XXX 系统安全渗透测试报告

■ 文档编号		■ 密级	商业机密
■ 版本编号	V1.0	■ 日期	2012-01-13

批注 [S1]: 客户名称+系统名称+报告名称

批注 [S2]: 报告最后更新的版本

批注 [S3]: 报告最后更新的日期

■ 版权声明

■ 版本变更记录

时间	版本	说明	修改人
2011-12-27	V1.0	文档创建	专业服务部
2012-01-13	V1.1	丰富内容	专业服务部

批注 [S4]: 文档创建时间

批注 [S5]: 文档最后更新时间

批注 [S6]: 可写“专业服务部”也可写报告具体撰写人

■ 适用性声明

本文档为北京神州绿盟信息安全科技股份有限公司（以下简称“绿盟科技”）在 2011 年 12 月向民生银行信用卡中心实施渗透测试安全服务后提供的测试分析报告，适用于相关技术人员在对发现的漏洞进行安全修复时参考。

批注 [S7]: 具体测试的时间，精确到月份即可，夸月时按实际情况描述

批注 [S8]: 客户名称

目录

批注 [S9]: 文档最后更新后要更新目录。

表格索引

批注 [S10]: 文档最后更新后要更新目录。

插图索引

批注 [S11]: 文档最后更新后要更新目录。

一. 摘要

经 XXX 的授权，绿盟科技渗透测试小组于 2011 年 11 月 27 日至 2011 年 12 月 31 日，对 XXX 下属 XXX 网站、XXX 系统进行了渗透测试。

绿盟科技认为被测 XXX 系统当前安全状态是：远程不安全系统[①]；被测 XXX 系统当前安全状态是：远程不安全系统。

测试结果如下[②]：

- ☑ **严重问题**[③]：1 个
- ☑ **中等问题**：2 个
- ☑ **轻度问题**：2 个

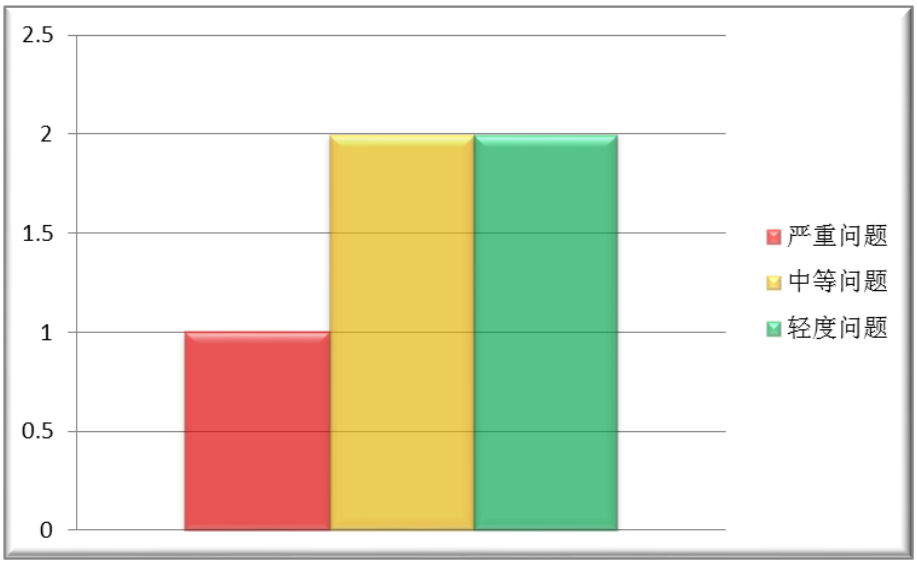


图 1.1 安全问题分布图

详细安全问题汇总如下：

问题等级	种类	数量	安全问题名称
严重问题	1 种	1 个	越权访问及操作
中度问题	1 种	1 个	跨站脚本编制

[①] 评定标准请参看附录 B。
[②]本份测试报告分析的各种安全风险，仅限定于在上述时间段内测试反馈信息的整理，不包括非上述时间段内的因系统调整、维护更新后出现的其他变化情况。
[③]问题定级请参看附录 A。

批注 [S12]: 修改页眉页脚报告名称。
批注 [S13]: 客户名称
批注 [S14]: 实际测试日期
批注 [S15]: 客户名称
批注 [S16]: 测试对象描述
批注 [S17]: 测试对象描述
批注 [S18]: 安全状态
批注 [S19]: 测试对象描述
批注 [S20]: 安全状态
批注 [S21]: 根据实际测试结果修改，并替换对应的分布图。
批注 [S22]: 根据实际测试结果描述发现的问题。

