

XX系统

安全测试方案&报告

目 录

1. [项目概要 3](#_bookmark0)
   1. [项目背景 3](#_bookmark1)
   2. [项目目标 3](#_bookmark2)
   3. [项目原则 4](#_bookmark3)
2. [渗透测试技术方案介绍 5](#_bookmark4)
   1. [渗透测试原理 5](#_bookmark5)
   2. [渗透测试的必要性 5](#_bookmark6)
   3. [渗透测试的方法 5](#_bookmark7)
   4. [渗透测试流程 6](#_bookmark8)
   5. [渗透测试技术 8](#_bookmark9)
   6. [渗透测试工具 10](#_bookmark10)
3. [项目实施方案 11](#_bookmark11)
   1. [项目实施范围 11](#_bookmark12)
   2. [项目实施地点 11](#_bookmark13)
   3. [项目时间安排 11](#_bookmark14)
   4. [客户配合内容 12](#_bookmark15)
   5. [项目交付 12](#_bookmark16)
   6. [质量控制 12](#_bookmark17)
   7. [保密控制 13](#_bookmark18)
   8. [风险与应对措施 14](#_bookmark19)

# 项目概要

## 项目背景

信息安全已经成为金融企业业务支撑的重要一环，金融企业的 IT 应用是各种网络应用和金融业务的集成，为金融企业所有内外部用户提供方便的业务信息和应用共享。金融企业的 Web 业务平台已经在电子交易、金融信息化中得到广泛的应用，金融组织和机构都纷纷将其业务应用架设在 Web 平台上，为客户提供更为方便、快捷的金融服务支持。伴随着这种趋势，入侵者也将注意力从以往对传统网络服务器的攻击逐步转移到了对金融企业 Web 业务的攻击上。根据 Gartner 的调查，信息安全攻击有 75% 都是发生在

Web 应用层而非网络层面上。同时数据也显示，三分之二的主机和 Web 站点都相当脆弱和易受攻击。

融盛财产保险股份有限公司（以下简称“融盛保险”）将“超越保险”作为经营理念，定位于“互联网+”时代信息化、专业化、特色化的财产保险公司， 透过将互联网、大数据、人工智能技术与保险业务的充分融合，融盛保险将积极打造以客户价值创造为核心的全新互联网保险商业模式，努力寻找出保险业发展的新路径，为探索保险业转型发展之路做出应有的贡献，让客户实现由单纯的购买保险模式转变成对新生活方式的体验。

融盛有限公司（以下简称“融盛”）将根据[融盛财产保险股份有限公司](http://company.zhaopin.com/CC337840236.htm)（以下简称“融盛保险”）的渗透测试具体需求，采用国际/国内成熟、规范的测试方法和业界常用的测试工具对XX系统进行渗透性测试，以及时发现存在的安全问题和安全隐患， 提出详细及合理的改进建议和修复策略，为融盛保险业务系统的平稳运行提供更高质量的安全保障。

## 项目目标

针对本次项目，通过渗透测试的方式，不断发现和总结测试目标业务系统的网络、主机、应用系统中可能面临的各类安全风险，并

提出针对性的安全改进建议，提高目标系统的安全性。

## 项目原则

融盛在项目实施全过程将遵循以下项目原则：

规范性原则：

在项目实施过程中，融盛的工作团队采用规范、统一的标准化工作流程和工作方式；项目文档化遵循融盛保险的文档规范，文档的设计将依照国际、国内及行业内部的相关成熟标准和最佳实践。

可控性原则：

项目实施过程中所采用的工具、方法和过程要经融盛保险的认可，确保项目进度的推进，保证本次项目的可控性。

最小影响原则：

项目实施应尽可能小地影响业务系统的正常运行，不能对现有网络的运行和业务的正常运行产生显著影响(包括系统性能明显下降、网络拥塞、服务中断等)。

保密原则：

对服务过程中的过程数据和结果数据严格保密（甲乙双方将就此项目签署保密协议），未经授权不泄露给任何单位和个人，不利用此数据进行任何侵害融盛保险的行为。

# 渗透测试技术方案介绍

## 渗透测试原理

渗透测试主要依据 CVE 已经发现的安全漏洞，模拟入侵者的攻击方法对网站应用、服务器系统和网络设备进行非破坏性质的安全性测试。

## 渗透测试的必要性

融盛在渗透测试过程中将按照融盛保险的要求，利用各种业内安全扫描器和富有经验的安全测试工程师的人工技术经验对客户的业务系统进行非破坏性质的模拟入侵攻击，最终目的是侵入系统、获取机密信息并将入侵的过程和细节产生报告给用户。由此确定用户业务系统所存在的安全威胁， 并能及时提醒客户完善安全策略，降低安全风险。

