山东科技大学
网络安全基线配置标准

2020 年 6 月

目　录

第1章 概述

1.1 基线目的

为做好网络安全防护，保证联网终端、服务器、网络与安全设备等以及应用系统的安全基线配置规范，特制定本标准。

1.2 标准说明

本标准是网络安全防护基本要求，联网设备和应用系统的安全配置应当满足本标准要求，可在本标准之上做更严格、更深化的安全配置和部署。

本标准配置范例以windows操作系统和华为网络设备为代表，具体安全配置应当根据设备和系统的实际情况参考范例配置。

1.3 适用范围

本标准适用校园网。

第2章 终端安全基线

2.1 账户及口令

2.1.1 管理账户安全

基线名称	终端管理账户安全基线要求
基线要求	不得使用 administrator、admin、sa 等默认用户名作为管理账户；禁用 guest 等来宾账户。
配置范例	进入“控制面板→管理工具→计算机管理”，在“系统工具→本地用户和组”： 缺省账户 Administrator→属性,Guest 账户→属性。
适用范围	PC 机、视频会议终端及其他联网终端设备。

2.1.2 密码有效期

基线名称	终端密码有效期安全基线要求
基线要求	账户口令的生存期不长于 90 天，修改密码 5 次内不得重复。
配置范例	进入“控制面板→管理工具→本地安全策略”,在“账户策略→密码策略”： 查看“密码最长存留期”和“强制密码历史”。
适用范围	PC 机、视频会议终端及其他联网终端设备。

2.1.3 密码复杂度

基线名称	终端密码复杂度安全基线要求
基线要求	操作系统账户不得使用空密码，不得使用全数字密码（如 11111、123456）和存在输入规律（如 1qaz2wsx）的弱密码，必须设置足够强壮的密码，最短密码长度 8 个字符，至少包含大写字母、小写字母、数字和字符中的 3 类；启用本机组策略中密码必须符合复杂性要求的策略。
配置范例	设置登录密码，至少 8 位，至少包含大写字母、小写字母、数字和字符中的 3 类。可采用“XXXX@****”组合设置密码，其中 XXXX 为长度不少于 3 位的大小写字母组合，可选择使用姓名拼音缩写，****为长度不少于 4 位的数字组合，可选择使用出生年月日或电话号码等。 进入“控制面板→管理工具→本地安全策略”，在“账户策略→密码策略”查看是否“密码必须符合复杂性要求”选择“已启动”。
适用范围	PC 机、视频会议终端及其他联网终端设备。

2.1.4 账户锁定策略

基线名称	终端账户锁定策略安全基线要求
基线要求	配置当用户连续认证失败次数超过 5 次(不含 5 次),锁定该用户使用的账户，锁定时间 20 分钟。
配置范例	进入“控制面板→管理工具→本地安全策略”,在“账户策略→账户锁定策略”: 查看“账户锁定阀值”设置。
适用范围	PC 机、视频会议终端及其他联网终端设备。

2.1.5 禁用远程服务

基线名称	终端远程服务安全基线要求
基线要求	PC 机不得开启远程桌面、Telnet、远程协助等服务。
配置范例	进入“我的电脑右键→属性→远程”，在“允许用户远程连接到此计算机”选项上不得勾选。
适用范围	PC 机。

2.2 安全策略配置

2.2.1 开启安全审核

基线名称	终端审核策略安全基线要求
基线要求	必须配置审核日志功能，审核登录事件、系统事件、账户管理、策略更改和权限使用 5 类操作行为，记录 5 类操作行为的成功和失败操作结果。
配置范例	进入“ 控制面板→管理工具→本地安全策略→审核策略”基线要求的策略全部选中“成功”和“失败”。
适用范围	PC 机。

2.2.2 关闭危险端口

基线名称	终端端口管理安全基线要求
基线要求	禁用 135、137、138、139 和 445 端口。
配置范例	点击“ 开始→运行”输入“regedit”进入“注册表编辑器”依次点击进入“HKEY_LOCAL_MACHINE→SYSTEM→CurrentControlSet→services→NetBT→Parameters”选项，在“Parameters”这个子项的右侧，点击鼠标右键，“新建→QWORD（64 位）值”，然后重命名为“SMBDeviceEnabled”，将“数值数据”的值改为 0，即可关闭 445 端口。
适用范围	PC 机。

