**安全检测范围确认单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **主机检测范围表** | | | | |
| **序号** | **主机地址** | **主机操作系统** | **端口与端口开放的服务** | **要求** |
|  |  |  |  | **主机扫描相关**：主机、中间件、数据库等所有生产环境ip地址可以ping通主机漏洞扫系统地址10.238.103.13（针对此地址全端口开放）  Ps：如果不通请申请开通防火墙策略。 |
|  |  |
|  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **应用系统检测范围表** | | | | |
| **子系统名称** | **部署环境** | **访问地址** | **帐户名/密码** | **要求** |
| 子系统1  （多系统请自行添加） | 测试环境 |  |  | 测试环境地址可以ping通   |  | | --- | | 10.3.111.223 | | 10.3.111.225 | | 10.3.111.226 | | 10.3.111.229 | | 10.3.111.230 | | 10.3.111.231  10.3.111.232  10.3.111.233 |   10.246.162.185  10.246.162.186  10.246.162.187  10.246.162.189  Ps：如果不通请申请开通两个段的防火墙策略。 |
| 正式环境 |  |  |  |
| 检查条件准备 | 测试环境登陆口，请关闭验证码机制或提供一个写成固定验证码的账户。 | | | |

|  |  |  |
| --- | --- | --- |
| **基础配置检测范围表** | | |
| 1 | 安全检查申请表中提交web容器类型及版本（例如Apache tomcat、IIS、Weblogic、Apache等） |  |
| 2 | 开发时使用的语言 |  |
| 3 | 网站基础框架 |  |
| 4 | 数据库类型及版本（例如sql server、mysql、oracle等） |  |
| 5 | 安全检查申请表中说明登录口使用的登录方式（例如自研、AD域、统一身份认证） |  |
| 6 | 说明系统支持的浏览器类型（ie7、火狐、goog le等） |  |
| 7 | 请提供网络拓扑图，若没有请详细说明测试涉及到的所有主机所在的区域（例如内网，DMZ，外网等） |  |

|  |  |  |
| --- | --- | --- |
| **App检测准备表（ps：没有app检测的不填）** | | |
| 1 | 请提供无waf、ids、ips防护的服务器，app部署在此服务器上。（或者开通外界防火墙策略，允许10.3.37.0/24访问） | 如果不能访问，请申请开通防火墙策略 |
| 2 | 应用系统是否部署了网防g01、阿里云盾等安全防护机制 | 请备注 |
| 3 | 如果是外网环境请说明是否部署在阿里云 | 请备注 |

**检测条件准备表**

|  |  |  |  |
| --- | --- | --- | --- |
| **条件分类** | **检测前提条件** | **满足打钩** | **备注说明** |
| 网络 | **主机扫描相关**：生产应用环境、数据库等所有检测边界内与检测ip地址网络互通，可以ping通检测地址10.238.103.13（针对此地址全端口开放） |  |  |
| **应用扫描相关：**测试应用环境、测试数据库等测试系统边界内的ip地址可以ping通10.3.37.0/24 |  |  |
| 测试环境 | 1、测试环境搭建完善（提供测试系统环境），与生产系统功能一致，连接好后端数据库，功能能够正常使用(例如上传、下载、搜索) |  |  |
| 2、配备专人（技术人员）配合检测，提供专人联系方式，配合应用扫描时放开账号密码锁定策略；渗透测试时开启账号密码锁定机制 |  |  |
| 3、备份数据库 |  |  |

**安全检测流程介绍**

攻防实验室安全检测涉及四个部分：主机扫描，应用扫描，配置检查和渗透测试。其中主机扫描和应用扫描要求项目组对所有中高危漏洞进行整改。整体流程如下：

1. ***主机扫描***

主机扫描是针对**生产主机**的系统，数据库和相关插件进行漏洞检测的扫描方式。

实验室使用的官方软件为“绿盟”扫描器，因此要求生产主机与扫描器所在主机（10.238.103.13）能够直接互通。项目组要针对报告对中高危漏洞进行整改。

1. ***应用扫描***

应用扫描是对在开发过程中因相关人员缺乏安全意识而导致的配置不规范、参数未过滤等风险进行检查和评估的扫描方式。应用扫描的进行能够帮助开发人员培养良好的安全习惯，为今后的安全开发打下基础。

实验室使用AppScan作为应用扫描工具，通过Web前端与Web应用程序通信，自动检查Web应用程序，探测、分析其响应，从而发现潜在的安全问题和架构缺陷。生成原始数据后手工进行误报排除工作，保证最终检测报告版本的准确性。在扫描过程中会生成垃圾数据，因此应用扫描要求项目组准备测试环境和数据备份。个别系统因AppScan无法成功爬取页面需要手动扫描获取流量，而导致检测时间延长。

1. ***配置检查***

配置检查是确保**生产主机**底层配置可靠规范的安全检查。内容涉及查看相关操作系统、中间件的配置文件和数据库配置项（密码是否符合规则，日志备份是否开启等）。

项目组收到基线表需要提前进行自查，基线表中所有项目要求全部符合。因配置检查涉及项目组人员到场进行，需要跟基础设施运行保障部负责人（朱勇，张琳等）提前预约时间并确保生产服务器能够远程登录。

1. ***渗透测试***

渗透测试是指渗透人员在不同的位置（比如从内网、从外网等位置）利用各种手段对某个特定网络模拟真实黑客攻击，以期发现和挖掘应用中存在的漏洞，后输出渗透测试报告，并提交给项目组。

实验室手工对目标网站或APP进行渗透测试，有针对性得挖掘测试系统应用、逻辑层面的漏洞，因涉及信息收集过程，一般周期相对较长，视项目复杂程度而定。