【应用安全】浅谈 LINUX 系统 APACHE 安全配置

文/EmmaDai

0x00 Apache 应用介绍

Apache 是世界使用排名第一的 Web 服务器软件。它可以运行在几乎所有广泛使用的计算机平台上，由于其跨平台和安全性被广泛使用，是最流行的 Web 服务器端软件之一。它快速、可靠并且可通过简单的 API 扩充，将 Perl/Python 等解释器编译到服务器中。

0x01 为什么要做安全配置

Apache 的默认配置中存在一些安全问题，例如版本号信息泄露、未配置使用 SSL 协议等。因此安全配置 Apache 服务器能有效的减少安全威胁，下面将对 Apache 的安全配置进行讨论。

0x02 如何进行安全配置

1. Apache 用户账号 Shell 无效

apache 账号不能用作常规登录帐户，应该分配一个无效或 nologin shell 确保帐号不能用于登录。apache 账号 shell 应为：/sbin/nologin 或/dev/null。

加固方法：
修改 apache 账号使用 nologin shell 或例如 /dev/null 的无效 shell，

```
# chsh -s /sbin/nologin apache
```

2. 锁定 Apache 用户账号

Apache 运行的用户帐号不应该有有效的密码，应该被锁定。

加固方法：
使用 passwd 命令锁定 apache 账号

```
# passwd -l apache
```

3. 配置错误日志

LogLevel 指令用于设置错误日志的严重级别。ErrorLog 指令设置错误日志文件名称。日志级别值为 emerg，alert，crit，error，warn，notice，info 和 debug 的标准 syslog 级别。推荐级别为 notice，以便记录从 emerg 到 notice 级别的所有错误。core 模块建议设置为 info，以便任何"not found"请求包含在错误日志中。

加固方法：
a.在 Apache 配置中添加或修改 LogLevel 的值，core 模块设置为 info 或更低，所有其他模块设置为 notice 或更低。如果需要更详细的日志，并且存储和监视进程能够处理额外的负载，那么也可以设置为 info 或 debug。建议值是 notice core:info。

```
LogLevel notice core:info
```

b.如果尚未配置，则添加 ErrorLog 指令。 文件路径可能是相对的或绝对的，或者日志可能被配置为发送到系统日志服务器。

```
ErrorLog "logs/error_log"
```

c.如果虚拟主机有不同的人负责网站，为每个配置的虚拟主机添加一个类似 ErrorLog 的指令。每个负责的个人或组织都需要访问他们自己的网络日志，并需要技能/训练/工具来监控日志。

4. 禁用弱 SSL 协议

Apache SSLProtocol 指令指定允许的 SSL 和 TLS 协议。由于 SSLv2 和 SSLv3 协议已经过时并且易受信息泄露的攻击，所以都应该禁用。应只启用 TLS 协议。

加固方法：
在 Apache 配置文件中查找 SSLProtocol 指令；如果不存在，则添加该指令，或修改该值以匹配以下值之一。如果还可以禁用 TLSv1.0 协议，则首选设置"TLSv1.1 TLS1.2"。

```
SSLProtocol TLSv1.1 TLSv1.2
SSLProtocol TLSv1
```

5. 不安全的 SSL Renegotiation 应被限制

为了 Web 服务器与 OpenSSL 0.9.8m 或更高版本连接，在 Apache 2.2.15 中添加了 SSLInsecureRenegotiation 指令，允许不安全的重新协商为使用较早的未修补 SSL 实现客户端提供向后兼容性。在提供向后兼容性的同时，启用 SSLInsecureRenegotiation 指令会使服务器容易遭受中间人重新协商攻击（CVE-2009-3555）。因此，不应启用 SSLInsecureRenegotiation 指令。

加固方法：
在 Apache 配置文件中查找 SSLInsecureRenegotiation 指令。如果存在，将该值修改为 off。

```
SSLInsecureRenegotiation off
```

6. TimeOut 应设置为小于等于 10

TimeOut 指令控制 Apache HTTP 服务器等待输入/输出调用完成的最长时间（以秒为单位）。建议将 TimeOut 指令设置为 10 或更小。

加固方法：
修改 Apache 配置文件，将 TimeOut 设置为 10 秒或更小。

```
Timeout 10
```

7. KeepAlive 应设置为 On

KeepAlive 指令决定当处理完用户发起的 HTTP 请求后是否立即关闭 TCP 连接。

加固方法：
修改 Apache 配置文件，将 KeepAlive 设置为 On，以启用 KeepAlive 连接。

```
KeepAlive On
```

8. MaxKeepAliveRequests 应设置为大于等于 100

当 KeepAlive 启用时，MaxKeepAliveRequests 指令限制每个连接允许的请求数量。如果设置为 0，则允许无限制的请求。建议将 MaxKeepAliveRequests 设置为 100 或更大。

加固方法：
修改 Apache 配置文件，将 MaxKeepAliveRequests 设置为 100 或更大。

```
MaxKeepAliveRequests 100
```