	1 种	1 个	网站支持部分弱的 SSL 算法
轻度问题	1 种	1 个	后台管理界面泄露
	1 种	1 个	网站安全证书不规范

二. 概述

本次渗透测试工作是由绿盟科技的渗透测试小组独立完成的。

绿盟科技渗透测试小组在2011年12月27日至2011年12月30日对XXX的XXX网站、XXX系统进行了远程渗透测试工作。在此期间，绿盟科技渗透测试小组利用部分前沿的攻击技术，使用成熟的黑客攻击手段，集合软件测试技术（标准）对指定网络、系统做入侵攻击测试，希望由此发现网站、应用系统中存在的安全漏洞和风险点。

批注 [S23]: 实际测试日期

批注 [S24]: 客户名称

批注 [S25]: 测试对象

2.1 测试流程

绿盟科技渗透测试服务流程定义为如下阶段。

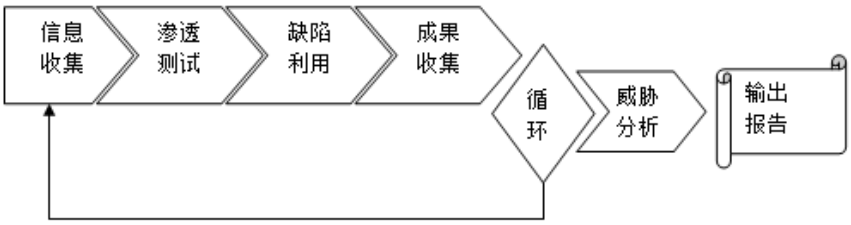


图 2.1 渗透测试流程

1. 信息收集：此阶段中，绿盟科技测试人员进行必要的信息收集，如 IP 地址、DNS 记录、软件版本信息、IP 段、Google 中的公开信息等。
2. 渗透测试：此阶段中，绿盟科技测试人员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。
3. 缺陷利用：此阶段中，绿盟科技测试人员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。
4. 成果收集：此阶段中，绿盟科技测试人员对前期收集的各类弱点、漏洞等问题进行分类整理，集中展示。
5. 威胁分析：此阶段中，绿盟科技测试人员对发现的上述问题进行威胁分类和分析其影响。
6. 输出报告：此阶段中，绿盟科技测试人员根据测试和分析的结果编写直观的渗透测试服务报告。

2.2 风险管理

为保障客户系统在渗透测试过程中稳定、安全的运转，我们将提供以下多种方式来进行风险规避。

对象的选择

为更大程度的避免风险的产生，渗透测试还可选择对备份系统进行测试。因为备份系统与在线系统所安装的应用和承载的数据差异较小，而其稳定性要求又比在线系统低，因此，选择对备份系统进行测试也是规避风险的一种常见方式。

时间的控制

从时间安排上，测试人员将将尽量避免在数据高峰时进行测试，以此来减小测试工作对被测试系统带来的压力。另外，测试人员在每次测试前也将通过电话、邮件等方式告知相关人员，以防止测试过程中出现意外情况。

技术手段

绿盟科技的渗透测试人员都具有丰富的经验和技能，在每一步测试前都会预估可能带来的后果，对于可能产生影响的测试（如：溢出攻击）将被记录并跳过，并在随后与客户协商决定是否进行测试及测试方法。

监控措施

针对每一系统进行测试前，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。

工具使用

在使用工具测试的过程中，测试人员会通过设置线程、插件数量等参数来减少其对系统的压力，同时还会去除任何可能对目标系统带来危害的插件，如：远程溢出攻击类插件、拒绝服务攻击类插件等等。

2.3 预期收益

通过实施渗透测试服务，可对贵方的信息化系统起到如下推进作用：

明确安全隐患

渗透测试是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此明确整体系统中的安全隐患点。

提高安全意识

如上所述，任何的隐患在渗透测试服务中都可能造成“千里之堤溃于蚁穴”的效果，因此渗透测试服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

提高安全技能

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的渗透测试报告，也能为用户提供当前流行安全问题的参考。

三. 测试服务介绍

3.1 测试对象

测试对象	相关域名、对应的 URL
商城网站	XX 系统： https://mall.cmbc.com.cn:1668/odsBackControlAction!login_index 用户名：securityscan 密码：wq_123

批注 [S26]: 如实描写测试对象

3.2 测试时间

测试工作时间段			
起始时间	2011-12-27	结束时间	2011-12-30

批注 [S27]: 如实描写测试时间

3.3 测试人员

参测人员名单					
姓名	XXX	所属部门	绿盟科技北京分公司专业服务部	联系方式	XXX@nsfocus.com
姓名	XXX	所属部门	绿盟科技北京分公司专业服务部	联系方式	XXX@nsfocus.com

