外部机构互联网安全渗透性测试指南

# 一、定义

渗透测试（Penetration Testing），是通过模拟恶意黑客的攻击方法，来评估计算机系统安全的一种评估方法。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析，这个分析是从一个攻击者的角度来进行的，并且从这个角度有条件主动的利用安全漏洞。

# 二、测试目标

渗透测试的目的在于通过使用各种已知的漏洞识别手段，充分挖掘网络层、系统层、应用层乃至业务逻辑层中可能存在且可被利用的潜在风险点，验证现有安全防御体系的有效性，在不影响业务系统正常运行的情况下，尽可能多的发现系统脆弱的环节，让系统管理人员能够直观的了解到系统面临的安全威胁。充分提高业务系统的健壮性和可靠性，加强系统管理人员的安全防范意识。

# 三、测试类型

渗透测试可分为两种基本类型：黑盒测试和白盒测试。

## 3.1 黑盒测试

黑盒测试（Black-box Testing）也被称为外部测试（External Testing）。渗透测试团队将从一个外部网络位置来评估目标业务系统，并没有任何目标网络内部拓扑等相关信息，完全模拟真实网络环境中的外部攻击者，有组织有步骤的对目标进行逐步的渗透和入侵，揭示目标系统中已知或者未知的安全漏洞，并评估这些漏洞是否能被利用以获取系统控制权或者造成业务资产等的损失。

## 3.2 白盒测试

白盒测试（White-box Testing）也被称为内部测试（Internal Testing）。进行白盒测试的团队将可以了解到关于目标环境的内部和底层知识，因此这可以让渗透测试团队以最小的代价发现和验证系统中最严重的安全漏洞。如果实施到位，白盒测试能够比黑盒测试发现更多的目标系统中存在的安全漏洞和弱点。

# 四、测试原则

在渗透测试期间，应确保测试工作不会对业务系统的运行造成影响，不会对业务系统本身造成危害和损失。

## 3.1 时间的选择

针对任何网站平台的渗透测试工作，均需在授权时间范围内进行。对于实时交易类、门户类的网站平台的测试工作应在非业务高峰期进行，以免对系统业务造成影响和损失。其他网站平台的测试工作，因视系统业务的不同，而选择合适的时间进行测试。

## 3.2 工具的选择

渗透测试过程中所使用的工具有多种来源，如：商业性安全测试工具、开源的安全测试工具、渗透测试工程师自己编写的小工具或脚本程序、测试机构自己开发的非公开测试工具等。

对于授权进行的渗透测试，所使用的工具不应给测试目标引入病毒、蠕虫或木马等恶意程序，不会给目标系统造成不必要的损失或带来潜在的安全隐患。

## 3.3 方法的选择

在渗透测试工作中，应选择不会对业务系统运行造成影响的方法进行测试。针对生产环境的测试不使用扫描工具，仅以低频手工测试加自动化辅助验证方法进行测试。

为防止渗透测试工作造成网络拥堵、服务器宕机、业务中断等后果，在渗透测试过程中不应使用包含DDOS攻击、CC攻击等压力性渗透测试方法。

为防止渗透测试工作造成程序运行失败、系统宕机、系统重启等不良后果，不应在生产环境中对缓冲区溢出类的漏洞进行验证。

# 五、测试分工

在开始渗透测试工作前，组织方应提前和系统平台主管单位、开发单位、运维单位和测试机构进行沟通协调，确定渗透测试范围、时间，明确在测试工作中各方职责。

组织方：选择测试机构，协调测试范围和测试时间，跟进测试进度，协调测试期间各项工作，组织漏洞修复，提供漏洞修复建议，了解漏洞修复进度，安排漏洞复测。

业务主管单位：协助组织协调测试工作，提供测试范围，选定测试时间，了解测试情况，跟进漏洞修复进度，参与应急处置工作。

开发单位：了解测试情况，负责应用等漏洞修复工作，了解漏洞复测情况，参与应急处置工作。

运维单位：协助确定测试时间，负责系统、应用、数据备份工作，加强监控系统性能和系统异常情况，及时进行应急工作，及时通报系统异常情况，根据本单位职责负责操作系统等漏洞修复工作，根据测试报告删除测试过程中上传的测试文件。