2.2.3 临时信息清除

基线名称	终端临时信息保护安全基线要求
基线要求	在退出系统时删除临时文件夹，关机时清理虚拟内存页面文件，用户登录时不显示最后的用户名，不允许将 Everyone 权限应用于匿名用户，不允许在下次更改密码时存储 LAN Manager 的哈希值，不允许 SAM 账户和共享的匿名枚举。
配置范例	进入“ 控制面板→管理工具→本地安全策略→本次策略→安全选项”禁用以下选项：“在退出时不删除临时文件夹”、“网络访问：将 Everyone 权限应用于匿名用户”，启用以下选项：“关机：清理虚拟内存页面文件”、“交互式登录：不显示最后的用户名”、“网络安全：不要在下次更改密码时存储 LAN Manager 的哈希值”、“网络访问：不允许 SAM 账户和共享的匿名枚举”。
适用范围	PC 机。

2.2.4 运行杀毒软件

基线名称	终端杀毒软件安全基线要求
基线要求	必须安装并运行统一的企业版杀毒软件，并保持病毒库及时更新。
配置范例	安装市局指定的杀毒软件，并保证杀毒软件正常运行。
适用范围	PC 机。

2.2.5 管理用户权限控制

基线名称	终端权限控制安全基线要求
基线要求	系统重要操作如：提高计划优先级、管理审核和安全日志、取得文件或其他对象的所有权、创建一个页面文件、从远程系统强制关机、加载和卸载设备驱动程序、调试程序、执行卷维护任务和配置文件系统性能等仅允许管理用户组。
配置范例	进入“ 控制面板→管理工具→本地安全策略→本次策略→用户权限分配”将“提高计划优先级”、“管理审核和安全日志”、“取得文件或其他对象的所有权”、“创建一个页面文件”、“从远程系统强制关机”、“加载和卸载设备驱动程序”、“调试程序”、“执行卷维护任务”和“配置文件系统性能”的“安全设置”调整为 Administrators（管理用户组）。
适用范围	PC 机。

2.3 实名注册及软件安装

基线名称	终端实名注册及软件安装基线要求
基线要求	终端接入公安网必须进行实名注册，必须安装一机两用客户端、安全助手和终端安全接入客户端，办理公安网入网审批流程。
配置范例	终端使用者进行实名注册安装一机两用客户端，安装终端安全接入客户端并通过终端安全接入系统入网审批，下载安装公安网安全助手。
适用范围	PC 机。

第3章 服务器安全基线

3.1 账户及口令

3.1.1 管理账户安全

基线名称	操作系统管理账户安全基线要求
基线要求	不得使用 administrator、admin、sa 等默认用户名作为管理账户；禁用 guest 等来宾账户。
配置范例	进入“控制面板→管理工具→计算机管理”，在“系统工具→本地用户和组”: 缺省账户 Administrator一〉属性，Guest 账户→属性。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统)。

3.1.2 密码有效期

基线名称	操作系统密码有效期安全基线要求
基线要求	账户口令的生存期不长于 90 天，修改密码 5 次内不得重复。
配置范例	进入“控制面板→管理工具→本地安全策略”,在“账户策略→密码策略”,查看“密码最长存留期”和“强制密码历史”。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统） 。

3.1.3 密码复杂度

基线名称	操作系统密码复杂度安全基线要求
基线要求	操作系统账户不得使用空密码，不得使用全数字密码（如 11111、123456）和存在输入规律（如 1qaz2wsx）的弱密码，必须设置足够强壮的密码，最短密码长度 8 个字符，至少包含大写字母、小写字母、数字和字符中的 3 类；启用本机组策略中密码必须符合复杂性要求的策略。
配置范例	设置登录密码，至少 8 位，至少包含大写字母、小写字母、数字和字符中的 3 类，可采用“XXXX@****”组合设置密码，其中 XXXX 为长度不少于 3 位的大小写字母组合，可选择使用姓名拼音缩写，****为长度不少于 4 位的数字组合，可选择使用出生年月日或电话号码等； 进入“控制面板→管理工具→本地安全策略”，在“账户策略→密码策略”查看是否“密码必须符合复杂性要求”选择“已启动”。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.1.4 账户锁定策略

