Apache 系统加固规范

0psec. cn

2010 年 9 月

目 录

本文档适用于Apache服务器。本规范明确了Apache服务器安全配置方面的基本要求。

1 账号管理、认证授权

1.1.1 SHG-Apache-01-01-01

编号	SHG-Apache-01-01-01
名称	以特定用户运行服务
实施目的	以特定用户运行服务,不要使用系统管理员账号启动 APACHE
问题影响	越权使用造成非法攻击。
系统当前状态	**# ps -aux | grep httpd | grep -v grep** **# ls -al `which apachectl`** **# apachectl -V | grep SERVER_CONFIG** Solaris 用 ps -ef 代替 ps -aux 查看当前进程
实施步骤	一般情况下，Apache 是由 Root 来安装和运行的。如果 Apache Server 进程具有 Root 用户特权，那么它将给系统的安全构成很大的威胁，应确保 Apache Server 进程以最可能低的权限用户来运行。通过修改 httpd.conf 文件中的下列选项，以 Nobody 用户运行 Apache 达到相对安全的目的。 备份 httpd.conf 文件 修改： User nobody Group# -1 重启 APACHE **./apachectl restart**

回退方案	恢复 httpd.conf 文件，重启 APACHE
判断依据	判断是否漏洞。
实施风险	中
重要等级	★★★

1.1.2 SHG-Apache-01-01-02

编号	SHG-Apache-01-01-02
名称	ServerRoot 目录的权限
实施目的	非超级用户不能修改该目录中的内容
问题影响	非法修改
系统当前状态	# ls –al /usr/local/apache
实施步骤	为了确保所有的配置是适当的和安全的，需要严格控制 Apache 主目录的访问权限，使非超级用户不能修改该目录中的内容。Apache 的主目录对应于 Apache Server 配置文件 httpd.conf 的 Server Root 控制项中，应为： Server Root /usr/local/apache
回退方案	恢复目录权限
判断依据	尝试修改，看是否能修改。
实施风险	中
重要等级	★★
备注	

1.1.3 SHG-Apache-01-01-03

编号	SHG-Apache-01-01-03
名称	控制哪些主机能够访问服务器的一个区域
实施目的	防止恶意攻击
问题影响	非法访问
系统当前状态	
实施步骤	如果你只想让某个网段或者某个 IP 接入，你可以在 apache 配置文件中强制实行。 如：你想限制你的 intranet，只能被 176.16.网段接入： Order Deny,Allow Deny from all Allow from 176.16.0.0/16 Or by IP: Order Deny,Allow Deny from all Allow from 127.0.0.1 备注： 详细请参考： http://www.souzz.net/online/ApacheManual/mod/mod_access.html
回退方案	恢复原始状态。
判断依据	尝试非法访问。
实施风险	高
重要等级	★★
备注	

1.1.4 SHG-Apache-01-01-04

编号	SHG-Apache-01-01-04
名称	禁止访问外部文件
实施目的	禁止 Apache 访问 Web 目录之外的任何文件。的 IP 地址等内容。
问题影响	非法访问，恶意攻击。
系统当前状态	Cat httpd.conf
实施步骤	**1、参考配置操作** 编辑 httpd.conf 配置文件， <Directory /> Order Deny,Allow Deny from all </Directory> **2、补充操作说明** 设置可访问目录， <Directory /web> Order Allow,Deny Allow from all </Directory> 其中/web 为网站根目录。
回退方案	恢复原始状态。
判断依据	**1、判定条件** 无法访问 Web 目录之外的文件。 **2、检测操作** 访问服务器上不属于 Web 目录的一个文件，结果应无法显示。
实施风险	中
重要等级	★★★