人工渗透测试可以作为自动化工具扫描的补充。虽然安全工具扫描具有很好的效率和速度，但是存在一定的误报率，不能发现高层次、复杂的安全问题；渗透测试需要对测试者的专业技能要求很高（渗透测试报告的价值直接依赖于测试者的专业机能），但是非常准确，可以发现逻辑性更强、更深层次的弱点。

## 渗透测试的方法

黑箱测试

黑箱测试又被称为所谓的“zero-knowledge testing”，渗透者完全处于对系统一无所知的状态，通常这类型测试，最初的信息获取来自于 DNS、Web、

Email 及各种公开对外的服务器。白盒测试

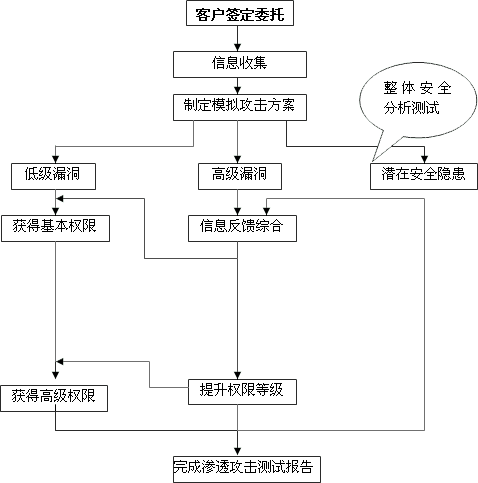
白盒测试与黑箱测试恰恰相反，测试者可以通过正常渠道向被测单位取得各种资料，包括网络拓扑、员工资料甚至网站或其它程序的代码片断，也能够与单位的其它员工（销售、程序员、管理者……）进行面对面的沟通。

这类测试的目的是模拟企业内部雇员的越权操作。隐秘测试

隐秘测试是对被测单位而言的，通常情况下，接受渗透测试的单位网络管理部门会收到通知：在某些时段进行测试。因此能够监测网络中出现的变化。但隐秘测试则被测单位也仅有极少数人知晓测试的存在，因此能够有效地检验单位中的信息安全事件监控、响应、恢复做得是否到位。

## 渗透测试流程

* + 1. 渗透测试流程



* + 1. 客户委托

客户委托是进行渗透测试的必要条件。Xx公司将努力做到融盛保险对渗透测试所有细节和风险的知晓、所有过程都在融盛保险的控制下进行。这也是专业服务与入侵者攻击入侵的本质不同。

* + 1. 信息收集

信息收集分析是所有入侵测试的前提和基础。“知己知彼，百战不殆”，信息收集分析就是完成的这个任务。通过信息收集分析，详细了解渗透测试目标的全面信息，为下一步模拟攻击方案提供依据。

* + 1. 制定模拟攻击方案

根据信息收集过程获取的网络及应用系统信息，可确定对应用系统的攻击面及安全风险点，制定下一步的模拟攻击方案。

* + 1. 漏洞利用与权限提升

通过收集的信息和分析，存在两种可能性，其一是目标系统存在重大弱点：测试者可以直接控制目标系统，这时测试者可以直接调查目标系统中的弱点分布、原因，形成最终的测试报告；其二是目标系统没有远程重大弱点， 但是可以获得远程普通权限，然后通过该普通权限进一步收集目标系统信息。

* + 1. 完成渗透攻击测试报告

整理渗透测试过程中发现的安全漏洞，确定风险等级，根据客户网络及业务系统的实际情况提供可行的修复建议并整理成渗透攻击测试报告。

## 渗透测试技术

* + 1. 信息收集

信息收集的方法包括 DNS 信息查询、Whois 信息查询、网络扫描、主机扫描、操作系统类型判别、WEB 应用判别、账号扫描等。

信息收集过程主要包括：

网络信息收集：在这一步还不会直接对渗透测试目标进行扫描，会先从网络上搜索一些相关信息，包括 Google Hacking，Whois 查询，DNS 等信息。

目标系统信息收集：通过上面的一步，可以简单的描绘出目标系统的网络结构，如公司网络所在区域，公司 IP 地址分布，VPN 接入地址等。从获取的地址列表中进行系统判断，了解其组织架构及操作系统使用情况。

端口**/**服务信息收集：信息收集的方法包括主机网络扫描、端口扫描、操作类型判别、应用判别、账号扫描、配置判别等等，通过端口及服务信息搜集可以获取 WEB 应用服务情况、数据库信息和应用站点结构信息。

* + 1. 口令猜解测试

常见的操作系统及应用系统均使用帐号口令的认证方式，因此，在渗透测试过程中，对用户口令的猜解测试也是一个重要的工作环节，融盛在渗透测试过程中，将根据系统的不同，通过暴力破解的方法可进行包括