批注 [S28]: 如实修改测试人员

3.4 测试环境

本次渗透测试过程中，绿盟科技测试小组使用过多个互联网 IP 地址开展的分析工作，在此通知 XXX 的 XX 网站、XX 系统相关人员在对受测试的目标站点服务器、相应的网络入侵检测系统进行安全监控和日志分析时，排除以下 IP 地址产生的任何违规信息，以保证分析结果的准确有效。

批注 [S29]: 客户名称

批注 [S30]: 测试网站或系统名称

IP 地址	IP 地址	IP 地址	IP 地址
211.103.182.2~32	暂无	暂无	暂无

批注 [S31]: 如实记录 IP 地址

3.5 工具资源

本次渗透测试使用部分工具如下：

批注 [S32]: 可根据情况自行添加测试工具及描述

表 3.1 测试工具：NetCat

工具名称	NetCat
工具用途	端口连接，数据提交
相关信息	http://joncraton.org/files/nc111nt.zip

表 3.2 测试工具：Nmap

工具名称	Nmap
工具用途	端口扫描，服务识别，操作系统指纹识别
相关信息	http://nmap.org/

表 3.3 测试工具：httprint

工具名称	Httprint
工具用途	通过远程 http 指纹判断 http 服务类型
相关信息	http://www.net-square.com/httprint/

表 3.4 测试工具：Tamper IE

工具名称	Tamper IE
工具用途	HTTP 数据包修改、转发工具（Firefox 插件）
相关信息	http://www.bayden.com/TamperIE/

表 3.5 测试工具：安全检测工具集

工具名称	绿盟科技整理的安全检测工具集
工具用途	跨站及 SQL 注入测试、远程溢出测试、暴力破解测试、嗅探分析
相关信息	www.nsfocus.com

在具体的分析过程中，绿盟科技测试小组在微软的 Windows 平台上（涵盖 2003/Vista），使用了 IE（涵盖 6.0/7.0/8.0）和 Firefox 浏览器对指定的测试对象进行的分析、校验、测试。因此，漏洞分析检测到的部分安全问题可能与特定的操作系统、软件版本有具体关系，提醒后期实施漏洞修复工作的人员特别注意其中的差异。

批注 [S33]: 根据实际情况修改

批注 [S34]: 根据实际情况修改

批注 [S35]: 本章节根据测试情况修改。

四. 测试过程详述

4.1 目标信息探测

4.1.1 域名信息

渗透测试人员首先通过 nslookup 对主机的 IP 地址、NS 记录等信息的查询，对站点进行基本的信息探测，结果如下。

```
Default Server:    dns1.datadragon.net
Address:    211.147.6.3
> www.cmbc.com.cn
Server:    dns1.datadragon.net
Address:    211.147.6.3

Non-authoritative answer:
Name:       www.cmbc.com.cn
Address:    219.142.89.144
//查询 ns 记录
> set type=ns
> mall.cmbc.com.cn
Server:    dns1.datadragon.net
Address:    211.147.6.3

Non-authoritative answer:
mall.cmbc.com.cn            nameserver = ns1.mall.cmbc.com.cn
mall.cmbc.com.cn            nameserver = ns2.mall.cmbc.com.cn

ns1.mall.cmbc.com.cn        internet address = 116.213.80.30
ns2.mall.cmbc.com.cn        internet address = 114.255.47.61_
//测试区域传输
> set type=axfr
```

```
> ls -d mall.cmbc.com.cn
[dns1.datadragon.net]
*** Can't list domain mall.cmbc.com.cn:
 //查询站点 mx 记录
> set type=mx
> mall.cmbc.com.cn
Server:    dns1.datadragon.net
Address:   211.147.6.3
Non-authoritative answer:
mall.cmbc.com.cn          MX preference = 0, mail exchanger =
mall.cmbc.com.cn          nameserver = ns1.mall.cmbc.com.cn
mall.cmbc.com.cn          nameserver = ns2.mall.cmbc.com.cn
mall.cmbc.com.cn          internet address = 116.213.80.15
ns1.mall.cmbc.com.cn      internet address = 116.213.80.30
ns2.mall.cmbc.com.cn      internet address = 114.255.47.61
```

对 WWW 目标进行 Whois 的查询，获取到的 Whois 信息如下。

域名：cmbc.com.cn
域名 ID： 20021209s10011s00051629-cn
域名状态：域名服务器上禁止删除保护
域名状态：域名服务器上禁止修改保护
域名状态：域名服务器上禁止转移保护
域名所有者： 中国民生银行股份有限公司
注册人： 王婷
管理员邮件： wangting@cmbc.com.cn
注册商： 北京东方网景信息科技有限公司
DNS 服务器：ns1.cmbc.com.cn
DNS 服务器：ns.cmbc-online.com.cn
DNS 服务器：ns3.cmbc.com.cn
DNS 服务器：ns4.cmbc.com.cn
注册时间： 1998-01-09 00:00:00
过期时间： 2014-01-09 00:00:00