备注	

1.1.5 SHG-Apache-01-01-05

编号	SHG-Apache-01-01-05
名称	目录列表访问限制
实施目的	禁止 Apache 列表显示文件。
问题影响	恶意攻击。
系统当前状态	查看 httpd.conf 文件，查看 Options FollowSymLinks 是否与原来相同。
实施步骤	**1、参考配置操作** (1) 编辑 httpd.conf 配置文件， <Directory "/web"> Options FollowSymLinks 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。 (2)设置 Apache 的默认页面，编辑%apache%\conf\httpd.conf 配置文件， <IfModule dir_module> DirectoryIndex index.html </IfModule> 其中 index.html 即为默认页面，可根据情况改为其它文件。 (3)重新启动 Apache 服务
回退方案	恢复原始状态。

判断依据	**1、判定条件** 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、检测操作** 直接访问 http://ip:8800/xxx（xxx 为某一目录）
实施风险	高
重要等级	★
备注	

2 日志配置

2.1.1 SHG-Apache-02-01-01

编号	SHG-Apache-02-01-01
名称	审核登陆
实施目的	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。
问题影响	非法访问，恶意攻击。
系统当前状态	查看 httpd.conf 文件中的 ErrorLog 、LogFormat（cat httpd.conf | grep ErrorLog） 查看 ErrorLog 指定的日志文件如 logs/error_log 中的内容是否完整(cat logs/error_log)
实施步骤	**1、参考配置操作** 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。
回退方案	恢复原始状态。
判断依据	查看 logs 目录中相关日志文件内容，记录完整。
实施风险	中
重要等级	★★
备注	

3 通信协议

3.1.1 SHG-Apache-03-01-01

编号	SHG-Apache-03-01-01
名称	更改默认端口
实施目的	更改 Apache 服务器默认端口，防止非法访问。
问题影响	恶意攻击。
系统当前状态	查看 httpd.conf 文件，查看端口是否与原来相同。

实施步骤	**1、参考配置操作** （1）修改 httpd.conf 配置文件，更改默认端口到 8080 Listen x.x.x.x:8080 （2）重启 Apache 服务
回退方案	恢复原始状态。
判断依据	**1、判定条件** 使用 8080 端口登陆页面成功 **2、检测操作** 登陆 http://ip:8080
实施风险	高
重要等级	★
备注	

4 设备其他安全要求

4.1.1 SHG-Apache-04-01-01

编号	SHG-Apache-04-01-01
名称	补丁修复
实施目的	升级 APACHE 修复漏洞
问题影响	容易引起恶意攻击。
系统当前状态	查看版本 Linux : apachectl -V

实施步骤	到 www.apache.org 下载新版本的 APACHE 公开的 apache 漏洞

2008-08-11	Apache Tomcat <= 6.0.18 UTF8 Directory Traversal Vulnerability
2008-07-18	Apache mod_jk 1.2.19 Remote Buffer Overflow Exploit (win32)
2008-07-17	Bea Weblogic Apache Connector Code Exec / Denial of Service Exploit
2008-04-06	Apache Tomcat Connector jk2-2.0.2 (mod_jk2) Remote Overflow Exploit
2008-03-31	mod_jk2 v2.0.2 for Apache 2.0 Remote Buffer Overflow Exploit (win32)
2007-10-21	Apache Tomcat (webdav) Remote File Disclosure Exploit (ssl support)
2007-10-14	Apache Tomcat (webdav) Remote File Disclosure Exploit
2007-07-08	Apache Tomcat Connector (mod_jk) Remote Exploit (exec-shield)
2007-06-22	Apache mod_jk 1.2.19/1.2.20 Remote Buffer Overflow Exploit
2007-05-26	Apache 2.0.58 mod_rewrite Remote Overflow Exploit (win2k3)
2007-04-07	Apache Mod_Rewrite Off-by-one Remote Overflow Exploit (win32)
2007-02-28	Ubuntu/Debian Apache 1.3.33/1.3.34 (CGI TTY) Local Root Exploit
2006-08-21	Apache < 1.3.37, 2.0.59, 2.2.3 (mod_rewrite) Remote Overflow PoC
2006-07-23	Apache Tomcat < 5.5.17 Remote Directory Listing Vulnerability
2005-06-20	Apache <= 2.0.49 Arbitrary Long HTTP Headers Denial of Service
2005-03-04	Apache <= 2.0.52 HTTP GET request Denial of Service Exploit
2005-01-16	Apache (mod_auth_radius) Remote Denial of Service Exploit
2004-11-18	Apache 2.0.52 Multiple Space Header Denial of Service Exploit (v2)
2004-11-02	Apache 2.0.52 Multiple Space Header DoS (c code)
2004-11-02	Apache 2.0.52 Multiple Space Header DoS (Perl code)
2004-10-21	Apache <= 1.3.31 mod_include Local Buffer Overflow Exploit
2004-09-16	htpasswd Apache 1.3.31 Local Exploit
2004-08-02	Apache HTTPd Arbitrary Long HTTP Headers DoS (c version)
2004-07-22	Apache HTTPd Arbitrary Long HTTP Headers DoS
2004-01-21	Apache OpenSSL ASN.1 parsing bugs <=0.9.6j BruteForce Exploit
2003-12-06	Apache 1.3.*-2.0.48 mod_userdir Remote Users Disclosure Exploit