SMB、TELNET、SSH、FTP、MySQL、Oracle、HTTP 等口令猜解测试。

* + 1. 溢出攻击测试

溢出攻击的测试过程中，测试人员将根据收集的信息以确认应用或系统的版本，从而判断在当前应用或系统上是否存在已知溢出漏洞和可利用的攻击程序，同时，测试人员会在攻击程序对系统的稳定运行不产生影响的前提下使用攻击程序发起溢出攻击，直接获取系统或应用程序的权限。

* + 1. **Web** 安全测试

在金融业务系统中，WEB 应用通常是根据业务需求进行的定制性开发， 区别与传统的网络设备或操作系统，定制开发的 Web 系统更容易存在由于开发人员技术不规范导致的安全漏洞，融盛也将参考 OWASP 组织定义的 TOP10 应用安全风险对目标业务系统进行全面的安全测试。

Web 安全测试主要内容如下： 身份鉴别及管理测试：

测试系统登陆身份管理功能，包括注册过程测试、账户枚举测试、测试是否存在可猜测用户名、突破用户名注册规则等安全问题。

认证及授权测试：

检查系统登陆认证过程，检查是否存在弱口令、认证绕过、任意密码重置及密码策略绕过、密码暴力破解等安全问题。

检查应用系统授权管理过程，是否存在授权绕过、水平权限提升、垂直权限提示等安全问题。

会话管理测试：

检查应用系统会话管理机制，查看是否存在会话无超时、会话令牌泄露、

CSRF、会话绕过等安全问题。应用安全配置：

检查应用系统的相关配置，测试是否存在默认参数、默认路径、目录遍历、错误的 HTTP 头配置以及包含敏感信息的错误页面导致的信息泄露等安全问题。

输入输出验证测试：

检查应用系统各数据输入输出功能，测试是否存在 XSS 跨站脚本漏洞、

SQL 注入漏洞、LDAP 注入漏洞、代码注入漏洞、命令注入漏洞、文件上传漏洞等安全问题。

**XML** 外部实体测试：

检查应用系统 XML 文件中的外部实体引用，测试是否存在利用外部实体窃取使用 URI 文件处理器的内部文件和共享文件、监听端口、执行远程代码和实施拒绝服务的安全问题。

反序列化测试：

检查应用系统是否存在不安全的反序列化问题，测试是否存在可利用反序列化缺陷进行远程代码执行的安全问题。

数据传输安全测试：

检查数据传输机制，使用的协议，测试是否存在敏感数据未加密传输、未加密存储等安全问题。

不安全的组件测试：

检查应用系统是否使用存在已知漏洞的库文件、框架或第三方软件模块。功能逻辑测试：

检查系统处理逻辑情况，测试是否存在控制功能逻辑可绕过的问题。

* + 1. 权限提升及持续访问

根据模拟攻击方案进行测试后，检查系统是否存在可导致获取应用系统操作系统级权限及持续保留该权限的安全问题。

* + 1. 其他测试

除了以上的攻击技术、在渗透测试中还会根据实际情况并结合个人经验进行其他的安全测试，以全面检测业务系统的安全性。

2.6 渗透测试工具

|  |  |
| --- | --- |
| 工具类别 | 工具名称 |
| 信息搜集工具 | Nslookup、Whois、Tracert、Dirbuster、Dirbuster |
| 网络扫描及分析工具 | Nmap，Zenmap、Wireshark |
| 主机漏洞扫描工具 | Tenable Nessus、OpenVAS |
| WEB 漏洞扫描及分析工具 | Awvs、BurpSuite、SQLMap、Arachni、 |

|  |  |
| --- | --- |
| 密码破解工具 | John the Ripper、L0pht Crack、hydra、pwdump |
| 漏洞利用工具及平台 | Metasploit，Kali、其他专用漏洞利用工具 |

# 项目实施方案

## 项目实施范围

本次渗透测试范围为XX业务系统及相关的应用程序、数据库及服务器系统等。

具体测试目标如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 访问地址 | 说明 |
| 1 |  | 系统前端访问地址 |
| 2 |  | 系统后端访问地址 |