测试机构：提供测试方案，组织测试工作，提供发现问题清单以及测试文件的上传地址，提供漏洞修复建议，进行漏洞复测。

# 六、测试准备与授权

组织方在跟各相关单位协调沟通好测试的范围、内容和各自分工后，应当和测试机构就测试过程中的注意事项进行明确，具体要求见第十部分。

在准备阶段的相关内容都已经确认无误的情况下，可对测试机构进行授权，开始渗透测试工作。

# 七、测试实施

## 5.1 SQL注入测试

**漏洞描述**：SQL注入漏洞是目前针对WEB服务最危险、且攻击成本最低的漏洞之一。攻击者可以通过构建巧妙的URL请求来获得服务器后台运行的数据库数据，包括用户名、密码、权限、网页数据、资料等，更甚至可以构建URL来修改数据、删除数据、创建远程可控制的cmd、shell、木马等。目前最常见的攻击方法就是修改某用户ID的权限至管理员和修改网页数据。

## 5.2 跨站脚本测试

**漏洞描述**：跨站脚本攻击是通过在网页中加入恶意代码，当访问者浏览网页时恶意代码会被执行或者通过给管理员发信息的方式诱使管理员浏览，从而获得管理员权限，控制整个网站。攻击者利用跨站请求伪造能够轻松地强迫用户的浏览器发出非故意的HTTP请求，如诈骗性的电汇请求、修改口令和下载非法的内容等请求。

## 5.3 认证会话管理测试

**漏洞描述**：攻击者通过窃听正常用户访问页面时提交的用户名和密码以及认证令牌，从而冒充用户进行正常访问的过程。

## 5.4 弱口令类测试

**漏洞描述**：登录口令使用常用的单词、数字等组合。密码猜测是攻击者最常用的手段之一，此类攻击是专门针对弱口令的。攻击者会构建一份密码本表，其中包含非常多的弱口令，利用计算机程序自动进行循环尝试登录，可以非常轻易的破解出存在弱口令的认证。

## 5.5 信息未加密类测试

**漏洞描述**：在系统的开发、部署过程中，由于某些需求或是开发设计存在安全漏洞，往往会造成机密数据的安全得不到保障，常见的不安全的数据存储包括：未能识别全部的机密数据；对某个机密数据未能识别其所有的存放地；机密数据未加密或加密强度不足等，其造成的后果是极为严重的。

## 5.6 文件包含类测试

**漏洞描述**：本地文件包含漏洞，是攻击者通过构建精妙的URL请求来获得服务器的重要文件，而恶意用户的目标很可能就是存储着重要信息的文件，如用户名密码shadow文件、init.d配置文件、安全策略文件等。得到此类文件后攻击者可以通过暴力破解、逆向工程等手段得到管理员密码以及计算机脆弱点等信息，从而可以为进一步渗透服务器提供可能。

## 5.7 目录浏览类测试

**漏洞描述**：利用存在该漏洞的URL，通过返回上一级目录的方式进行目录改变，就可以越权访问到其它文件夹下的内容。

## 5.8 不安全的URL访问类测试

**漏洞描述**：一个已经授权的用户，通过更改访问时的一个参数，从而访问到了原本其并没有得到授权的对象。Web应用往往在生产Web页面时会用它的真实名字，且不会对所有的目标对象访问时来检查用户权限，所以这就造成了不安全的对象直接引用的安全漏洞。重定向所引向的目的是带有用户输入参数的目的URL，而如果这些重定向未被验证，那么攻击者就可以引导用户访问他们所要用户访问的站点。

## 5.9 信息泄露类测试

**漏洞描述**：在默认安装模式下，许多Web服务器和应用程序服务器都提供了样本应用程序和文件，以便开发者测试安装之后服务器是否能正常运行。默认安装页面可被远程访问，是信息泄露类型漏洞的一种，他为攻击者提供了Web服务的部分信息，其中包含了版本、模块组件等。通过这些信息，可以利用其相关的漏洞或者脆弱性进行攻击。

