策略

## 总体测试策略

### 测试点分析

* 登录—用户通过鉴权访问系统；
* 数据存储与数据展示；
* 用户权限设置，是否存在越权；
* 环境检查及相关工具扫描；
* 信息传输通道；
* 业务测试点以及日志检查

|  |  |  |
| --- | --- | --- |
| 序号 | 特性 | 说明 |
| 1 | 营销活动 | 创建、修改营销活动，并可对营销活动做权限设置 |
| 2 | 广告位信息录入 | 创建、修改、删除、发布、重置、广告位信息 |
| 3 | 着陆连接（Vmall） | 录入、修改、发布、重置、着陆链接（vmall） |
| 4 | 着陆连接（荣耀官网） | 录入、修改、发布、重置、着陆链接（荣耀官网） |
| 5 | 监控代码（BI） | 生成、重置、监控代码 |
| 6 | 流量报表 | 查看营销活动下的数据信息 |
| 7 | 着陆平台 | 新建、修改、删除 着陆平台 |
| 8 | 推广产品 | 新建、修改、删除 推广产品 |
| 9 | 广告媒体 | 新建、修改、删除 广告媒体信息 |
| 10 | 常用联系人 | 联系人列表，包含用户名、姓名、部门、电话号码、邮箱、描述信息 |
| 11 | 用户管理 | 添加、删除、修改用户信息 |
| 12 | 角色管理 | 新增、修改角色，赋予角色权限 |
| 13 | 操作日志 | 记录所有用户对营销广告分析的操作 |

涉及模块主要由Mktserver、BIportal

重点测试Web安全、敏感数据是否加密存储，日志检查（包括日志权限），用户权限控制、密码/验证码安全等安全红线测试用例，并使用安全工具对web、接口、数据库、代码等进行扫描和检查，并进行fuzz工具进行测试。

### 高风险模块分析

BIportal:主要负责用户登陆检查、认证、鉴权等；需重点进行操作、应用系统安全以及Web安全方面的测试

Mktserver:通过web向用户提供直接的服务，测试过程中需要考虑基本的web测试规范。

两个模块提供的服务，包括接口等需要重点测试。

### 继承特性的安全测试策略

自研部件需要全部测试，因此这部分的继承特性分析不涉及，部分第三方安全软件可参考公司相关规范处理。

### 安全基线用例集覆盖策略

覆盖已经定稿的安全基线用例库，重点测试应用及操作系统安全、Web安全测试规范、口令安全等安全红线测试用例，敏感数据是否加密存储，日志中是否有敏感信息，用户权限控制等安全红线测试点，工具扫描等。

### 测试风险分析

测试能力：目前安全测试能力比较薄弱，对一些工具掌握不够，投入时间也不足；目前只能针对安全红线测试用例做防御性的测试设计和测试执行，缺乏渗透测试等测试能力。

### **网上问题分析**

**暂无安全方面的网上问题，需要分析其他产品产生的网上安全问题，进行相应测试。**

### **威胁建模分析和测试策略**

### 3.1.7.1外部交互方分析

#### Hadoop

|  |  |  |
| --- | --- | --- |
| 元素名称 | Hadoop | |
| 元素概述 | 支撑后台数据 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全检查，传输通道检查 |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 统一Portal

|  |  |  |
| --- | --- | --- |
| 元素名称 | 统一Portal | |
| 元素概述 | 包括统一Portal和华为IT机房域认证系统 | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **不分析：在信任边界内**  内部信任系统 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 信息传输通道，加密算法，密码安全、验证码机制，Web安全等 |
| 抵赖（R） | 风险（Risk） | **不分析：在信任边界内**  内部信任系统 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### 用户

|  |  |  |
| --- | --- | --- |
| 元素名称 | 用户 | |
| 元素概述 | NA | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  用户被仿冒,可以配置查看系统的数据  【可能性】  1. 同时获得vpn账号、vpn证书和华为员工域账号密码  2.同时获得iaccess接入权限和华为员工域账号密码  **可能性评估：**  无 |
| 已有消减措施 | 1.使用公司域账号进行认证  2.必须接入iaccess或vpn才能访问  3.使用https通道 |
| 建议消减措施 | 1. 无 |
| 测试策略 | 访谈，登陆通道/方法验证 |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  修改系统配置信息  【可能性】  获取授权系统账号及数据库账号删除操作日志数据  **可能性评估：**  无 |
| 已有消减措施 | 1.只有运维人员通过vpn才能访问业务数据库  2.只有授权的Linux账号才能访问数据库并删除数据  3.通过接口等方式也无法访问日志数据  4.根据运维管理制度，运维人员定期修改密码 |
| 建议消减措施 | 1. 无 |
| 测试策略 | 用户权限测试，日志权限测试 |