4.2 系统测试

4.2.1 端口扫描

通过使用 Nmap 端口扫描工具对主机在 Internet 上的端口开放情况进行检查：

> nmap -sT -P0 -O mall.cmbc.com.cn，结果如下。

```
D:\> nmap -sT -P0 -O mall.cmbc.com.cn
Starting Nmap 5.00 ( http://nmap.org ) at 2011-12-27 16:25 中国标准时间
Interesting ports on 114.255.47.46:
PORT       STATE SERVICE
80/tcp     open  http
443/tcp    open  https
1666/tcp open  netview-aix-6
1667/tcp open  netview-aix-7
1668/tcp open  netview-aix-8
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
No OS matches for host
Nmap done: 1 IP address (1 host up) scanned in 2526.609 seconds
```

通过 Nmap 扫描报告，我们确认由于防火墙或前端设备回包的影响，Nmap 扫描不出具体开放的真实端口，因此，无法判断开放了那些实际端口，初步判断，系统开放了 80、443、1666、1667、1668 端口。

- TCP/80 （HTTP 服务）
- TCP/443 (HTTPS 服务)
- 1666/tcp (netview-aix-6 服务)
- 1667/tcp (netview-aix-7 服务)
- 1668/tcp (netview-aix-8 服务)

4.2.2 信息探测

由于此次测试系统为 ODS，所以只对 TCP 1667 端口（WEB 应用服务）做服务信息探测，因此，后继的渗透测试工作主要针对 ODS 应用本身及运行于 WEB 应用上的代码展开。

使用 httprecon 对远程主机的 WEB 应用版本进行判断，但无法获取信息成功。

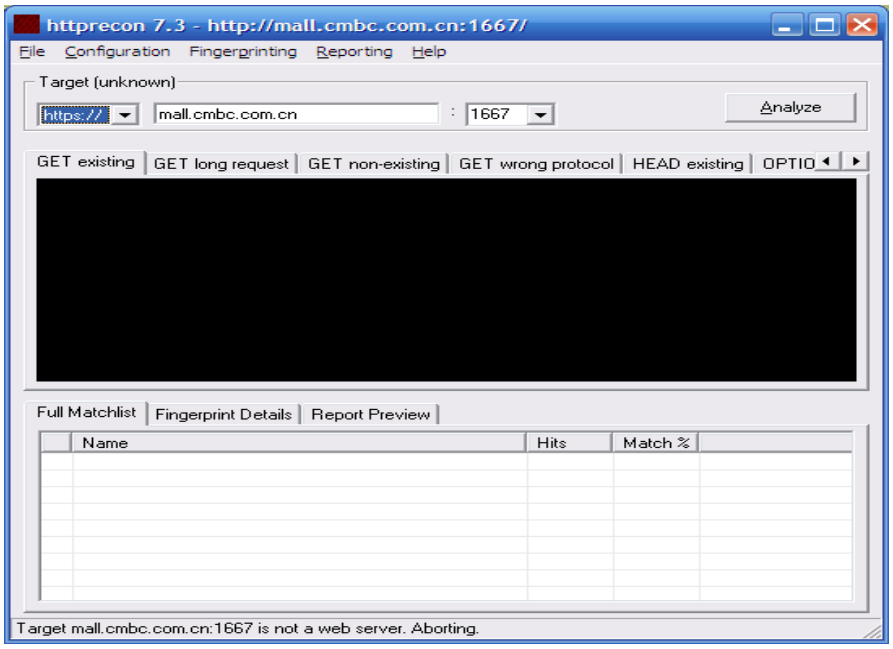


图 4.1 httprecon 判断远程 WEB 应用版本结果 1

使用 httprint 对远程主机的 WEB 应用版本进行判断，也无法获取信息成功。经测试人员分析，是由于边界防火墙做了策略，不允许 ICMP 包的 echo，故无法通过 ICMP 来刺探信息。

