**华为技术有限公司**

**华为**

**安全深度测评报告**

**北京长亭科技有限公司**

**2020年11月30日**

**版权声明**

**本报告中出现的全部文字、图表、流程、方法、程序码、文档格式、截屏贴图等内容，除另有特别注明，版权均属华为技术有限公司与北京长亭科技有限公司所有，受有关产权及版权法保护。任何机构、单位、个人未经华为技术有限公司与北京长亭科技有限公司的书面授权许可，不得用任何方式或理由复制、引用本报告的任何片段。**

**特此郑重法律声明！**

**本报告为商业机密，未经授权请勿传播**

**目录**

[1.服务摘要 4](#__RefHeading___Toc641_1990131375)

[2.华为安全评测概述 6](#__RefHeading___Toc643_1990131375)

[2.1.测试流程 6](#__RefHeading___Toc645_1990131375)

[2.2.测试人员 6](#__RefHeading___Toc647_1990131375)

[2.3.测试风险管理 6](#__RefHeading___Toc649_1990131375)

[2.4.安全深度检测结论 10](#__RefHeading___Toc651_1990131375)

[3.测试范围与环境 10](#__RefHeading___Toc653_1990131375)

[4.安全威胁详情 11](#__RefHeading___Toc655_1990131375)

[4.1.a（高危） 11](#__RefHeading___Toc657_1990131375)

[5.安全状况评估 12](#__RefHeading___Toc659_1990131375)

[6.安全建议汇总 13](#__RefHeading___Toc661_1990131375)

[7.致谢 13](#__RefHeading___Toc663_1990131375)

# 服务摘要

经过华为技术有限公司关于华为项目安全深度检测授权，北京长亭科技有限公司安全服务组在 2020年11月16日 至 2020年11月30日（非业务高峰时段），对华为技术有限公司协议中限定的受测范围进行了安全检测。测试过程严格按照合同中规定的测试范围进行。

本次测试项目负责人:**杨坤**，邮箱： **kun.yang@chaitin.com**。

本次安全深度检测共发现漏洞 高危1个 ：

* a [等级：高危]

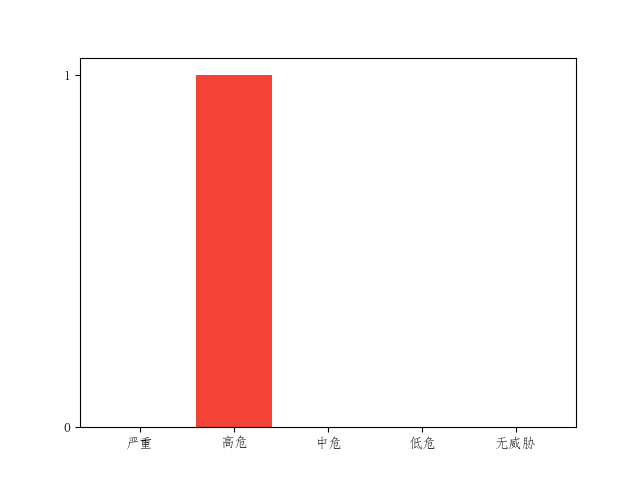


图 1：漏洞统计

\*参考标准如下表所示：

表 1：测试参考标准

|  |  |
| --- | --- |
| 参考标准 | * OWASP Top 10 Application Security Risks - 2010 * OWASP Top 10 - 2013 The Ten Most Critical Web Application Security Risks * GB/T 17859-1999 计算机信息系统安全保护等级划分准则 * GB/T 18336.1-2015 信息技术 安全技术 信息技术安全评估准则 第1部分:简介和一般模型 * GB/T 18336.2-2015 信息技术 安全技术 信息技术安全评估准则 第2部分:安全功能组件 * GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件 * GB/T 19716-2005 信息技术 信息安全管理实用规则 * GB/T 20984-2007 信息安全技术 信息安全风险评估规范 * GB/T 20988-2007 信息系统灾难恢复规范 * GB/Z 20986-2007 信息安全事件分类分级指南 * GB/T 20984-2007 信息安全技术 信息安全风险评估规范 * ISO/IEC PDTR 19791: 2004 信息技术-安全技术-运行系统安全评估 * ISO/IEC 13335-1: 2004 信息技术-安全技术-信息技术安全管理指南 * ISO/IEC TR 15443-1: 2005 信息技术安全保障框架 * ISO/IEC 27001:2005 信息技术-安全技术-信息系统规范与使用指南 * OWASP Risk Rating Methodology |

