|  |  |  |  |
| --- | --- | --- | --- |
| xxx渗透测试报告 | | | |
| ■ 文档编号 |  | ■ 密级 | **商业机密** |
| ■ 版本编号 | 1.0 | ■ 日期 | 20xx-xx-xx |

|  |
| --- |
| © 2020 |

|  |
| --- |
| **目录**  [xxx门户网站 1](#_Toc457749369)  [渗透测试报告 1](#_Toc457749370)  [一. 摘要 1](#_Toc457749371)  [1.1 基本信息 1](#_Toc457749372)  [1.2 测试方法 1](#_Toc457749373)  [1.3 漏洞概要 1](#_Toc457749374)  [1.3.1 系统层安全测试漏洞概要 1](#_Toc457749375)  [1.3.2 应用层安全测试漏洞概要 2](#_Toc457749376)  [1.4 系统当前安全状况 3](#_Toc457749377)  [二. 渗透测试概述 3](#_Toc457749378)  [2.1 概述 3](#_Toc457749379)  [2.2 风险管理 4](#_Toc457749380)  [2.3 收益 5](#_Toc457749381)  [三. 系统层安全测试 6](#_Toc457749382)  [3.1 操作系统漏洞扫描 6](#_Toc457749383)  [3.2 系统结构分析及测试信息收集 6](#_Toc457749384)  [3.2.1 端口收集 6](#_Toc457749385)  [3.2.2 域名信息 6](#_Toc457749386)  [3.3 远程溢出 7](#_Toc457749387)  [3.4 未授权访问 7](#_Toc457749388)  [3.5 口令猜测 7](#_Toc457749389)  [3.6 跳板攻击 7](#_Toc457749390)  [四. 应用层安全测试 8](#_Toc457749391)  [4.1 配置管理测试（含中风险） 8](#_Toc457749392)  [4.1.1 基础配置管理测试 8](#_Toc457749393)  [4.1.2 应用管理界面测试 8](#_Toc457749394)  [4.1.3 HTTP方法测试 8](#_Toc457749395)  [4.1.4 SSL/TLS测试（低风险） 8](#_Toc457749396)  [4.1.5 应用配置管理测试(中风险) 8](#_Toc457749397)  [4.1.6 过期、备份页面测试 9](#_Toc457749398)  [4.2 数据验证测试（含中风险） 9](#_Toc457749399)  [4.2.1 跨站脚本测试 9](#_Toc457749400)  [4.2.2 HTTPSPLITTING测试 9](#_Toc457749401)  [4.2.3 SQL注入测试 9](#_Toc457749402)  [4.2.4 命令执行测试 10](#_Toc457749403)  [4.2.5 代码注入测试 10](#_Toc457749404)  [4.2.6 XML注入测试 10](#_Toc457749405)  [4.2.7 XPATH注入测试 10](#_Toc457749406)  [4.2.8 URL跳转测试 10](#_Toc457749407)  [4.2.9 文件上传测试（中风险） 10](#_Toc457749408)  [4.2.10 程序报错测试 11](#_Toc457749409)  [4.2.11 金额篡改测试 11](#_Toc457749410)  [4.3 认证测试（含中风险） 12](#_Toc457749411)  [4.3.1 认证模式绕过测试 12](#_Toc457749412)  [4.3.2 用户枚举测试（中风险） 12](#_Toc457749413)  [4.3.3 暴力破解测试（中风险） 13](#_Toc457749414)  [4.3.4 竞争条件测试 14](#_Toc457749415)  [4.3.5 图形验证码测试 14](#_Toc457749416)  [4.3.6 密码修改点测试 14](#_Toc457749417)  [4.3.7 密码重置点测试 14](#_Toc457749418)  [4.3.8 注销登录测试 15](#_Toc457749419)  [4.4 业务逻辑测试（含高风险） 15](#_Toc457749420)  [4.4.1 遍历用户信息（高风险） 15](#_Toc457749421)  [4.5 会话管理测试（含中风险） 16](#_Toc457749422)  [4.5.1 会话管理模式测试（中风险） 16](#_Toc457749423)  [4.5.2 会话固定测试 17](#_Toc457749424)  [4.5.3 会话变量泄露测试 17](#_Toc457749425)  [4.5.4 CSRF测试 17](#_Toc457749426)  [4.6 敏感信息保护测试（含中风险） 17](#_Toc457749427)  [4.6.1 用户敏感信息保护（中风险） 17](#_Toc457749428)  [4.6.2 业务敏感信息保护 18](#_Toc457749429)  [4.7 第三方插件测试 18](#_Toc457749430)  [4.7.1 Struts2远程代码执行漏洞测试 18](#_Toc457749431)  [4.8 后门与暗链检查测试 18](#_Toc457749432)  [4.8.1 后门检查 18](#_Toc457749433)  [4.8.2 暗链检查 18](#_Toc457749434)  [五. 参考与建议 18](#_Toc457749435)  [5.1 安全等级评定参考 18](#_Toc457749436)  [5.1.1 漏洞风险等级评定参考 18](#_Toc457749437)  [5.1.2 应用安全等级评定参考 20](#_Toc457749438)  [5.2 安全意见 21](#_Toc457749439)  [5.2.1 传输安全 21](#_Toc457749440)  [5.2.2 Web 安全编程 21](#_Toc457749441)  [5.2.3 安全复检 21](#_Toc457749442)  [5.2.4 定期进行安全审计 21](#_Toc457749443) |