#### 邮件服务器

|  |  |  |
| --- | --- | --- |
| 元素名称 | 邮件服务器 | |
| 元素概述 | NA | |
| 威胁 | SR | |
| 仿冒（S） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 传输通道、组网安全、工具扫描、接口鉴权等 |
| 抵赖（R） | 风险（Risk） | **风险等级：无**  **影响：**  NA  **可能性评估：**  局域网内内部组件，在同一信任区域内 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全 |

### 3.1.7.2数据流分析

#### Hadoop⇒MKT Server(数据导出)

|  |  |  |
| --- | --- | --- |
| 元素名称 | Hadoop⇒ MKT Server(数据导出) | |
| 元素概述 | NA | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全 |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全 |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 产品落地计划 | NA |

#### MKT Server⇒邮件服务器(发送邮件)

|  |  |  |
| --- | --- | --- |
| 元素名称 | MKT Server⇒邮件服务器(发送邮件) | |
| 元素概述 | NA | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全、鉴权、 |
| 信息泄漏（I） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | 组网安全、鉴权及协议检查测试等 |
| 拒绝服务（D） | 风险（Risk） | **不分析：在信任边界内**  内部处理模块，不对外交互，1层不做分析 |
| 已有消减措施 | NA |
| 建议消减措施 | NA |
| 测试策略 | NA |

#### 统一Portal⇔MKT Server(认证Token/用户信息)

|  |  |  |
| --- | --- | --- |
| 元素名称 | 统一Portal⇔MKT Server(认证Token/用户信息) | |
| 元素概述 | MKT到统一Portal认证token是否合法,统一Portal同步用户信息到MKT | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  影响业务登录,同步错误的用户信息  【可能性】  网元被劫持篡改数据  **可能性评估：**  无 |
| 已有消减措施 | 1.https传输，认证证书  2.认证消息头和时间戳 |
| 建议消减措施 | 无 |
| 测试策略 | 信息传输通道安全、加密算法、web安全（session）等 |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  泄露用户token信息  【可能性】  网络嗅探抓包分析  **可能性评估：**  无 |
| 已有消减措施 | 1.https传输 |
| 建议消减措施 | 无 |
| 测试策略 | 信息传输通道安全、加密算法、web安全（session）等 |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  攻击者发起大量请求导致统一Portal拒绝服务  【可能性】  攻击者模拟消息请求  **可能性评估：**  无 |
| 已有消减措施 | 1. 访问设置白名单IP控制  2.https配置证书认证  3.前段设有防火墙及Nginx进行流控 |
| 建议消减措施 | 无 |
| 测试策略 | 1、白名单检查，配置文件权限检查等 |

#### 用户⇔MKT Server(操作请求/Token/响应结果)

|  |  |  |
| --- | --- | --- |
| 元素名称 | 用户⇒ MKT Server(操作请求/Token/响应结果) | |
| 元素概述 | 用户配置应用信息，查询统计数据 | |
| 威胁 | TID | |
| 篡改（T） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  数据被篡改后MKT执行错误的操作，用户看到异常的结果  【可能性】  劫持网元修改数据流内容  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.https加密传输 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道检查测试，传输通道安全，算法安全，web安全（session） |
| 信息泄漏（I） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  泄露用户token及数据统计结果  【可能性】  网络抓包分析  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.https加密传输 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道检查测试，传输通道安全，算法安全，web安全（session） |
| 拒绝服务（D） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  恶意攻击导致MKT拒绝服务  【可能性】  模拟数据攻击  **可能性评估：**  无 |
| 已有消减措施 | 1.运维vpn或者iaccess通道，不对外提供服务  2.域账号密码认证  3.设置有防火墙进行流控 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道测试（VPN等） |

