|  |
| --- |
| **老男孩信息系统安全配置基线**  **Apache中间件分册（初稿）** |
| **版本 V1.0** |

**二○一九年一月**

|  |  |  |  |
| --- | --- | --- | --- |
| ■版本变更记录 | | | |
| 时间 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| 目录 |
| [一. 概述 4](#_Toc408347845)  [1.1适用范围 4](#_Toc408347846)  [1.2规范依据 4](#_Toc408347847)  [1.3实施策略 4](#_Toc408347848)  [二. 安全配置基线标准 5](#_Toc408347849)  [2.1访问控制 5](#_Toc408347850)  [2.1.1配置Apache运行账户 5](#_Toc408347851)  [2.1.2禁止访问外部文件 6](#_Toc408347852)  [2.1.3禁止目录浏览 7](#_Toc408347853)  [2.1.4配置敏感文件访问权限 8](#_Toc408347854)  [2.1.5配置使用安全的HTTP请求 8](#_Toc408347855)  [2.2安全审计 9](#_Toc408347856)  [2.2.1配置安全日志 9](#_Toc408347857)  [2.3资源控制 10](#_Toc408347858)  [2.3.1配置抗拒绝服务攻击参数 10](#_Toc408347859)  [2.3.2设置连接数 11](#_Toc408347860)  [2.4其它安全项 13](#_Toc408347861)  [2.4.1删除缺省文件 13](#_Toc408347862)  [2.4.2设置隐藏Apache版本号 14](#_Toc408347863)  [2.4.3配置错误页面处理 14](#_Toc408347864)  [2.4.4更新补丁 15](#_Toc408347865)  [三. 评审与修订 16](#_Toc408347866) |

1. 概述
   1. 适用范围

本配置基线适用于老男孩的Apache中间件，主要涉及Apache中间件安全配置方面的基本要求，用于指导安全例行工作、新系统入网安全检查等场合。

在未特别说明的情况下，均适用于所有运行Apache中间件系统。

* 1. 规范依据

根据老男孩目前Apache中间件安全现状，综合参考各信息系统运维部门的意见，结合金融行业等级保护实施指引，制定适合于老男孩的基线配置规范。

主要参考依据如下：

* JR/T0071-2012《金融行业信息系统信息安全等级保护实施指引》（2012年7月发布）
  1. 实施策略

结合网络和信息系统建设情况，考虑安全配置项影响的范围，结合以往工作经验，提出如下安全项目实施策略：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **配置类别** | **安全基线项目名称** | **实施策略** |
| 1 | 访问控制 | 配置Apache运行账户 | 必须实施 |
| 2 | 访问控制 | 禁止访问外部文件 | 必须实施 |
| 3 | 访问控制 | 禁止目录浏览 | 必须实施 |
| 4 | 访问控制 | 配置敏感文件访问权限 | 必须实施 |
| 5 | 访问控制 | 配置使用安全的HTTP请求 | 必须实施 |
| 6 | 安全审计 | 配置安全日志 | 必须实施 |
| 7 | 资源控制 | 配置抗拒绝服务攻击参数 | 按需实施 |
| 8 | 资源控制 | 设置连接数 | 按需实施 |
| 9 | 其它安全项 | 删除缺省文件 | 必须实施 |
| 10 | 其它安全项 | 设置隐藏Apache版本号 | 必须实施 |
| 11 | 其它安全项 | 配置错误页面处理 | 必须实施 |
| 12 | 其它安全项 | 更新补丁 | 按需实施 |

1. 安全配置基线标准
   1. 访问控制
      1. 配置Apache运行账户

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置Apache运行账户（必须实施） |
| **安全基线编号** | 中间件-Apache-1 |
| **安全基线项说明** | 以专门的用户账户和组运行Apache |
| **配置方法** | 以下操作使用root账号或者有httpd修改权限账号进行修改。  修改httpd.conf配置文件，添加如下语句：  User apache  Group apachegroup  其中apache、apachegroup分别是为Apache创建的用户和组。  说明：  应为apache的用户和组设置适当的权限。 |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆   1. 检查是否使用非专用账户（如root）运行apache 2. 查看httpd.conf文件，查看是否定义了如下形式的脚本。   User apache  Group apachegroup  检查apache用户和组的权限，该用户不应该具有最高的管理员权限。 |
| **依据** | 6.2.1.4，2）访问控制（S3），d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。 |
| **备注** |  |