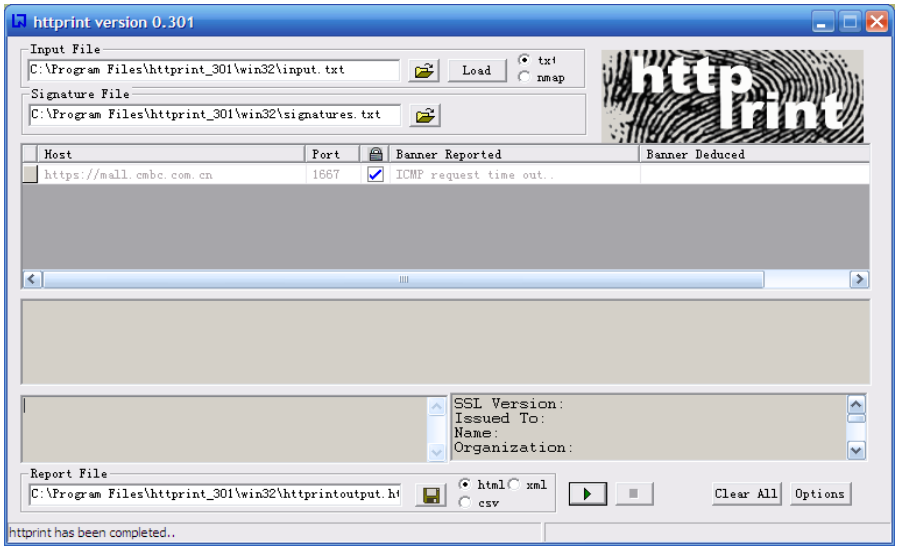


图 4.2 httprint 判断远程 WEB 应用版本结果 2

4.3 测试内容

测试人员根据 WASC 威胁分类[①]，对应用程序的渗透测试从五个类型的安全方面进行测试，这五个威胁类型包括：认证和授权、命令执行、逻辑攻击、客户端攻击、信息泄露。

表 4.1 WASC 威胁分类图

认证和授权类	命令执行类
暴力攻击	LDAP 注入
认证不充分	SSI 注入
会话定置	SQL 注入
会话期限不充分	Xpath 注入
凭证/会话预测	操作系统命令
授权不充分	格式字符串攻击
逻辑攻击类	缓冲区溢出
功能滥用	**信息泄漏类**
拒绝服务	可预测资源定位
客户端攻击类	路径遍历
跨站点脚本编制	目录索引
内容电子欺骗	信息泄露

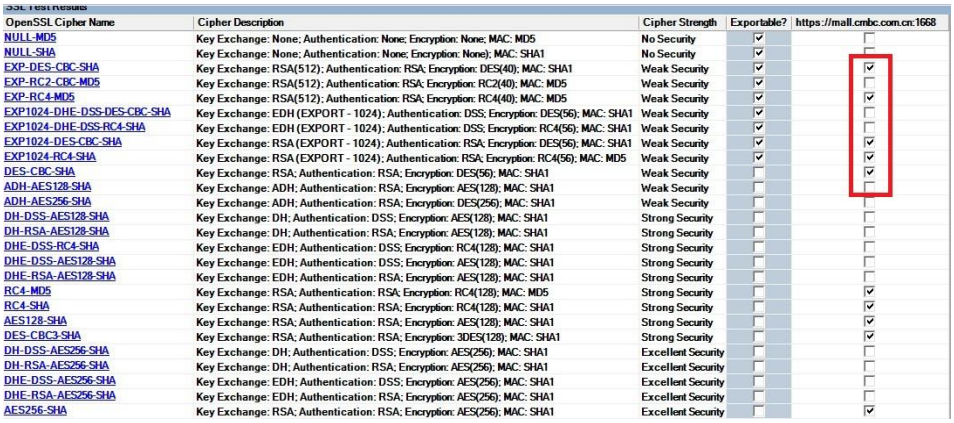
[①] WASC 即 Web Application Security Consortium。是一个由安全专家、行业顾问和诸多组织的代表组成的国际团体。他们负责为 WWW 制定被广为接受的应用安全标准。WASC 组织的关键项目之一是“Web 安全威胁分类”，也就是将 Web 应用所受到的威胁、攻击进行说明并归纳成具有共同特征的分类。

4.3.2 认证和授权类

测试人员在对网站进行认证和授权类的测试时，主要进行了会话固定和授权不充分的测试，经测试发现被测网站存在上述漏洞。

◆ 网站支持部分弱的 SSL 算法（风险点）

测试人员通过对 SSL 检查发现，当前系统 https://mall.cmbc.com.cn:1668/网站支持部分弱的 SSL 算法，而使用弱算法有可能导致恶意攻击者从客户端强制服务器端使用弱算法协商通信，当发生网络窃听后，信息被泄露风险加大。如下图：