### 3.1.7.3处理过程分析

#### MKT Server

|  |  |  |
| --- | --- | --- |
| 元素名称 | MKT Server | |
| 元素概述 | 为用户提供操作入口,配置应用信息、查询统计数据 | |
| 威胁 | STRIDE | |
| 仿冒（S） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  仿冒MKT为客户端浏览器提供服务  【可能性】  用户本地hosts被修改，或者DNS被劫持，导致用户 访问到仿冒的钓鱼网站  **可能性评估：**  无 |
| 已有消减措施 | 用户本地需要是vpn或iaccess接入，规避DNS被篡改 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道、Web安全、用户权限控制 |
| 篡改（T） | 风险（Risk） | **风险等级：中**  **影响：**  【影响】  影响正常的业务逻辑  【可能性】  利用输入通道注入，获取相应权限篡改程序  **可能性评估：**  无 |
| 已有消减措施 | 1. 代码层面完成安全编码（codecc、代码检视等）  2.系统层面通过appscan扫描 防止出现注入  3.系统运行环境和容器定时更新漏洞 |
| 建议消减措施 | 无 |
| 测试策略 | Web安全、工具扫描 |
| 抵赖（R） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  修改系统配置信息  【可能性】  获取授权系统账号及数据库账号删除操作日志数据  **可能性评估：**  无 |
| 已有消减措施 | 1.只有运维人员通过vpn才能访问业务数据库  2.只有授权的Linux账号才能访问数据库并删除数据  3.通过接口等方式也无法访问日志数据  4.根据运维管理制度，运维人员定期修改密码 |
| 建议消减措施 | 无 |
| 测试策略 | 用户访问通道、Web安全、用户权限控制（日志权限等） |
| 信息泄漏（I） | 风险（Risk） | **风险等级：低**  **影响：**  影响】  泄露系统信息  【可能性】  1.利用漏洞获取特权  **可能性评估：**  无 |
| 已有消减措施 | 1.系统中不存在涉及用户隐私的数据  2.appscan扫描防止漏洞出现  3.codecc 检查、规范日志 防止泄露系统信息  4.系统运行环境仅运维人员通过vpn接入才能访问 |
| 建议消减措施 | 无 |
| 测试策略 | 1、工具扫描、数据存放及加密 |
| 拒绝服务（D） | 风险（Risk） | **风险等级：低**  **影响：**  系统提供服务相应变慢  【可能性】  恶意用户Dos攻击  **可能性评估：**  无 |
| 已有消减措施 | 1. 内部系统，必须通过iaccess/vpn访问，用户量较少，且有操作日志。可以减少恶意攻击的风险  2. 关键资源有排队机制，超出范围数据等待  3.提供主备倒换能力  4.系统设有防火墙减少恶意攻击  5.运维对cpu、内存等使用情况有监控机制 |
| 建议消减措施 | 无 |
| 测试策略 | Web安全、验证码机制等 |
| 特权提升（E） | 风险（Risk） | **风险等级：低**  **影响：**  【影响】  获得高级权限，查看高级数据或执行高级操作  【可能性】  低  **可能性评估：**  无 |
| 已有消减措施 | 1.账号使用华为域账号  2.权限基于角色进行管理  3.使用拦截器实现用户权限控制  4.以单独的linux账号运行程序，且仅分配必须的权限 |
| 建议消减措施 | 无 |
| 测试策略 | 用户权限控制，信息传输通道及加密 |

## SDV安全测试策略

#### 测试重点

重点测试Web安全、敏感数据是否加密存储，日志检查（包括日志权限），用户权限控制、密码/验证码安全等安全红线测试用例，并使用安全工具对web、接口、数据库、代码等进行扫描和检查，并进行fuzz工具进行测试。

#### 入口准则

入口条件，开发提供如下交付件。

|  |  |
| --- | --- |
| **序号** | **交付件名称** |
|
| 1 | 特性列表 |
| 2 | 需求设计说明书 |
| 3 | 安全性威胁分析及需求说明书 |
| 4 | 安全设计说明书 |
| 5 | 安全及隐私设计检视Checklist（含共性设计问题） |
| 6 | 差异化分析说明书 |
| 7 | 代码静态扫描报告 |
| 8 | 代码安全检视报告 |
| 9 | AppScan扫描报告 |
| 10 | Fuzz测试结果以及问题跟踪记录 |
| 11 | 通信矩阵 |
| 12 | 安全配置/加固指南 |
| 13 | 安全操作维护手册 |
| 14 | 防病毒部署指南 |
| 15 | 安全技术白皮书 |
| 16 | 业务安全相关文件信息说明 |
| 17 | 第三方代码开源认证报告 |
| 18 | 开源及第三方软件使用申请单 |
| 19 | 源代码 |
| 20 | 安全红线&隐私设计自检 |
| 21 | 安全测试策略 |
| 22 | 安全测试方案 |
| 23 | 安全测试用例 |

#### 出口准则

经过SDV测试，业务团队在经过测试后发现的所能发现的所有安全问题，在开发修改后，可以闭环，达到SDV测试结束的条件（无AB类安全红线问题遗留），可以结束SDV的安全测试。

## SIT安全测试策略

#### 测试重点

经过SDV的安全红线基线用例集覆盖测试，已经完成红线排查和和安全问题闭环。业务团队在SIT阶段测试的重点为核心代码走读，解读敏感接口的流程，对于算法的具体实现进行排查，这也是之前在线升级送测暴露的一些问题。

#### 入口准则

1.SDV安全测试结束。

2.发现的安全问题闭环，无AB类安全红线问题遗留。

#### 出口准则

1.完成SIT制定的测试工作和测试用例。

2.发现的问题闭环，无AB类安全红线问题遗留，无CVSS打分大于7分的严重级别问题遗留。

# 参考资料清单

## Web安全测试规范

## 