## 项目实施地点

本次渗透测试实施地点在融盛大连河口园区，通过 VPN 远程访问被测系统。

## 项目时间安排(**可根据实际计划修改**)

本次项目共分两期实施，每期实施时间安排如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 阶段 | 计划完成日期 | 内容 | 可交付文档 |
| 项目启动会 | 1 个工作日 | 项目启动、测试目标信息沟通、实施计划确定以及资源确定、签署保  密协议等 | 《项目启动会会议记录》 |
| 测试方案评审 | 1 个工作日 | 评审安全测试方案 | 《安全测试方案评审记录》 |
| 渗透测试项目实施 | 4 个工作日 | 对目标系统进行渗透  测试实施。 |  |
| 渗透测试报告初稿整理 | 1 个工作日 | 对各个信息系统渗透测试的结果进行数据  分析，确认问题并整理 | 《渗透测试报告初稿》 |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | 报告初稿。 |  |
| 渗透测试报告沟通 | 1 个工作日 | 就测试结果与客户沟  通交流，确定测结果。 | 《会议记录》 |
| 渗透测试的报告终  稿整理 | 0.5 工作日 | 整理完善渗透测试报  告终稿。 | 《渗透测试报告终稿》 |
| 项目验收总结会 | 0.5 工作日 | 提交报告，项目验收 | 《项目总结会会议记录》 |

## 客户配合内容

本次测试需要融盛保险协助准备和配合事宜如下： 测试工位，可直接通过网络接入到相应的测试系统； 目标系统测试帐号；

系统管理员、系统核心维护人员、软件开发人员等需要及时配合，提供相关人员联系方式表；

其他与测试相关的未尽事宜可当面协商解决。

## 项目交付

通过本次渗透测试项目，融盛将为融盛保险交付以下成果：

* + - 项目会议纪要
    - 渗透测试的过程记录包括测试文件、扫描报告等
    - 《XX系统渗透测试报告》

本报告将详细记录本次渗透测试的过程、方法、发现的安全漏洞详细信息包括测试过程、使用的技术方法、漏洞影响及风险等级、修复建议，整体安全分析及安全改善建议等内容。

## 质量控制

为确保安全服务的过程与预先定义的项目方案和技术规范是一致的，保证测试质量，融盛在项目实施过程中会保存全部测试过程记录，通过对操作记录的审查核对测试内容及发现实施过程与标准的偏离。

## 保密控制

为保障融盛保险的信息保密工作，通过如下控制措施加强风险保密工作。

* + 1. 保密承诺

所有参与融盛保险项目的融盛技术顾问都要签订《保密承诺》。

* + 1. 场地环境项目期间内的风险保密管理规定

所有进入融盛保险工作场地的融盛项目实施人员，均应遵守双方协定风险保密规定。确保在场地环境内信息的安全传递。同时，在远程进行测试的融盛项目实施人员也要保证物理环境的安全，防止通过其他渠道导致客户信息的泄露。

* + 1. 文档材料的风险管理办法

对需要融盛保险提供的文档资料，融盛项目经理提交《文档调用单》给融盛保险接口人，融盛保险在调用单规定期限内提供要求的文档资料。

文档调用单上，明确文档申请人，文档使用人员等涉及此文档的人员。对纸质文档，统一保管在指定的文件柜里。使用完后返还给融盛保险，

并填写《文档调用单》的交回部分。

电子文档传递通过融盛保险接口人指定的 U 盘，保存在文档申请人及使用人员的笔记本上或指定的计算机上。

* + 1. 离场及项目结束的风险管理办法

融盛项目组在项目离场时，笔记本交由融盛保险专人清理后方可带出。所有本地提供的纸质文档，在项目结束的事后，都要返给提供方，并填写《文档调用单》的交回部分。

* + 1. 例外情况

遇到未列明的涉及保密方面的例外情况，双方就个案单独洽谈，由项目领导小组签字确认。

## 风险与应对措施

## 时间选择

为减轻渗透测试对网络和主机的影响，渗透测试时间尽量安排在业务量不大的时段或晚上。

* + 1. 系统备份策略

为防止在渗透测试过程中出现的异常的情况，所有被评估系统均应在被评估之前作一次完整的系统备份或者关闭正在进行的操作，以便在系统发生灾难后及时恢复。

* + 1. 系统恢复策略

在渗透测试过程中，如果出现被评估系统没有响应或中断的情况，应当立即停止测试工作，与客户方配合人员一起分析情况，在确定原因后，及时恢复系统， 并采取必要的预防措施（比如调整测试策略）之后，确保对系统无影响， 并经客户方同意之后才可继续进行。

* + 1. 过程监控

在每一次系统渗透测试前，安全测试人员都会告知被测试系统管理员，并且在测试过程中会随时关注目标系统的负荷等信息，一旦出现任何异常，将会停止测试。

1. 渗透测试结果及整改建议

渗透测试问题汇总表：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 漏洞分类 | 漏洞名称 | 风险等级 |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |

；

* 1. 业务安全：

**详细阐述每个漏洞的风险等级，漏洞详细描述（附带截图），破解方法（附带截图），修复建议**

1. 测试总结

针对本次测试发现的高危问题进行总结，评估风险等级，提出安全加固方案