	2003-11-20 Apache mod_gzip (with debug_mode) <= 1.2.26.1a Remote Exploit 2003-07-28 Apache 1.3.x mod_mylo Remote Code Execution Exploit 2003-06-08 Apache <= 2.0.45 APR Remote Exploit -Apache-Knacker.pl 2003-05-29 Webfroot Shoutbox < 2.32 (Apache) Remote Exploit 2003-04-11 Apache <= 2.0.44 Linux Remote Denial of Service Exploit 2003-04-09 Apache HTTP Server 2.x Memory Leak Exploit 2003-04-04 Apache OpenSSL Remote Exploit (Multiple Targets) (OpenFuckV2.c)
回退方案	升级补丁的风险极高，必须在万无一失的条件下升级，如当前版本没有漏洞不建议升级
判断依据	判断是否漏洞。
实施风险	高
重要等级	★★★
备注	

4.1.2 SHG-Apache-04-01-02

编号	SHG-Apache-04-01-02
名称	禁用 Apache Server 中的执行功能
实施目的	避免用户直接执行 Apache 服务器中的执行程序，而造成服务器系统的公开化。
问题影响	越权使用造成非法攻击。
系统当前状态	`# ls -al `which apachectl`` `# apachectl -V | grep SERVER_CONFIG`

实施步骤	在配置文件 access.conf 或 httpd.conf 中的 Options 指令处加入 Includes NO EXEC 选项，用以禁用 Apache Server 中的执行功能。避免用户直接执行 Apache 服务器中的执行程序，而造成服务器系统的公开化。 备份 access.conf 或 httpd.conf 文件 修改： Options Includes Noexec
回退方案	恢复 access.conf 和 httpd.conf 文件，重启 APACHE
判断依据	看是否禁用了 Apache Server
实施风险	中
重要等级	★

4.1.3 SHG-Apache-04-01-03

编号	SHG-Apache-04-01-03
名称	隐藏 Apache 的版本号及其它敏感信息
实施目的	隐藏 Apache 的版本号及其它敏感信息
问题影响	越权使用造成非法攻击。
系统当前状态	**# ls -al `which apachectl`** **# apachectl -V | grep SERVER_CONFIG**
实施步骤	默认情况下，很多 Apache 安装时会显示版本号及操作系统版本，甚至会显示服务器上安装的是什么样的 Apache 模块。这些信息可以为黑客所用，并且黑客还可以从中得知你所配置的服务器上的很多设置都是默认状态。 添加到你的 httpd.conf 文件中：

	ServerSignature Off ServerTokens Prod **补充说明：** ServerSignature 出现在 Apache 所产生的像 404 页面、目录列表等页面的底部。ServerTokens 目录被用来判断 Apache 会在 Server HTTP 响应包的头部填充什么信息。如果把 ServerTokens 设为 Prod，那么 HTTP 响应包头就会被设置成： Server：Apache 也可以通过源代码和安全模块进行修改
回退方案	将备份的 httpd.conf 文件恢复，重新启动 APACHE
判断依据	访问看是否给隐藏了。
实施风险	低
重要等级	★