基线名称	操作系统账户锁定策略安全基线要求
基线要求	配置当用户连续认证失败次数超过 5 次(不含 5 次),锁定该用户使用的账户，锁定时间 20 分钟。
配置范例	进入“控制面板→管理工具→本地安全策略”,在“账户策略→账户锁定策略”: 查看“账户锁定阀值”设置。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统)。

3.1.5 登录超时锁定

基线名称	操作系统登录操作超时锁定安全基线要求
基线要求	配置当用户操作空闲时间超过 20 分钟后，中断会话连接。
配置范例	进入“组策略→计算机配置→管理模板 Windows 组件→终端服务”，在“会话”中查看“空闲会话限制”时间，设置为 20 分钟。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统)。

3.1.6 远程管理加密

基线名称	操作系统远程管理安全基线要求
基线要求	服务远程管理必须采用 RDP（SSL 加密）或 SSH 等加密协议。
配置范例	进入“控制面板→管理工具→终端服务配置连接”，在“RDP—Tcp→属性”：查看“RDP—Tcp 属性”设置，选择 SSL。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.1.7 双因子认证登录

基线名称	操作系统登录认证安全基线要求
基线要求	重要服务器远程登录时，应采用双因子认证方式，在用户名、密码的基础上增加证书、Ukey 等鉴别因子，保证登录用户身份合法。
配置范例	通过堡垒机设备配合网络安全设备的访问控制策略实现。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.1.8 远程登录地址限制

基线名称	操作系统远程登录安全基线要求
基线要求	严格限制能够远程登录服务器的接入方式和地址范围，采用白名单方式，仅允许必要的终端以固定的协议（如远程桌面、SSH） 远程登录到服务器。
配置范例	通过主机防火墙、网络设备或安全设备的访问控制功能实现。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2 安全策略配置

3.2.1 开启安全审核

基线名称	操作系统审核策略安全基线要求
基线要求	必须配置审核日志功能，审核登录事件、系统事件、账户管理、策略更改和权限使用 5 类操作行为，记录 5 类操作行为的成功和失败操作结果。
配置范例	进入“ 控制面板→管理工具→本地安全策略→审核策略”基线要求的策略全部选中“成功”和“失败”。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.2 审核日志保护

基线名称	操作系统审核日志保护安全基线要求
基线要求	对于服务器的审核日志，应在服务器本地以外，另外保存一份备份日志，保留期限不少于 6 个月，保证设备出现问题时，可以找到重要的日志信息。
配置范例	通过独立的日志服务器、审计系统或异地备份等方式，实现服务器日志的保护和备份。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.3 日志时间校准

基线名称	操作系统日志时间准确性安全基线要求项
基线要求	必须配置时钟同步服务器,保证服务器日志记录时间的准确性。
配置范例	进入“ 控制面板→日期和时间→internet 时间→更改设置”配置正确的时钟同步服务器地址或域名。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统)。

3.2.4 关闭危险端口

基线名称	操作系统端口管理安全基线要求
基线要求	禁用 135、137、138、139 和 445 端口。
配置范例	点击“ 开始→运行”输入“regedit”进入“注册表编辑器”依次点击进入“HKEY_LOCAL_MACHINE→SYSTEM→CurrentControlSet→services→NetBT→Parameters”选项，在“Parameters”这个子项的右侧，点击鼠标右键,“新建→QWORD（64 位）值”，然后重命名为“SMBDeviceEnabled”，将“数值数据”的值改为 0，即可关闭 445 端口。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统)。

3.2.5 访问控制策略

基线名称	操作系统访问控制安全基线要求
基线要求	服务器应配置严格的访问控制策略,仅允许必要的地址和端口访问本机 。
配置范例	访问控制策略采用白名单方式,如数据库服务器可通过防火墙配置访问控制列表，仅允许相关应用服务器、堡垒机和远程管理用户终端等通过特定端口访问。根据应用的用户数量和信息敏感程度,限制应用访问范围（特殊情况须由专家讨论决定)。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统)。

3.2.6 运行杀毒软件

基线名称	操作系统杀毒软件安全基线要求
基线要求	服务器必须安装并运行统一的企业版杀毒软件,并保持病毒库及时更新。
配置范例	必须安装市局指定的杀毒软件并保证杀毒软件正常运行。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统)。