9. KeepAliveTimeout 应设置为小于等于 15

KeepAliveTimeout 指令指定在关闭持久连接前等待下一个请求的秒数。

加固方法：
修改 Apache 配置文件，将 KeepAliveTimeout 设置为 15 或更小。

```
KeepAliveTimeout 15
```

10. 禁用 WebDAV 模块

Apache mod_dav 和 mod_dav_fs 模块支持 Apache 的 WebDAV（网络分布式创作与版本管理）功能。 WebDAV 是 HTTP 协议的扩展，允许客户端创建，移动和删除 Web 服务器上的文件和资源。

加固方法：
a.对于静态模块的源码版本，运行 Apache ./configure 脚本时在--enable-modules=configure 选项中不包括 mod_dav 和 mod_dav_fs。

```
$ cd $DOWNLOAD/httpd
$ ./configure
```

b.对于动态加载的模块，在 apache 配置文件中注释掉或删除 mod_dav 和 mod_dav_fs 模块的 LoadModule 指令。

```
# LoadModule dav_module modules/mod_dav.so
# LoadModule dav_fs_module modules/mod_dav_fs.so
```

11. 隐藏 Apache 版本号及其他敏感信息

配置 Apache ServerTokens 指令提供最少的信息。通过将该值设置为 Prod 或 ProductOnly，服务器 HTTP 响应头中给出的唯一版本信息将是"Apache"，而不是提供已安装的模块和版本的详细信息。禁用在服务器生成文档（如错误页面）底部生成签名行作为页脚的服务器签名。

加固方法：
Apache 配置文件中 ServerToken 应设置为：Prod，ServerSignature 应设置为：Off

12. 防止默认 Apache 内容的泄漏信息

在之前的建议中，删除了默认内容，如 Apache 手册和默认 CGI 程序。但是，如果要进一步限制有关 Web 服务器的信息泄露，例如图标等默认内容不留在 Web 服务器上也很重要。

加固方法：
a.默认的源码版本将自动索引和图标配置放在 extra/httpd-autoindex.conf 文件中，因此可以通过在主 httpd.conf 文件中将 include 行注释掉来禁用：

```
# Fancy directory listings
# Include xxx/httpd-autoindex.conf
```

b.或者，可以将图标 alias 指令和目录访问控制注释掉，如下：

```
# We include the /icons/ alias for FancyIndexed directory listings. If
# you do not use FancyIndexing, you may comment this out.
#
#Alias /icons/ "/var/www/icons/"
#<Directory "/var/www/icons">
# Options Indexes MultiViews FollowSymLinks
# AllowOverride None
# Order allow,deny
# Allow from all
#</Directory>
```

13. 13.禁用 HTTP TRACE 方法

使用 Apache TraceEnable 禁用 HTTP TRACE 请求方法。因 HTTP TRACE 存在跨站攻击漏洞。

加固方法：
找到例如 httpd.conf 的主要 Apache 配置文件。在 server 级配置中将 TraceEnable 设置为 off。server 级配置是顶级配置，不嵌套在任何其他如<Directory>或<Location>的指令中。

14. 14.限制所有目录覆盖

Apache AllowOverride 允许使用.htaccess 文件来覆盖大部分配置，包括身份验证，文档类型处理，自动生成的索引，访问控制和选项。当服务器找到一个.htaccess 文件（由 AccessFileName 指定）时，它需要知道该文件中声明的哪个指令可以覆盖较早的访问信息。当这个指令设置为 None 时，那么.htaccess 文件将被完全忽略。在这种情况下，服务器甚至不会尝试读取文件系统中的.htaccess 文件。当这个指令设置为 All 时，在 .htaccess 文件中允许任何具有.htaccess 上下文的指令。

加固方法：
Apache 配置文件中的<Directory>中应设置：AllowOverride None

15. 15.删除默认 CGI 内容 test-cgi

大多数 Web 服务器（包括 Apache 安装）都带有不需要或不适合生产使用的默认 CGI 内容。这些示例程序的主要作用是展示 Web 服务器的功能。apache 安装的一个常见的默认 CGI 内容是脚本 test-cgi。这个脚本将打印回请求者的 CGI 环境变量，其中包括许多服务器配置细节。

加固方法：

a.通过 Script，ScriptAlias，ScriptAliasMatch 或 ScriptInterpreterSource 指令找到在 Apache 配置中启用的 cgi-bin 文件和目录。
b.删除 cgi-bin 目录中的 printenv 默认 CGI（如果已安装）。

0x03 总结

对 Apache 进行安全配置可以有效的防范一些常见安全问题，按照基线标准做好安全配置能够减少安全事件的发生。国内常见的基线标准有中国信息安全等级保护、电信网和互联网安全防护基线配置要求及检测要求，美国 CIS 基线也有详细的 Apache 基线标准，不同的企业也可以根据自身企业业务制定符合自己企业的安全基线标准。

0x04 参考链接

- 国家信息安全等级保护制度要求
- 电信网和互联网安全防护基线配置要求及检测要求
- CIS_Apache_HTTP_Server_2.4_Benchmark_v1.3.0
- CIS_Apache_HTTP_Server_2.2_Benchmark_v3.4.0