* + 1. 禁止访问外部文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁止访问外部文件（必须实施） |
| **安全基线编号** | 中间件-Apache-2 |
| **安全基线项说明** | 禁止Apache访问Web目录之外的任何文件。 |
| **配置方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  编辑httpd.conf配置文件，   1. 设置外部不可访问。   <Directory /> /\*\* “ / ”为外部文件目录，如/opt \*\*/  Order Deny,Allow  Deny from all  </Directory>   1. 设置可访问目录，   <Directory /web>  Order Allow,Deny  Allow from all  </Directory>  说明： /web为网站根目录。 |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  1. 无法访问Web目录之外的文件。  2. 访问服务器上不属于Web目录的一个文件，结果应无法显示。 |
| **依据** | 6.2.1.4，2）访问控制（S3），a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。 |
| **备注** |  |

* + 1. 禁止目录浏览

|  |  |
| --- | --- |
| **安全基线项目名称** | 禁止目录浏览（必须实施） |
| **安全基线编号** | 中间件-Apache-3 |
| **安全基线项说明** | 禁止当Apahce目录没有默认首页时，显示目录文件 |
| **配置方法** | **涉及的系统文件：**httpd.conf  以下操作使用root账号或者有httpd修改权限账号登陆   1. 编辑httpd.conf配置文件，   <Directory "/web">  Options Indexes FollowSymLinks #删掉Indexes  AllowOverride None  Order allow,deny  Allow from all  </Directory>  将Options Indexes FollowSymLinks中的Indexes 去掉，就可以禁止Apache 显示该目录结构。Indexes 的作用就是当该目录下没有 index.html文件时，就显示目录结构。  重新启动Apache服务 |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  1.当WEB目录中没有默认首页如index.html文件时，不会列出目录内容  2.检查httpd.conf文件，查看是否存在Options Indexes FollowSymLinks语句。若存在，则不符合要求。 |
| **依据** | 6.2.1.4，2）访问控制（S3），b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。 |
| **备注** |  |

* + 1. 配置敏感文件访问权限

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置敏感文件访问权限（必须实施） |
| **安全基线编号** | 中间件-Apache-4 |
| **安全基线项说明** | 严格设置配置文件和日志文件等敏感文件的访问权限，防止未授权访问 |
| **配置方法** | 以下操作使用root账号或者有httpd修改权限账号登陆。  使用命令“chmod 600 /etc/httpd/conf/httpd.conf”设置配置文件为属主可读写，其他用户无权限。  使用命令“chmod 644 /var/log/httpd/\*.log”设置日志文件为属主可读写，其他用户只读权限。 |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  使用命令查看配置文件和日志文件的权限   1. 使用如下命令查看httpd.conf文件权限是否符合要求。   ls -l /etc/httpd/conf/httpd.conf  若为-rw-------即符合要求，否则为不合格。使用chmod命令配置  2．按照上述方法查看.log格式的文件权限是否符合要求。  若为-rw-r—r—即为符合要求，否则为不合格。 |
| **依据** | 6.2.1.4，2）访问控制（S3），g) 宜依据安全策略严格控制用户对有敏感标记重要信息资源的操作。 |
| **备注** |  |

* + 1. 配置使用安全的HTTP请求

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置使用安全的HTTP请求（必须实施） |
| **安全基线编号** | 中间件-Apache-5 |
| **安全基线项说明** | 禁用PUT、DELETE等危险的HTTP方法 |
| **配置方法** | **涉及系统文件：httpd.conf**  在httpd.conf中，找到LimitExcept配置项，并按如下格式添加 GEP POST命令：  <LimitExcept GET POST> Deny from all< /LimitExcept> |
| **检查方法** | 参考安全配置方法查看httpd.conf中是否有相应内容 |
| **依据** | 6.2.1.4 应用安全：访问控制（S3）：a) 应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；  6.2.1.4 应用安全：访问控制（S3）：b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作； |
| **备注** |  |