1. 摘要
   1. 基本信息

经xx市xxx单位的授权，xxx渗透测试小组对xx市单位的官方网站（http://www.xxx.yyy.cn）进行了渗透测试。

|  |  |
| --- | --- |
| 评测时间 | 20xx年xx月xx日-20xx年xx月xx日 |
| 对象 | xxxxx市单位官方网站（http://www.xxx.xxx.cn）  (IP: xx.10.xx.95) |
| 说明 | 无 |

* 1. 测试方法

在不知道目标网络环境的情况下，模拟黑客攻击，使用各种主流测评工具及自主开发的内部测试工具，参照相应安全性能指标标准进行安全检查。

* 1. 漏洞概要
     1. 系统层安全测试漏洞概要

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 检查项 | 漏洞数 | | 章节 | 备注 |
| **高风险** | **中风险** |
| 服务器系统漏洞扫描 | 0 | 0 | 3.1 |  |
| 高危端口 | 0 | 2 | 3.2.1 | 对外开放了危险端口，可导致被攻击者暴力猜测出相关应用的账号与密码 |

问题列表

* + 1. 应用层安全测试漏洞概要

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 检查项 | 存在漏洞的检查项 | 威胁等级 | 漏洞数 | 章节 | 备注 |
| 配置管理测试 | SSL/TLS测试 | 低 | 1 | 4.1.4 |  |
| 应用配置管理测试 | 中 | 1 | 4.1.5 |  |
| 数据验证测试 | 文件上传测试 | 中 | 2 | 4.2.9 |  |
| 认证测试 | 用户枚举测试 | 中 | 1 | 4.3.2 |  |
| 暴力破解测试 | 中 | 1 | 4.3.3 |  |
| 业务逻辑测试 | 遍历用户信息 | 高 | 1 | 4.4.1 | 可获得网站上所有用户的个人信息，包括部门职位、手机号码、传真等信息 |
| 会话管理测试 | 会话管理模式测试 | 中 | 1 | 4.5.1 |  |
| 敏感信息保护测试 | 用户敏感信息保护 | -中 | 1 | 4.6.2 |  |
| 第三方插件测试 | - | - | 0 | - |  |
| 后门与暗链检查测试 | - | - | 0 | - |  |

问题列表

**漏洞数量：**

* 高危问题：1个
* 中危问题：9个
* 低危问题：1个

安全风险分布图

* 1. 系统当前安全状况

经xxx安全评估小组进行全面安全评估后，xxx安全评估小组认为当前系统安全状况如下图。级别为：

**远程高风险系统**

1. 渗透测试概述
   1. 概述

对于已经部署了安全防护措施（安全产品、安全服务）或者即将部署安全防护措施的用户而言，明确网络当前的安全现状对下一步的安全建设有重大的指导意义。渗透测试服务用于验证在当前的安全防护措施下网络、系统抵抗黑客攻击的能力。