# 华为安全评测概述

本次安全检测工作由北京长亭科技有限公司 安全服务组在确保测试细节无泄漏、正常业务无干扰的状态下独立完成。工作组通过模拟黑客真实入侵过程，并结合测试技术（标准）对协议范围目标进行安全检测，以发现目标网站、应用系统中存在的安全漏洞及安全隐患。

## 测试流程

1. 取得授权
2. 信息的搜集与整理（企业网络布局、员工资料、企业资料）
3. 应用漏洞测试、人员安全意识测试
4. 结合点的测试结果进行广度深度测试
5. 对深入过程中获得的新信息进行下一轮测试
6. 结合结果进行危害总结
7. 输出报告



图 2：安全测评流程图

## 测试人员

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名 | 联系方式 | 出口IP地址 | 备注 |
| 张天力 | tianli.zhang@chaitin.com | 0.0.0.0 | 代码审计 |

## 测试风险管理

北京长亭科技有限公司安全服务组在信息搜集和整理的环节会优先考虑受测网站或程序的基本参数，以便在安全检测过程中尽可能减少对受测网站或程序的压力，保证其安全、稳定的运转；除此之外，还通过以下方式方法对测试风险进行合理管控。

### 测试时间规划

北京长亭科技有限公司安全服务组会在安全检测开始前与对方项目负责人充分沟通，搜集并整理出受测网站或程序的负荷分布，并规划测试时间，避开运转高峰时段，确保业务流程不受影响，尽可能减小对受测目标的压力。

### 流程监控制度

为了防止测试过程中出现意外，安全服务组会在每一项测试前预估多种可能后果，对于可能产生不良后果的测试（如：任意命令执行等）将被记录并跳过，在与对方项目负责人沟通协商后决定是否进行此项测试，以及测试方法。

此外，安全服务组会在测试过程中随时关注受测网站或程序的负荷信息，以确保在异常状况发生时，及时停止测试并与相关负责人联络。

### 测试工具使用

为了保证检测的完整性，安全服务组的部分安全检测可能使用自动扫描工具，当使用自动扫描工具扫描时，会通过对线程、插件数量等参数的设置，尽可能减小对受测目标的系统压力；此外，类似远程溢出攻击类、拒绝服务攻击类等有可能对受测网站或系统产生不良影响的也会排除。