* 1. 安全审计
     1. 配置安全日志

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置安全日志（必须实施） |
| **安全基线编号** | 中间件-Apache-6 |
| **安全基线项说明** | 启用日志可以回溯事件进行检查或审计，日志详细信息级别如果配置不当，会缺少必要的审计信息。  设备应配置日志功能，对运行错误、用户访问等进行记录，记录内容包括时间，用户使用的IP地址等内容。 |
| **配置方法** | **涉及的系统文件：**httpd.conf  **涉及参数：**  LogLevel //记录内容  ErrorLog //日志文件  LogFormat //日志格式  ------------------------------------------------------------------------------------  以下操作使用root账号或者有httpd修改权限账号登陆  编辑httpd.conf配置文件，设置日志记录文件、记录内容、记录格式。  LogLevel notice  ErrorLog logs/error\_log  LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Accept}i\" \"%{Referer}i\" \"%{User-Agent}i\"" combined  CustomLog logs/access\_log combined  ------------------------------------------------------------------------------------  ErrorLog指令设置错误日志文件名和位置。错误日志是最重要的日志文件，Apache httpd将在这个文件中存放诊断信息和处理请求中出现的错误。若要将错误日志送到Syslog，则设置：ErrorLog syslog。  CustomLog指令设置访问日志的文件名和位置。访问日志中会记录服务器所处理的所有请求。  LogFormat设置日志格式。LogLevel用于调整记录在错误日志中的信息的详细程度，建议设置为notice。 |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  1.查看logs目录中相关日志文件内容，记录完整。  2.查看相关日志记录，要求对运行错误、用户访问等进行记录，记录内容包括时间，用户使用的IP地址等内容。 |
| **依据** | 6.2.1.4 应用安全：安全审计（G3）：a) 应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计； |
| **备注** | 必须记录日志，但考虑到磁盘I/O，不建议记录全部日志。 |

* 1. 资源控制
     1. 配置抗拒绝服务攻击参数

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置抗拒绝服务攻击参数（按需实施） |
| **安全基线编号** | 中间件-Apache-7 |
| **安全基线项说明** | 通过合理设置连接活跃时间和超时时间，减轻“拒绝服务攻击”的影响。 |
| **配置方法** | **涉及的系统文件：**httpd.conf  **涉及参数：**  KeepAlive //保持连接活跃  Timeout //客户端与服务器端建立连接前的时间间隔  KeepAliveTimeout //连接活跃时间  以下操作使用root账号或者有httpd修改权限账号登陆   1. 编辑httpd.conf配置文件，   Timeout 10 KeepAlive On  KeepAliveTimeout 15  AcceptFilter http data  AcceptFilter https data  重新启动Apache服务 |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  检查httpd.conf文件，查看是否进行了如下设置：  Timeout 10 KeepAlive On  KeepAliveTimeout 15  AcceptFilter http data  AcceptFilter https data |
| **依据** | 6.2.1.4 应用安全：资源控制（A3）：a) 对于有会话或短连接的应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话； |
| **备注** |  |

* + 1. 设置连接数

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置连接数（按需实施） |
| **安全基线编号** | 中间件-Apache-8 |
| **安全基线项说明** | 根据机器性能和业务需求，设置最大最小连接数 |
| **配置方法** | **涉及的系统文件：**httpd.conf  **涉及参数：**  StartServers //默认开启进程数  MinSpareServers //最小开启进程数  MaxSpareServers //最大开启进程数  MaxClients //最大连接数  MaxRequestsPerChild //每个子进程处理的请求数量  ServerLimit //系统最大连接数  ------------------------------------------------------------------------------------------  以下操作使用root账号或者有httpd修改权限账号登陆  使用httpd -l 检查Apache的工作模式，如列出prefork.c ，则进行下列操作：  修改httpd.conf文件找到  <IfModule prefork.c>  StartServers 8  MinSpareServers 5  MaxSpareServers 20  MaxClients 150  MaxRequestsPerChild 1000  </IfModule>  修改 MaxClients 150 为需要的连接数，如1500  ServerLimit 1500 //连接数大于 256 需设置此项  MaxClients 1500  然后保存退出。重新启动http 服务：  /etc/rc.d/init.d/httpd restart |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  使用httpd -l 检查Apache的工作模式，如列出prefork.c ，则检查httpd.conf中的<IfModule prefork.c>模块设置是否满足业务需求 |
| **依据** | 6.2.1.4 应用安全：资源控制（A3）：b) 应能够对系统的最大并发会话连接数进行限制； |
| **备注** |  |