透测试小组利用各种主流的攻击技术对网络、系统做模拟攻击测试，以发现网络、系统中存在的安全漏洞和风险点。企业、组织根据测试的结果遵循安全策略制定适合的、不同优先级别的安全防护措施、流程。

渗透测试流程定义为如下阶段：

**信息收集**

此阶段中，渗透测试小组进行必要的信息收集，如操作系统类型、开放的端口和服务、 web服务应用系统版本、后台数据库类型、web开发语言等。

**渗透测试**

此阶段中，渗透测试小组根据第一阶段获得的信息对网络、系统进行渗透测试。此阶段如果成功的话，可能获得普通权限或系统权限。

**本地信息收集**

此阶段中，渗透测试小组进行本地信息收集，用于下一阶段的权限提升。

**权限提升**

此阶段中，渗透测试小组尝试由普通权限提升为管理员权限，获得对系统的完全控制权。在时间许可的情况下，必要时从第一阶段重新进行。

**清除**

此阶段中，渗透测试小组清除日志记录等数据。

**输出报告**

此阶段中，渗透测试小组根据测试的结果编写直观的渗透测试服务报告。

* 1. 风险管理

相对其他服务而言，渗透测试是一种需要相当技术深度的高端服务，要求渗透测试人员有丰富的经验及新颖的思路。

在渗透测试过程中，虽然我们尽量避免影响正常业务的运行，也会采取适当的风险规避、风险降低的方法，但是由于测试的不确定性，渗透测试服务仍然有可能对网络、系统运行造成一定不同程度的影响，可能造成服务停止，甚至是宕机。