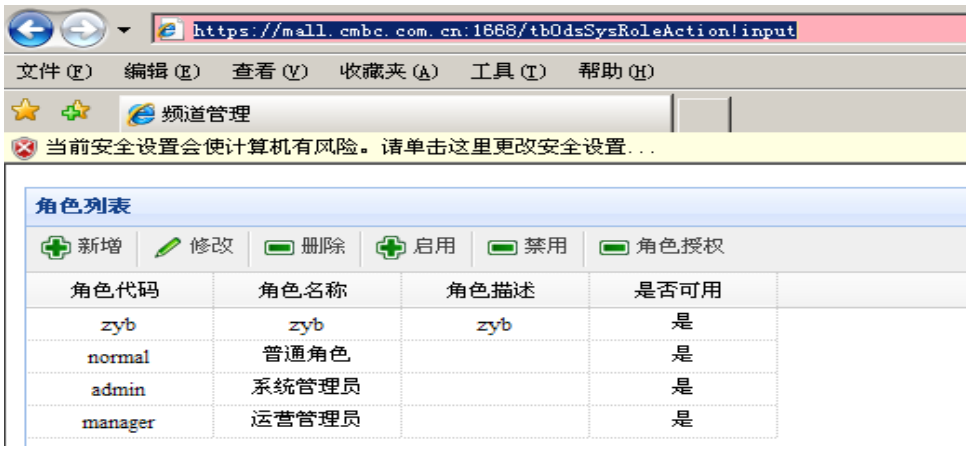
OpenSSL Cipher Name	Cipher Description	Cipher Strength	Exportable?	https://mall.cmbc.com.cn:1668
NULL-MD5	Key Exchange: None; Authentication: None; Encryption: None; MAC: MD5	No Security	☑	☐
NULL-SHA	Key Exchange: None; Authentication: None; Encryption: None; MAC: SHA1	No Security	☑	☐
EXP-DES-CBC-SHA	Key Exchange: RSA(512); Authentication: RSA; Encryption: DES(40); MAC: SHA1	Weak Security	☑	☑
EXP-RC2-CBC-MD5	Key Exchange: RSA(512); Authentication: RSA; Encryption: RC2(40); MAC: MD5	Weak Security	☑	☐
EXP-RC4-MD5	Key Exchange: RSA(512); Authentication: RSA; Encryption: RC4(40); MAC: MD5	Weak Security	☑	☑
EXP1024-DHE-DSS-DES-CBC-SHA	Key Exchange: EDH (EXPORT - 1024); Authentication: DSS; Encryption: DES(56); MAC: SHA1	Weak Security	☑	☐
EXP1024-DHE-DSS-RC4-SHA	Key Exchange: EDH (EXPORT - 1024); Authentication: DSS; Encryption: RC4(56); MAC: SHA1	Weak Security	☑	☐
EXP1024-DES-CBC-SHA	Key Exchange: RSA (EXPORT - 1024); Authentication: RSA; Encryption: DES(56); MAC: SHA1	Weak Security	☑	☑
EXP1024-RC4-SHA	Key Exchange: RSA (EXPORT - 1024); Authentication: RSA; Encryption: RC4(56); MAC: MD5	Weak Security	☑	☑
DES-CBC-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: DES(56); MAC: SHA1	Weak Security	☐	☑
ADH-AES128-SHA	Key Exchange: ADH; Authentication: RSA; Encryption: AES(128); MAC: SHA1	Weak Security	☐	☐
ADH-AES256-SHA	Key Exchange: ADH; Authentication: RSA; Encryption: DES(256); MAC: SHA1	Weak Security	☐	☐
DH-DSS-AES128-SHA	Key Exchange: DH; Authentication: DSS; Encryption: AES(128); MAC: SHA1	Strong Security	☐	☐
DH-RSA-AES128-SHA	Key Exchange: DH; Authentication: RSA; Encryption: AES(128); MAC: SHA1	Strong Security	☐	☐
DHE-DSS-RC4-SHA	Key Exchange: EDH; Authentication: DSS; Encryption: RC4(128); MAC: SHA1	Strong Security	☐	☐
DHE-DSS-AES128-SHA	Key Exchange: EDH; Authentication: DSS; Encryption: AES(128); MAC: SHA1	Strong Security	☐	☐
DHE-RSA-AES128-SHA	Key Exchange: EDH; Authentication: RSA; Encryption: AES(128); MAC: SHA1	Strong Security	☐	☐
RC4-MD5	Key Exchange: RSA; Authentication: RSA; Encryption: RC4(128); MAC: MD5	Strong Security	☐	☑
RC4-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: RC4(128); MAC: SHA1	Strong Security	☐	☑
AES128-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: AES(128); MAC: SHA1	Strong Security	☐	☑
DES-CBC3-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: 3DES(128); MAC: SHA1	Strong Security	☐	☑
DH-DSS-AES256-SHA	Key Exchange: DH; Authentication: DSS; Encryption: AES(256); MAC: SHA1	Excellent Security	☐	☐
DH-RSA-AES256-SHA	Key Exchange: DH; Authentication: RSA; Encryption: AES(256); MAC: SHA1	Excellent Security	☐	☐
DHE-DSS-AES256-SHA	Key Exchange: EDH; Authentication: DSS; Encryption: AES(256); MAC: SHA1	Excellent Security	☐	☐
DHE-RSA-AES256-SHA	Key Exchange: EDH; Authentication: RSA; Encryption: AES(256); MAC: SHA1	Excellent Security	☐	☐
AES256-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: AES(256); MAC: SHA1	Excellent Security	☐	☑