4.1.4 SHG-Apache-04-01-04

编号	SHG-Apache-04-01-04
名称	Apache 413 错误页面跨站脚本漏洞修复
实施目的	修复 Apache HTTP Server 处理畸形用户请求时存在漏洞
问题影响	远程攻击者可能利用此漏洞获取脚本源
系统当前状态	Cat httpd.conf

实施步骤	Apache HTTP Server 处理畸形用户请求时存在漏洞，远程攻击者可能利用此漏洞获取脚本源码。 向 Apache 配置文件 httpd.conf 添加 ErrorDocument 413 语句禁用默认的 413 错误页面。
回退方案	恢复原始状态。
判断依据	警 告 以下程序(方法)可能带有攻击性，仅供安全研究与教学之用。使用者风险自负! 请求： GET / HTTP/1.1 Host: <BADCHARS> Connection: close Content-length: -1 [LF] [LF]
实施风险	中
重要等级	★★★
备注	

4.1.5 SHG-Apache-04-01-05

编号	SHG-Apache-04-01-05
名称	限制请求消息长度
实施目的	限制 http 请求的消息主体的大小。
问题影响	恶意攻击。
系统当前状态	Cat httpd.conf 文件，看是否与原来相同。

实施步骤	**1、参考配置操作** 编辑 httpd.conf 配置文件，修改为 102400Byte LimitRequestBody 102400
回退方案	恢复原始状态。
判断依据	**1、判定条件** 检查配置文件设置。 **2、检测操作** 上传文件超过 100K 将报错。
实施风险	中
重要等级	★
备注	

4.1.6 SHG-Apache-04-01-06

编号	SHG-Apache-04-01-06
名称	错误页面处理
实施目的	Apache 错误页面重定向。
问题影响	恶意攻击。
系统当前状态	查看 httpd.conf 文件，查看 ErrorDocument 文件是否与修改前相同。
实施步骤	**1、参考配置操作** (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 Customxxx.html 为要设置的错误页面。 (2)重新启动 Apache 服务
回退方案	恢复原始状态。
判断依据	**1、判定条件** 指向指定错误页面 **2、检测操作** URL 地址栏中输入 http://ip/xxxxxxx~~~（一个不存在的页面）
实施风险	高
重要等级	★
备注	

4.1.7 SHG-Apache-04-01-07

编号	SHG-Apache-04-01-07
名称	拒绝服务防范。
实施目的	防止恶意攻击
问题影响	恶意攻击。
系统当前状态	查看 httpd.conf 文件，查看 Timeout 等文件是否与原来相同。
实施步骤	**1、参考配置操作** (1) 编辑 httpd.conf 配置文件， Timeout 10 KeepAlive On KeepAliveTimeout 15 AcceptFilter http data AcceptFilter https data (2)重新启动 Apache 服务

回退方案	恢复原始状态。
判断依据	**1、判定条件** **2、检测操作** 检查配置文件是否设置。
实施风险	高
重要等级	★
备注	

4.1.8 SHG-Apache-04-01-08

编号	SHG-Apache-04-01-08
名称	删除缺省安装的无用文件。
实施目的	防止恶意攻击
问题影响	恶意攻击。
系统当前状态	查看缺省的的 HTML 文件是否与原来相同。
实施步骤	**1、参考配置操作** 删除缺省 HTML 文件： # rm -rf /usr/local/apache2/htdocs/* 删除缺省的 CGI 脚本： # rm –rf /usr/local/apache2/cgi-bin/* 删除 Apache 说明文件： # rm –rf /usr/local/apache2/manual 删除源代码文件： # rm -rf /path/to/httpd-2.2.4* 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。
回退方案	恢复原始状态。

判断依据	**1、判定条件** **2、检测操作** 检查对应目录。
实施风险	高
重要等级	★
备注	