目录遍历是信息泄露的一种，它为攻击者提供了某目录下所有可见文件的列表。但由于访问可见文件仍是受到权限控制的，所以泄露出的信息并不是直接的、严重的。但如果列表下有未设置权限的文件，或是存在敏感信息的文件，这就成为了攻击者最大攻击点。

## 5.10 文件上传类测试

**漏洞描述**：文件上传测试测试面向的是允许上传，并可以下载上传文件的网页服务，测试主要检查服务器对上传文件的处理、放置和检查。避免服务器执行恶意文件或散播，同时也避免用户上传过滤不严格的超大文件等安全隐患。

## 5.11 未授权访问类测试

**漏洞描述**：攻击者可利用该漏洞绕过登录认证限制，查看诸如后台管理、账户信息等需要授权才能访问的内容。

# 八、测试中的影响及应对措施

## 8.1 针对SQL注入测试

**测试影响**：

测试人员通过自动化工具或手工编写SQL语句方式，构造特殊的SQL代码传入到应用程序中，从而通过执行非设计预期的SQL代码，达到窃取数据或破坏的目的。由于需要对被测系统的所有动态页面进行尝试，具体工作量将视被测系统的动态页面数量确定。测试期间将会提交大量查询语句对后台数据库进行直接操作，由于采用的是黑盒测试方法，提交的查询量较大，且对数据库的影响存在较多不确定性，可能会造成数据库服务器宕机或数据回滚，影响业务的正常使用。

**应对措施**：

需要在测试前对数据库进行全量备份，测试期间应对业务系统以及数据库系统做好监控措施。

## 8.2 针对跨站脚本测试

**测试影响**：

测试人员利用自动化工具或手工编写Script脚本代码，将其提交到对被测系统的每个动态页面上，通过返回信息判断其是否存在跨站脚本漏洞。由于该测试采用黑盒方式，过程中产生大量对服务器的请求，并且工具向服务器端发送的带有跨站脚本攻击的数据存在一定程度的不确定性，可能会对服务器的正常访问造成一定影响。

**应对措施**：

需要在测试前做好系统、应用的备份工作，测试期间应对系统性能做好监控措施，如有出现数据库资源耗尽等情况及时通知测试人员暂停测试。并要求测试工程师在测试过程中做好记录工作，以便后期进行数据清除。

## 8.3 针对认证会话管理测试

**测试影响**：

在这个测试中，会检查Cookie与Session的令牌是否是由一种安全的、不可逆的方法生成。可预测的会话令牌会非常容易通过修改Cookie或Session的参数，进行会话劫持，并伪装成合法用户。令牌操纵测试主要面向于令牌的算法，分析其算法的强度和随机性。

**应对措施**：

测试期间应对业务系统做好监控措施。

## 8.4 针对弱口令类测试

**测试影响**：

此类测试主要针对的是密码设置或密码强度相对较弱而产生的漏洞。采用缺省密码，或使用比较简单的密码，都可以通过密码字典来进行尝试破解，而且成功率相对较高。其中，空口令的威胁更加严重，也是测试的重点。字典攻击主要针对基于HTML表单提交的验证方式进行的。

测试过程中可能会锁定某些重要用户账号，解锁时间根据系统设置而定，对该用户将会造成一定时间的业务中断，需要维护人员进行解锁操作。同时会在系统日志中产生大量登录失败日志造成服务器或应用程序报警。