注：本次安全测试服务不包括对备份系统的测试，如有相关需求，请在深度测试服务之前提出。

### 漏洞类型与检测方法

\*检测漏洞类型与检测方法如下表所示：

表 2：漏洞类型与检测方法

|  |  |  |
| --- | --- | --- |
| 漏洞类型 | 检测方法 | 漏洞危害 |
| XSS | 通过对交互点传入危险标签和闭合符号，结合前端内容判断XSS漏洞是否存在。 | XSS可以在访问了被插入XSS页面的用户的浏览器上执行js，从而进行一系列的操作。常见的攻击方式主要是利用XSS盗取用户身份，进一步获取权限，甚至利用高级攻击技巧直接攻击企业内网。 |
| 权限越权 | 通过对相关参数进行更改，测试返回内容是否有区别，能否获得本账户不该获取的数据、权限。 | 获取其他用户的数据，修改其他用户的信息，乃至直接获取管理员权限从而可以对整个网站的数据进行操作。 |
| CSRF | 通过对功能逻辑点进行测试，抓取请求包分析参数，结合不同的用户测试结果，判断 CSRF 是否存在。 | CSRF 可以实现在其不知情的情况下转移用户资金、发送邮件等功能逻辑操作。但是如果受害者是一个具有管理员权限的用户时 CSRF 则可能威胁到整个Web系统的安全。 |
| SSRF | 通过对网站获取远程连接信息等交互点进行测试，对回显信息进行判断是否存在SSRF。 | SSRF由攻击者构造形成由服务端发起请求的一个安全漏洞。一般情况下，SSRF攻击的目标是从外网无法访问的内部系统，直接导致影响企业内网安全。 |
| 敏感信息泄漏 | 通过对各个交互点，敏感目录和文件进行fuzz，对返回信息进行判断。 | 获取泄漏的服务器，web应用等相关敏感信息，进一步为后续渗透收集信息。 |
| SQL注入 | 按照可显注入、报错注入、盲注的方式检测，通过添加‘,",+,and,or,xor等闭合符号，逻辑字符判断SQL注入漏洞是否存在。 | 攻击者利用SQL注入漏洞，可以获取数据库中的多种信息（例如：管理员后台密码），从而脱取数据库中内容（脱库）。在特别情况下还可以修改数据库内容或者插入内容到数据库，如果数据库权限分配存在问题，或者数据库本身存在缺陷，那么攻击者可以通过SQL注入漏洞直接获取webshell或者服务器系统权限。 |
| 文件上传 | 通过白盒或黑盒的方式，对文件上传的功能点进行请求截断，插入恶意字符，修改文件后缀等方式，以落写上传任意后缀文件，拿到 webshell。 | 文件上传攻击被利用于上传可执行文件、脚本到服务器上，进而进一步导致服务器沦陷。 |
| 代码注入 | 通过白盒或黑盒的方式，对可能将字符串转为代码执行的功能点进行截断，注入字符等方式以执行攻击者精心构造的恶意代码。 | 代码注入攻击可以使攻击者直接执行任意代码，远程获取服务器代码执行权限甚至直接获取服务器系统权限。 |
| 命令注入 | 通过白盒或黑盒的方式，对可能调用外部命令，程序，将用户输入作为系统命令参数拼接的功能点进行截断，注入字符等方式以执行攻击者精心构造的恶意命令。 | 命令执行攻击可以使攻击者直接执行任意命令，读写文件，远程获取服务器系统权限。 |
| 运维不当 | 针对测试目标使用的服务，中间件，系统进行测试，获取运维信息或其他配置文件。 | 获取到系统，服务，中间件敏感信息，甚至有可能直接拿到系统权限。 |
| XXE | 发送包含有恶意的参数实体和内部实体XML请求，观察服务端是否返回相应数据或在外网监听相应端口，查看服务器是否会解析XML回连至外网服务器。 | 通过构造恶意XML实体，可导致读取任意文件、执行系统命令、探测内网端口、攻击内网网站等危害。 |
| 弱口令 | 通过对员工账户进行大数据分析和构造密码暴破或撞库攻击。 | 获取员工权限，拿到网站管理或内部系统权限，对进一步渗透打下基础，甚至可能直接获取系统权限。 |
| 任意文件读取 | 对系统程序中实现下载文件的功能模块进行测试，可尝试使用“../”跳转绕过下载文件目录的限制，读取其他目录下的敏感文件。 | 任意文件读取漏洞能够读取服务器上任意的脚本代码、服务及系统的配置文件等敏感信息，造成企业代码与数据的泄漏，威胁主机安全。 |
| 文件包含(RFI/LFI) | 通过白盒或黑盒的方式，对可能使用$include,$require等函数的交互点进行测试，以判断是否执行攻击者文件中的代码。 | 文件包含攻击可以使攻击者执行外部恶意代码，以读写文件，获取服务器权限等。 |
| 逻辑缺陷 | 针对测试目标的业务场景，对业务进行测试，利用逻辑问题执行非预期的功能。 | 实现刷单、刷评论等恶意操作，或获取到系统，服务，中间件敏感信息，甚至有可能直接拿到系统权限。 |