3.2.7 临时信息清除

基线名称	操作系统临时信息保护安全基线要求
基线要求	在退出系统时删除临时文件夹，关机时清理虚拟内存页面文件，用户登录时不显示最后的用户名，不允许将 Everyone 权限应用于匿名用户，不允许在下次更改密码时存储 LAN Manager 的哈希值，不允许 SAM 账户和共享的匿名枚举。
配置范例	进入“ 控制面板→管理工具→本地安全策略→本次策略→安全选项”禁用以下选项：“在退出时不删除临时文件夹”、“网络访问：将 Everyone 权限应用于匿名用户”，启用以下选项：“关机：清理虚拟内存页面文件”、“交互式登录：不显示最后的用户名”、“网络安全：不要在下次更改密码时存储 LAN Manager 的哈希值”、“网络访问：不允许 SAM 账户和共享的匿名枚举”。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.8 管理用户权限控制

基线名称	操作系统权限控制安全基线要求
基线要求	系统重要操作如：提高计划优先级、管理审核和安全日志、取得文件或其他对象的所有权、创建一个页面文件、从远程系统强制关机、加载和卸载设备驱动程序、调试程序、执行卷维护任务和配置文件系统性能等仅允许管理用户组。
配置范例	进入“ 控制面板→管理工具→本地安全策略→本次策略→用户权限分配”将“提高计划优先级”、“管理审核和安全日志” 、“取得文件或其他对象的所有权”、“创建一个页面文件” 、“从远程系统强制关机” 、“加载和卸载设备驱动程序” 、“调试程序”、“执行卷维护任务”和“配置文件系统性能”的“安全设置”调整为 Administrators（管理用户组）。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.2.9 服务器运行状态监控

基线名称	操作系统运行状况监控安全基线要求
基线要求	重要服务器必须监控操作系统运行状况，监控范围包含 CPU、内存、硬盘等，设置服务水平阈值，在系统的服务水平降低到一定值时进行报警。
配置范例	通过虚拟机管理工具、服务器运行监控软件等工具软件实现对系统运行状态的监控和报警。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

3.3 实名注册及软件安装

基线名称	服务器实名注册及软件安装基线要求
基线要求	Windows 操作系统服务器接入公安网必须进行实名制注册安装一机两用客户端及公安网安全助手。其他操作系统必须在一机两用系统内申请设备保护，并填报相关设备信息。
配置范例	服务器安装一机两用客户端和公安网安全助手，或者申请保护设置。
适用范围	所有服务器（包含 Windows、Linux 及 UNIX 等操作系统）。

第4章 网络、安全设备安全基线

4.1 账户及口令

4.1.1 管理账户安全

基线名称	网络、安全设备管理账户安全基线要求
基线要求	所有网络、安全设备不得使用 admin、root 等常见默认用户名，不同管理员应使用不同的管理账户。
配置范例	local—user XXXX。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.2 口令加密存储

基线名称	网络、安全设备用户口令加密存储安全基线要求
基线要求	用户口令必须使用不可逆加密算法加密后保存于配置文件中。
配置范例	password cipher XXXX
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.3 密码复杂度

基线名称	网络、安全设备密码复杂度安全基线要求
基线要求	不得使用空密码，不得使用全数字密码（如 11111、123456）和存在输入规律（如 1qaz2wsx）的弱密码，必须设置足够强壮的密码，最短密码长度 8 个字符，至少包含大写字母、小写字母、数字和字符中的 3 类；可采用“XXXX@****”组合设置密码，其中 XXXX 为长度不少于 3 位的大小写字母组合,可选择使用姓名拼音缩写，****为长度不少于 4 位的数字组合，可选择使用出生年月日或电话号码等。
配置范例	根据设备情况，选择密码复杂度符合要求的配置选项。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.4 账户锁定策略

基线名称	网络、安全设备账户锁定安全基线要求
基线要求	网络、安全设备应启用登录失败处理功能，当用户连续认证失败次数超过 5 次（不含 5 次），锁定该用户使用的账户，锁定时间 20 分钟。
配置范例	password—control login—attempt 5 exceed lock—time 20
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.5 登录超时锁定