**应对措施**：

维护人员对异常访问的日志进行监控，如出现重要账户锁定情况及时进行解锁操作恢复正常运行。

## 8.5 针对信息未加密类测试

**测试影响**：

低强度测试，不会对系统运行造成影响。

**应对措施**：

暂无。

## 8.6 针对文件包含类测试

**测试影响**：

通过构建精妙的URL请求，发送到服务器来获得未授权访问的文件。由于请求量比较大，可能会造成被测系统网络拥挤，页面响应时间较长，严重时可造成服务中断。

**应对措施**：

为保险起见可选择非业务高峰期进行该项测试。网站维护人员应全程监控网站运行状态和系统资源使用情况。

## 8.7 针对目录浏览类测试

**测试影响**：

测试人员可能会利用相关工具发现可能存在该漏洞的URL，之后通过构造特殊的URL请求，验证其准确性。在利用工具的过程中，可能会造成被测系统网络拥挤，页面响应时间较长，严重时可造成服务中断。

**应对措施**：

为保险起见可选择非业务高峰期进行该项测试。网站维护人员应全程监控网站运行状态和系统资源使用情况。

## 8.8 针对不安全的URL访问类测试

**测试影响**：

测试人员可能会利用相关工具发现可能存在该漏洞的URL，之后通过构造特殊的URL请求，验证其准确性。在利用工具的过程中，可能会造成被测系统网络拥挤，页面响应时间较长，严重时可造成服务中断。

**应对措施**：

为保险起见可选择非业务高峰期进行该项测试。网站维护人员应全程监控网站运行状态和系统资源使用情况。

## 8.9 信息泄露类测试

**测试影响**：

测试人员利用相应方法发现系统中个别组件模块的信息泄露问题，测试期间可能会对目标系统得应用服务产生一定的延时响应情况，尽量避免在业务高峰期进行测试。

**应对措施**：

为保险起见可选择非业务高峰期进行该项测试。网站维护人员应全程监控网站运行状态和系统资源使用情况。

## 8.10 针对文件上传类测试

**测试影响**：

测试人员上传的文件以及对文件的操作可能会对目标系统造成不确定的影响，如可能会覆盖已上传的文件、占用系统存储空间等。测试过程也可以选择上传控制类文件，用以验证整个系统的控制策略是否能阻止非法外联等情况，但这可能会给非法攻击者提供可利用的后门。

**应对措施**：

需要在测试前做好应用、数据的备份工作，并要求测试工程师在测试过程中做好记录工作，以便后期将上传的相关文件进行清除。

## 8.11 针对未授权访问类测试

**测试影响**：

由于要借助相应工具，可能会造成被测系统网络拥挤，页面响应时间较长，严重时可造成服务中断。

**应对措施**：

为保险起见可选择非业务高峰期进行该项测试。网站维护人员应全程监控网站运行状态和系统资源使用情况。

# 九、测试报告

测试报告的出具应当符合组织方的相关要求，若组织方没有特殊要求的，测试机构可自行出具测试报告。

如果测试机构在测试过程中发现严重问题，应及时汇报相关漏洞，并停止对该系统的继续测试，由组织方和主管单位沟通决定是否继续进行测试。

如果没有发现严重问题，应在每周对测试情况进行汇总，并将测试结果汇报给组织方。测试报告中的漏洞应经过验证真实有效，并且可以被实际利用。测试报告中的漏洞等级标准应符合《银联软硬件缺陷快速协作与处置机制》中的漏洞等级标准。

# 十、对外部测试机构的要求

1、禁止向第三方平台（如360补天、漏洞盒子、漏洞银行等）提交任何与测试项目相关的漏洞。

2、禁止向项目组以外的人员泄露相关测试信息，包括测试项目名称、测试范围、测试结果等信息。

3、禁止对系统使用拒绝服务攻击类、缓冲区溢出攻击类等危害较大的测试方法进行测试。

4、禁止在未授权情况下，使用扫描工具对生产业务系统进行扫描。

5、禁止对授权范围以外的系统进行测试，若在测试过程中涉及到业务相关性的其他系统，需和组织方进行沟通。

6、禁止在非授权时间范围内进行测试。

7、禁止使用所提交IP端以外的IP地址进行测试。

8、测试仅限于确定漏洞的存在，禁止利用漏洞获取客户的生产数据。

9、测试类上传文件大小应控制在1MB以内，如成功上传，应在测试报告中给出明确上传地址，便于运维人员进行删除。