* 1. 其它安全项
     1. 删除缺省文件

|  |  |
| --- | --- |
| **安全基线项目名称** | 删除缺省文件（必须实施） |
| **安全基线编号** | 中间件-Apache-9 |
| **安全基线项说明** | 删除缺省安装的无用文件。 |
| **配置方法** | **涉及的系统文件：**  apache2/htdocs  apache2/cgi-bin  apache2/manual  以下操作使用root账号或者有httpd修改权限账号登陆  删除缺省HTML文件，位置为apache2/htdocs下的默认目录及文件。  删除缺省的CGI脚本，位置为apache2/cgi-bin目录下的所有文件。  删除Apache说明文件，位置为apache2/manual目录  注：根据安装步骤不同和版本不同，某些目录或文件可能不存在或位置不同。 |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  检查如下目录中的文件是否存在。  缺省HTML文件，位置为apache2/htdocs目录。  缺省的CGI脚本，位置为apache2/cgi-bin目录。  Apache说明文件，位置为apache2/manual目录 |
| **依据** | 6.2.1.4 应用安全：剩余信息保护（S3）：b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。 |
| **备注** |  |

* + 1. 设置隐藏Apache版本号

|  |  |
| --- | --- |
| **安全基线项目名称** | 设置隐藏Apache版本号（必须实施） |
| **安全基线编号** | 中间件-Apache-10 |
| **安全基线项说明** | 隐藏Apache的版本号及其它敏感信息。 |
| **配置方法** | **涉及的系统文件：**httpd.conf  **涉及参数：**  ServerSignature //服务器标示  ServerTokens // http头部返回的apache版本信息  以下操作使用root账号或者有httpd修改权限账号登陆  修改httpd.conf配置文件：  ServerSignature Off  ServerTokens Prod |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  检查httpd.conf配置文件，检查其是否进行了如下配置。  ServerSignature Off  ServerTokens Prod |
| **依据** | 6.2.1.4 应用安全：剩余信息保护（S3）：b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。 |
| **备注** |  |

* + 1. 配置错误页面处理

|  |  |
| --- | --- |
| **安全基线项目名称** | 配置错误页面处理（必须实施） |
| **安全基线编号** | 中间件-Apache-11 |
| **安全基线项说明** | Apache默认的错误页面会泄露系统及应用的敏感信息。因此需要采用自定义错误页面的方式防止信息泄露的问题。 |
| **配置方法** | **涉及的系统文件：**httpd.conf  **涉及参数：**  ErrorDocument //错误文件  ----------------------------------------------------------------------------------------------  以下操作使用root账号或者有httpd修改权限账号登陆   1. 修改httpd.conf配置文件：   ErrorDocument 400 /custom400.html  ErrorDocument 401 /custom401.html  ErrorDocument 403 /custom403.html  ErrorDocument 404 /custom404.html  ErrorDocument 405 /custom405.html  ErrorDocument 500 /custom500.html  其中，Customxxx.html为要设置的错误页面。需要手动建立相关文件并自定义内容。   1. 重新启动Apache服务 |
| **检查方法** | 以下操作使用root账号或者有httpd修改权限账号登陆  1.查看httpd.conf文件，查看定义的错误文件  2.在浏览器中浏览相关文件，检查是否泄漏了敏感信息 |
| **依据** | 6.2.1.4 应用安全：软件容错（A3）：c) 应能够有效屏蔽系统技术错误信息，不将系统产生的错误信息直接反馈给客户。 |
| **备注** |  |

* + 1. 更新补丁

|  |  |
| --- | --- |
| **安全基线项目名称** | 更新补丁（建议实施） |
| **安全基线编号** | 中间件-Apache-12 |
| **安全基线项说明** | 在不影响业务的情况下，升级解决高危漏洞，而且该补丁要通过实验测试。 |
| **配置方法** | 访问http://httpd.apache.org/download.cgi，查看最新的apache版本，在实验室测试通过的前提下，编译升级apache，以解决高危漏洞。 |
| **检查方法** | 使用安全漏洞扫描工具对Apache中间件进行扫描，或通过搜索引擎检索当前版本脆弱性来检查是否存在高危安全漏洞。 |
| **依据** |  |
| **备注** |  |

1. 评审与修订

本标准由老男孩定期进行审查，根据审视结果修订标准，并颁发执行。