基线名称	网络、安全设备登录操作超时锁定安全基线要求
基线要求	网络、安全设备必须启用登录操作超时锁定功能，可通过设备登录配置或安全设备（如防火墙、堡垒机）配置实现，操作空闲时间超过（最长）20 分钟后，断开会话连接。
配置范例	Line vty Exec—timeout 20 0
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.6 远程管理加密

基线名称	网络、安全设备远程管理安全基线要求
基线要求	网络、安全设备远程登录时，使用 SSH 或 https 等加密方式。
配置范例	user—interface vty 0 4 authentication—mode scheme protocol inbound ssh local—user XXXX ….. service—type ssh
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.1.7 登录地址限制

基线名称	网络、安全设备远程登录安全基线要求
基线要求	严格限制能够远程登录和管理网络、安全设备的登录地址范围，采用白名单方式，仅允许必要的终端以固定的协议（如 SSH、https 等） 远程登录和管理网络、安全设备。
配置范例	通过设备安全配置和网络、安全设备的访问控制策略实现。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.2 安全策略配置

4.2.1 开启安全审计

基线名称	网络、安全设备审计策略安全基线要求
基线要求	开启日志审计功能，审计系统日志，操作日志和告警日志等。
配置范例	根据具体设备自行配置，开启日志功能。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.2.2 审计日志保护

基线名称	网络、安全设备日志保护安全基线要求项
基线要求	日志信息通过 SYSLOG 等方式传输至日志服务器备份保存，保留期限不少于 6 个月。
配置范例	搭建 SYSLOG 日志服务器，接收保存各类设备发送的 SYSLOG 日志。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.2.3 日志时间校准

基线名称	网络、安全设备日志时间准确性安全基线要求项
基线要求	开启 NTP 服务，保证日志功能记录的时间的准确性。所有网络、安全设备与 NTP SERVER 之间要开启认证功能。
配置范例	ntp-service authentication enable ntp-service unicast-server 192.168.1.1
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

4.2.4 访问控制策略

基线名称	网络系统访问控制安全基线要求
基线要求	在同一网络中，应当根据安全级别不同将网络划分为不同的安全区域，各个安全区域的边界处分别部署具有访问控制隔离功能的网络安全设备，并配置严格的访问控制策略。
配置范例	访问控制策略应采用白名单方式，控制粒度至少包含源、目的地址和端口号（协议）。
适用范围	所有网络系统。

4.2.5 入侵攻击防御

基线名称	网络系统入侵防御安全基线要求
基线要求	在网络重要区域（如核心网络交换机、服务器汇聚交换机等）必须部署入侵防御或检测设备，对服务器区和其他重要区域的入侵行为进行检测和阻断。
配置范例	可选择入侵防御系统或入侵检测系统，必须能够对入侵行为进行发现和阻断，并提供入侵告警功能。
适用范围	所有网络系统。

4.2.6 网络系统运行状态监控

基线名称	网络系统运行状态监控安全基线要求
基线要求	监控网络系统运行状况，监控范围包含所有网络设备运行情况和带宽、流量等信息。
配置范例	通过网络管理软件、IT 运维管理软件等工具软件实现对网络系统运行状态的监控和报警。
适用范围	所有网络、安全设备（如交换机、路由器、防火墙、IPS 等）。

第5章 应用系统开发安全基线

5.1 身份与访问控制

5.1.1 账户锁定策略

基线名称	Web 应用账户锁定策略安全基线要求项
基线说明	用户登录失败 3-5 次后，系统自动锁定账户不少于 15 分钟，并记录日志。
检测方式	尝试使用错误用户名口令失败登录多次,查看是否允许无限制尝试。
符合判定依据	用户登录失败 3-5 次后系统自动锁定账户。

5.1.2 登录图片验证码

基线名称	Web 应用登录图片验证码安全基线要求项
基线说明	用户登录需输入图片验证码,以防止固定密码暴力猜测账户。
检测方式	检查登录认证界面输入项,并右键点击图片查看链接属性。
符合判定依据	要求包含图片验证码输入项,并且图片链接属性不包含图片中验证码。