◆ 越权访问及操作（漏洞）

测试人员首先利用普通帐号登录，配置允许访问页面，如下图：

然后，直接修改访问页面 URL 为角色管理页面，如下图：

https://mall.cmbc.com.cn:1668/tbOdsSysRoleAction!input



在该页面，修改角色管理权限，增加额外管理权限，甚至可以添加新管理员。至此，一个普通用户帐号便得到了管理员权限帐号。

◆ 网站安全证书不规范（风险点）

测试人员对网站检测发现，当前网站使用的安全证书不规范，“颁发给：test.com.cn; 颁发者：CNCA”，而这种方式的不规范证可能导致用户无法与假冒网站混淆不清，从而导致钓鱼攻击的发生。如下图：

4.3.3 逻辑攻击类

测试人员在对网站进行逻辑攻击类的测试时，主要进行了功能滥用的测试，经测试没有发现被测网站存在上述漏洞。

4.3.4 客户端攻击类

测试人员在对网站进行客户端攻击类的测试时，主要测试了跨站脚本编制，经过测试发现被测试网站存在上述漏洞，详细如下：

◆ 存在跨站脚本编制（漏洞）

测试人员在对网站进行 https://mall.cmbc.com.cn:1668/odsBackControlAction!login 登录访问测试时，在“客户信息”的“添加电话记录”里面，向“客户问题”和“客服回答”这两个留言框里面提交了测试代码，发现可以被执行。如下图：

4.3.5 命令执行类

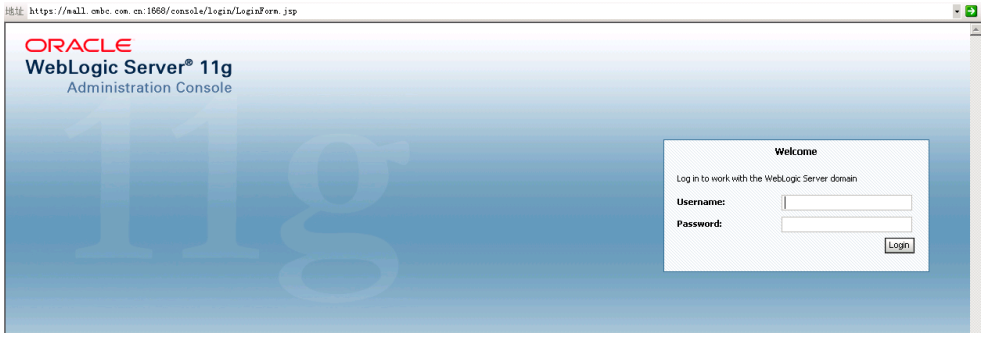
测试人员在对网站进行命令执行类的测试时，主要进行了 SQL 注入、格式字符串攻击、缓冲区溢出攻击的测试，经过测试没有发现被测网站存在上述漏洞。

4.3.6 信息泄露类

测试人员在对网站进行信息泄露类的测试时，主要进行了资源定位、路径遍历和敏感信息获取的测试，经过测试发现敏感信息泄露问题。

◆ WebLogic 后台管理界面泄露（风险点）

测试人员发现 URL 地址为 https://mall.cmbc.com.cn:1668/console/login/LoginForm.jsp 的 WebLogic 后台管理界面暴漏，而这很容易易受到暴力破解攻击。


地址 https://mall.cmbc.com.cn:1668/console/login/LoginForm.jsp
ORACLE
WebLogic Server® 11g
Administration Console
11g
Welcome
Log in to work with the WebLogic Server domain
Username:
Password:
Login

五. 测试结果及建议

5.1 测试结果

在本次渗透测试的 ODS 网站系统中，绿盟科技渗透测试小组发现了部分严重等级风险漏洞，这一级别的漏洞可能会深刻威胁到系统安全性。

发现 ODS 网站系统问题总结如下。

编号	发现问题	漏洞描述	威胁程度
1	越权访问及操作	导致用户越权操作，甚至是操作管理员的数据	严重
2	跨站脚本编制	留言框内可以执行提交的精心构造的 XSS 攻击代码，可能会窃取或操纵客户会话和 cookie。	中等
3	网站支持部分弱的 SSL 算法	SSL 的算法加密强度不够，有被窃听的风险	中等
4	网站安全证书不规范	网站的证书 CA 和被颁发者命名混乱	轻度
5	台管理界面泄露	Oracle weblogic 后台管理界面暴漏	轻度