另外，对于安全防护措施严密的网络、系统，在有限的时间内进行渗透测试可能不会获得成功结果。这在一定程度也证明了网络、系统能够在一定程度上抵抗黑客的攻击。

* 1. 收益

从攻击者的角度进行测试将有助于发现并识别出一些隐性存在的安全漏洞和风险点。

从客户收益的角度来说，特别是在进行安全项目之前进行渗透测试，可以对信息系统的安全性得到较深的感性认知，有助于后续的安全建设。

在进行了安全项目之后进行渗透测试，则可以用于验证经过安全保护后的网络是否真实的达到了预定安全目标、遵循了安全策略。

1. 系统层安全测试
   1. 操作系统漏洞扫描

通过漏洞扫描发现服务器操作系统信息和操作系统的安全漏洞，同时检验防火墙和DDoS防护等安全设施的抗攻击能力。

* 测试过程：

经系统漏洞扫描器扫描，发现服务器补丁更新及时，暂未发现安全风险。

* 1. 系统结构分析及测试信息收集

信息收集工作包括WEB服务器和应用程序指纹探测、后台应用程序发掘、爬网和Googling、错误代码挖掘、应用程序配置管理测试等。

* + 1. 端口收集

|  |  |
| --- | --- |
| 端口/协议 | 服务 |
| 21/tcp | ftp |
| 23/tcp | telnet |

经过端口探测扫描发现，系统对外只开放了多个端口，其中存在21，23等高危端口，建议将这些不必要提供的端口关闭。

* + 1. 域名信息

域名：www.xxx.yyy.cn

域名状态： clientTransferProhibited

注册人：xxxx市yyyy院

管理员邮件： xxxxx@qq.com

注册商： 广东时代互联科技有限公司

DNS服务器： ns5010.01isp.com

DNS服务器：ns5011.01isp.cn

注册时间： 2009-08-19 15:30:06

过期时间： 2019-08-19 15:30:06

* 1. 远程溢出

远程溢出测试基于漏洞扫描的结果，扫描发现的系统漏洞可能是误报，不过一旦远程溢出被利用，攻击者很有可能就会获得系统的最高权限。

* 测试结论：

经系统漏洞扫描，发现服务器补丁更新及时，暂未发现可利用的远程溢出漏洞，暂未发现安全风险。

* 1. 未授权访问

服务器第三方软件默认配置会有匿名访问或者空密码访问的权限，攻击者利用该漏洞可直接入侵服务器。

* 测试结论：

服务器安全配置良好，暂未发现安全风险。

* 1. 口令猜测

使用常见的密码对服务器系统进行远程密码猜解。包括系统密码，WEB等系统应用。

* 测试结论：

服务器安全配置良好，无弱口令，暂未发现安全风险。

* 1. 跳板攻击

攻击者控制同网段的一台主机后向目标主机进行入侵。

* 测试结论：

C段服务器未发现可入侵的主机，暂未发现安全风险。

1. 应用层安全测试
   1. 配置管理测试（含中风险）
      1. 基础配置管理测试

经过测试，此项未发现问题。

* + 1. 应用管理界面测试

经过测试，此项未发现问题。

后台管理登录口、cms管理口、

* + 1. HTTP方法测试

经过测试，此项未发现问题。

OPTION DELETE PUT TRACE

* + 1. SSL/TLS测试（低风险）

未使用SSL/TLS对传输的数据进行保护。

* + 1. 应用配置管理测试(中风险)

Robot.txt web-inf

**【问题链接】**

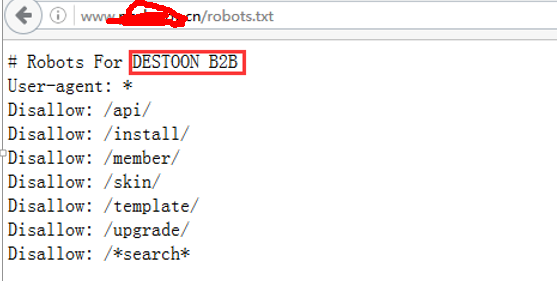
<http://www.xxxx.gov.cn/robots.txt>

**【危险等级】**

**中**

**【问题说明】**

从robots文件里可以获取到网站一些目录信息并且可获知网站采用DESTOON B2B网站管理系统进行二次开发，攻击者可能会采用该管理系统通用漏洞对网站发起攻击。



**【修复建议】**

删除robots.txt文件。

* + 1. 过期、备份页面测试

经过测试，此项未发现问题。

* 1. 数据验证测试（含中风险）
     1. 跨站脚本测试

经过测试，此项未发现问题。

* + 1. HTTPSPLITTING测试

经过测试，此项未发现问题。

头拆分

* + 1. SQL注入测试

经过测试，此项未发现问题。

* + 1. 命令执行测试

经过测试，此项未发现问题。

1. 具有命令执行的功能的
2. Imagemagick
3. Struts2
4. Java反序列化漏洞
   * 1. 代码注入测试

经过测试，此项未发现问题。

* + 1. XML注入测试

经过测试，此项未发现问题。

XXE XML external entity 外部实体使用

* + 1. XPATH注入测试

经过测试，此项未发现问题。

* + 1. URL跳转测试

经过测试，此项未发现问题。

* + 1. 文件上传测试（中风险）

**【问题链接】**

1. <http://www.xxxxx.gov.cn/member/fckeditor/editor/dialog/fck_image.html>
2. <http://www.xxxxx.gov.cn/member/fckeditor/editor/dialog/fck_attach.html>

**【危险等级】**

**中**

**【问题说明】**

网站存在上传测试页面暴露，可能存在上传非法脚本到服务端获取webshell的风险。

**【修复建议】**

删除上传测试页面。

* + 1. 程序报错测试

经过测试，此项未发现问题。

* + 1. 金额篡改测试

经过测试，此项未发现问题。

* 1. 认证测试（含中风险）
     1. 认证模式绕过测试

经过测试，此项未发现问题。

* + 1. 用户枚举测试（中风险）

【问题链接】

1. http://www.xxxx.gov.cn/member/login.php

【危险等级】

**中**

【问题说明】

当用户名存在但密码错误时，服务端返回“密码错误，请重试”；当用户名不存在时，返回“会员不存在”。利用返回结果的不同可判定哪些用户是系统真实存在的。

【修复建议】

1、登录校验失败提示统一改为“用户名或密码错误”。

* + 1. 暴力破解测试（中风险）

【问题链接】

1. http://www.xxxx.gov.cn/member/chat.php

【危险等级】

**中**

【问题说明】

登陆系统后在我的对话栏目中，由于发起对话处没有设置验证码防范暴力破解，导致可暴力猜解系统已存在的用户。