5.1.3 口令传输

基线名称	Web 应用口令传输策略安全基线要求项
基线说明	应采用密文方式传输用户登录密码。
检测方式	尝试登录系统，并使用抓包工具查看交互过程中在网络传输的内容。
符合判定依据	要求不得出现明文用户名和口令。

5.1.4 保存登录功能

基线名称	Web 应用保存登录安全基线要求项
基线说明	不提供“保存登录”功能，不得在浏览器中缓存用户登录信息。
检测方式	检查登录界面是否提供了保存登录功能。
符合判定依据	不得提供“保存登录”功能，浏览器缓存中不能存在用户登录信息。

5.1.5 纵向访问控制

基线名称	Web 应用纵向访问安全基线要求项
基线说明	合理进行纵向访问控制，不允许非授权用户访问管理功能。
检测方式	了解是否有不允许普通用户访问的功能，尝试直接在浏览器中访问功能链接。
符合判定依据	用户不得跨权限访问受控页面。

5.1.6 横向访问控制

基线名称	Web 应用横向访问安全基线要求项
基线说明	合理进行横向访问控制,不允许用户访问其他用户的敏感数据。
检测方式	了解是否存在敏感信息,检查是否对个人敏感信息进行了有效保护。
符合判定依据	用户不得跨权限查看其它用户受保护的敏感信息。

5.1.7 敏感资源访问

基线名称	Web 应用敏感资源访问安全基线要求项
基线说明	必须严格限制对敏感资源的访问，如重要用户数据、后台管理和日志记录等。
检测方式	查看服务器上敏感资源的访问权限设置。
符合判定依据	严格限制敏感资源的访问权限。

5.1.8 证书单轨制登录

基线名称	Web 应用证书登录安全基线要求项
基线说明	必须使用公安数字证书作为用户身份认证与应用权限管理的依据。
检测方式	检查应用系统用户登录方式,是否只有证书登录一种方式。
符合判定依据	用户登录应用系统只能够使用公安数字证书登录。

5.2 会话管理

5.2.1 会话超时

基线名称	Web 应用会话超时安全基线要求项
基线说明	当用户长时间不操作时，系统自动终止超时会话。
检测方式	登录系统后不操作，等待合理的时间间隔，检查系统是否会自动断开。
符合判定依据	要求预先设计的时间间隔后查看页面自动中止超时会话。

5.2.2 会话终止

基线名称	Web 应用会话终止安全基线要求项
基线说明	系统需提供“退出”功能，允许用户强制终止当前的会话。
检测方式	登录系统后，点击系统提供的“退出”功能，检查浏览器能否自动关闭或者退至系统登录页面。
符合判定依据	点击系统提供的“退出”功能后，检查浏览器能够自动关闭或者退至系统登录页面；若退至登录页面，浏览器不得返回系统操作界面，必须重新做用户认证登录后，才能进行正常操作。

5.2.3 会话标识

基线名称	Web 应用会话标识安全基线要求项
基线说明	应用系统会话标识必须是随机生成，防止攻击者猜测标识或依据当前标识推导后续的标识。
检测方式	检查系统会话标识的格式，检查会话标识方式，是否存在简单的逻辑关系。
符合判定依据	多个会话标识不得存在简单明了的逻辑关系，必须具有随机性。

5.3 代码质量

5.3.1 防范跨站脚本攻击

基线名称	Web 应用防范跨站脚本安全基线要求项
基线说明	应用系统应当对用户的输入内容进行预处理,不得未经检查将用户输入内容直接输出到用户浏览器,防范跨站脚本攻击。
检测方式	检查系统是否存在跨站脚本攻击漏洞。例如在能够回显的输入框输入<script> alert(“xss”)</script>。
符合判定依据	要求系统能够将输入内容中的控制字当作纯文本内容处理。

5.3.2 防范 SQL 注入攻击

基线名称	Web 应用防范 SQL 注入安全基线要求项
基线说明	系统必须对用户的输入内容进行预处理,防止用户利用输入内容构建 SQL 语句。
检测方式	检查系统是否存在 SQL 注入漏洞。例如在输入框中输入“’”字符。
符合判定依据	系统要使用诸如 prepared statement 等方式防止 SQL 注入，将输入内容中的控制字也当作纯文本处理。