批注 [S36]: 测试系统名称

批注 [S37]: 测试出的最严重的等级

批注 [S38]: 根据不同等级风险自行修改。

批注 [S39]: 多个系统时，按系统分别列表。

5.2 安全建议

针对上述发现的安全问题，绿盟科技建议立即采取措施进行修补，以避免发生安全问题，下面的安全建议措施可供参考：

编号	发现问题	安全建议	备注
1	越权访问及操作	将访问页面进行严格权限控制，禁止通过 URL 直接请求访问。	
2	跨站脚本编制	对客户提交的数据进行过滤，通过验证用户输入未包含危险字符，便可能防止恶意的用户导致应用程序执行计划外的任务，建议过滤出所有以下字符： [1] |（竖线符号） [2] & （& 符号） [3];（分号） [4] $（美元符号）	

批注 [S40]: 多个系统存在相同问题时，在备注中写上适用于那个对象。

		[5] %（百分比符号） [6] @（at 符号） [7] '（单引号） [8] "（引号） [9] \'（反斜杠转义单引号） [10] \"（反斜杠转义引号） [11] <>（尖括号） [12] ()（括号） [13] +（加号） [14] CR（回车符，ASCII 0x0d） [15] LF（换行，ASCII 0x0a） [16] ,（逗号） [17] \（反斜杠）	
3	网站支持部分弱的 SSL 算法	仅支持强壮的加密算法方式，禁用低等级加密算法	
4	网站安全证书不规范	安全证书密钥长度建议改为 2048 位，使用规范的证书信息。	
5	台管理界面泄露	屏蔽后台管理页面，禁止直接面对互联网，若需要互联网远程管理，建议通过白名单方式限定访问原地址。	

5.3 其他建议

针对 WEB 平台的渗透测试及定期的评估扫描等方式，均以暴露问题为目标，属于被动的安全手段，而这些方式也大大的增加开发和维护的成本，因此建议 XX 公司针对如 WEB 程序这类个性化产品开发前就应做好安全的相关工作，建议 XX 公司对定制开发的产品从以下几个方面进行相关的考察和关注：

批注 [S41]: 客户名称

- 制定以功能和安全兼顾的产品开发需求
- 将安全作为产品开发项目中的重要参考指标
- 产品开发过程中的人员安全意识和技能培训
- 完善的安全开发手册及通用的安全的代码库
- 在开发每阶段完成后的定期代码审计和扫描
- 产品整体上线前的审计工作和远程评估工作

六. 测试结论

经过本次远程渗透测试，我们对此远程系统的安全评价是远程不安全系统。

批注 [S42]: 根据发现漏洞多少自行评定。

七. 致谢

在本次远程渗透测试过程中，绿盟科技感谢 XX 公司 XX 系统部门的相关人员和在渗透测试过程中进行沟通、协调的相关部门和人员的大力配合，使得我们的工作能够顺利完成。对于您的大力支持我们深表感谢。

批注 [S43]: 客户名称

批注 [S44]: 被测试系统，多个时，需要罗列出来。

附录A 威胁程度分级

威胁程度的分级方式说明如下：

- **严重**：直接导致系统被入侵或数据被破坏，一旦发生，就是严重的安全事件。
- **中等**：可能导致重要信息的泄漏或有较高可能导致系统被入侵控制。
- **轻度**：敏感信息泄漏或存在轻微安全问题，一般不会产生严重的安全事件。

附录B 安全等级评定

安全等级	资源内容描述
远程不安全系统 （符合任何一个条件）	1. 存在一个或一个以上严重的安全问题，可直接导致系统受到破坏； 2. 与其他非安全系统连接，同时存在相互信任关系（或帐号互通）的主机； 3. 发现已经被人入侵且留下远程后门的主机； 4. 存在 3 个以上中等安全问题的主机； 5. 与其他非安全系统在一个共享网络中，同时远程维护明文传输口令； 6. 完全不能抵抗小规模的拒绝服务攻击
远程一般安全系统 （符合任何一个条件）	1. 存在一个或一个以上中等安全问题的主机； 2. 开放过多服务，同时可能被利用来进行拒绝服务的主机； 3. 与其他非安全系统直接连接，但暂时不存在直接信任(或帐号互通)关系； 4. 远程维护通过明文的方式传递信息； 5. 存在三个以上轻度安全问题的主机； 6. 只能抵御最低级的拒绝服务攻击；
远程安全系统	1. 最多存在 1-2 个轻度安全问题；

（符合全部条件）	2. 远程维护方式安全； 3. 与不安全或一般安全系统相对独立； 4. 能抵挡一定规模的拒绝服务攻击。