## 安全深度检测结论

鉴于测试结果的严重性，为了保护用户数据、公司机密信息、华为项目的安全以及保证华为项目的服务正常运行，长亭科技建议贵公司对全局的安全问题进行深度全面评测并尽快修复漏洞。

# 测试范围与环境

依照华为技术有限公司与北京长亭科技有限公司关于安全深度评测的协议，本次网站或应用程序安全深度测试范围及环境如下表所示：

表 3：测试范围与环境说明

|  |  |
| --- | --- |
| 网站范围 | * 各类线上服务以及企业内部系统真实环境 |
| IP 范围 | 本次测试甲方（华为技术有限公司）未提供 IP 范围。由乙方（北京长亭科技有限公司）安全服务组技术人员通过技术手段获得。 |
| 服务器环境 | * 各类线上服务以及企业内部系统真实环境 |
| 测试账号 | 本次测试甲方（华为技术有限公司） 未提供测试帐号。由乙方（北京长亭科技有限公司）安全服务组技术人员通过技术手段获得。 |
| 其他 | 无 |

# 安全威胁详情

## a（高危）

### 检测点

|  |  |
| --- | --- |
| 涉及站点 | a |
| 漏洞路径 | a |
| 漏洞威胁 | 高危 |
| 漏洞类型 | SQL注入 |
| 业务功能描述 | a |

### 检测结果与漏洞证明

a

### 漏洞危害

* 通过专业的安全评估判断，如果被攻击者利用，可非法读取、篡改、添加、删除数据库中的数据；
* 通过专业的安全评估判断，如果被攻击者利用，可盗取用户、系统的各类敏感信息与数据；
* 通过专业的安全评估判断，如果被攻击者利用，可通过修改数据库来修改网页上的展示内容；
* 通过专业的安全评估判断，如果被攻击者利用，可非法添加、修改或删除账号，造成系统、用户损失；
* 通过专业的安全评估判断，如果被攻击者利用，可能导致远程代码执行；
* 通过专业的安全评估判断，如果被攻击者利用，可通过数据库提权获取服务器权限；

### 建议

* 使用正确完善的“白名单”或“黑名单”来进行恰当规范化的输入验证；
* 进行数据库操作时，使用开发程序的安全转义库转义特殊字符；
* SQL语句预编译和变量绑定；
* 严格检查参数的数据类型、数值与数据长度；

# 安全状况评估

长亭科技安全服务组对华为项目进行专业的安全深度评估，发现华为项目网络环境存在危害度极高的安全问题，这些安全问题可能导致结果评估如下：

* 如果受到恶意攻击，可能因为已存在的漏洞导致机密数据被窃取。,如果受到恶意攻击，可能因为已存在的漏洞导致核心业务数据被篡改，导致不可估量的经济损失。,如果受到恶意攻击，可能因为已存在的漏洞导致网页内容被随意篡改，甚至网站主页被篡改。,如果受到恶意攻击，可能因为已存在的漏洞导致网站服务器被控制，并被留下后门导致长期被入侵。,如果受到恶意攻击，可能因为已存在的漏洞导致企业内网被入侵，导致企业大量的网络数据被窃取，甚至企业的核心代码也存在被窃取的风险。

# 安全建议汇总

本次安全检测由北京长亭科技有限公司安全服务组独立完成，测试中发现华为项目中存在严重的安全隐患，测试详情和安全建议请参看报告内容。

鉴于测试结果的严重性，为保护用户数据、公司敏感信息，以及项目的安全运行，北京长亭科技有限公司安全服务组建议尽快修复安全问题，并做好安全管理工作，定期进行安全巡检，最大程度地避免安全问题。

# 致谢

在贵公司的大力配合下，本次安全深度检测得以顺利完成。北京长亭科技有限公司 安全服务组向华为技术有限公司所有参与并提供支持的部门及个人表示深深的感谢。

北京长亭科技有限公司

CEO 陈宇森