5.3.3 防范路径遍历攻击

基线名称	Web 应用防范路径遍历安全基线要求项
基线说明	系统必须对用户的输入内容进行预处理，防止用户利用输入内容构建文件路径进行路径遍历攻击。
检测方式	尝试在 URL 与输入中构造文件路径并查看页面反应。
符合判定依据	不允许通过构造文件路径的方式直接查看文件。

5.3.4 防范命令注入攻击

基线名称	Web 应用防范命令注入安全基线要求项
基线说明	系统必须对用户的输入内容进行预处理，防止用户利用输入内容构造操作系统命令并执行。
检测方式	尝试在各个输入点进行命令注入攻击。
符合判定依据	命令注入攻击不得成功。

5.3.5 防范其他常见注入攻击

基线名称	Web 应用防范其它注入安全基线要求项
基线说明	系统不得存在 LDAP 注入、XML 注入、XPATH 注入、SMTP 注入等漏洞。
检测方式	尝试在各个输入点进行其它常见注入攻击。
符合判定依据	各类注入攻击不得成功。

5.3.6 防范上传后门脚本

基线名称	Web 应用防范上传漏洞安全基线要求项
基线说明	提供文件上传功能的系统,必须对上传的内容进行检测和处理，防止用户上传后门脚本。
检测方式	利用系统提供的上传功能，测试能否上传恶意文件。
符合判定依据	各类上传攻击不得成功。

5.3.7 保证释放资源

基线名称	Web 应用释放资源基线要求项
基线说明	应用系统必须及时释放与回收资源,保证合法用户的正常使用。
检测方式	分析检查正常与异常流程中资源释放的动作。
符合判定依据	资源释放覆盖所有流程分支。

5.4 内容管理

5.4.1 加密存储敏感信息

基线名称	Web 应用加密存储敏感信息基线要求项
基线说明	应用系统应当使用国产密码算法对账户、密码等敏感信息做加密保护。
检测方式	分析系统中敏感信息的存储与加密，是否使用安全的国产密码算法。
符合判定依据	要求敏感信息在存储时，必须使用安全的国产密码算法。

5.4.2 避免泄露敏感技术细节

基线名称	Web 应用信息泄漏基线要求项
基线说明	应用系统不得向用户反馈详细的错误信息，只反馈页面友好错误提示。
检测方式	分析各个页面的源代码，查看提示页面，尤其是出错提示页面是否存在不安全的信息。
符合判定依据	各个页面不得包含技术性注释，各个提示页面不得包含 Web 服务器版本、源代码等信息。

5.5 密码算法

5.5.1 密码算法安全

基线名称	Web 应用密码算法基线要求项
基线说明	应用系统应当采用国产密码算法保护。
检测方式	检查系统中使用的密码算法，是否为国产密码算法。
符合判定依据	不得使用已经被证明为不安全的算法、自定义不安全算法或非国产密码算法。

5.5.2 密钥管理安全

基线名称	Web 应用密钥管理基线要求项
基线说明	采用国产密码算法保护的应用系统,必须妥善保管密钥，并制定和执行相应的密钥管理办法。
检测方式	检查系统中使用的密钥管理方式,是否存在不安全的密钥管理情形。
符合判定依据	制定有密钥管理办法，且得到严格执行。

5.6 交付安全

5.6.1 应用系统交付安全

基线名称	应用系统交付安全基线要求项
基线说明	开发公司交付应用系统时，交付内容中不得包含调试页面、后门管理页面、备份数据（如程序源码、认证信息和注释信息等）、默认超级用户等。
检测方式	通过常规页面检测和渗透测试等方式，检查是否存在调试页面、后门管理页面、备份数据（如程序源码、认证信息和注释信息等）和默认超级用户等。
符合判定依据	不存在调试页面、后门管理页面、备份数据（如程序源码、认证信息和注释信息等）及默认超级用户等。

5.6.2 业务逻辑安全

基线名称	应用系统业务逻辑安全基线要求项
基线说明	开发公司交付应用系统前应对系统的业务逻辑操作进行检查，避免存在业务漏洞。
检测方式	需由第三方测评机构进行软件安全测评或渗透测试，检测是否存在业务逻辑漏洞。
符合判定依据	提供相关测试证明文件或在验收前组织第三方测评机构进行软件安全测评或渗透测试，消除业务漏洞。