【应用安全】浅谈 LINUX 系统 NGINX 安全配置

文/EmmaDai

0x00 Nginx 应用介绍

Nginx 是一个高性能的 HTTP 和反向代理服务器，也是一个 IMAP/POP3/SMTP 服务器。Nginx 作为负载均衡服务器：Nginx 既可以在内部直接支持 Rails 和 PHP 程序对外进行服务，也可以支持作为 HTTP 代理服务器对外进行服务。

0x01 为什么要做安全配置

Nginx 存在因为安全配置不合适导致的安全问题。Nginx 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 Nginx 服务器能有效的减少安全威胁，下面将对 Nginx 的安全配置进行讨论。

0x02 如何进行安全配置

1. 配置 SSL 协议

Nginx web 服务器的应配置使用 Secure Sockets Layer Protocol (SSL 协议)。为了数据传输的安全，SSL 依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

加固方法：
编辑 nginx.conf 文件和可用站点默认文件包含 ssl on

2. 限制 SSL 协议和密码

SSLv2 协议不安全，不应使用。较新的 TLS 协议也应该优于旧的。并使用安全的加密密钥。

加固方法：
nginx.conf 文件中的 ssl_ciphers 字段应包含 ALL:!EXP:!NULL:!ADH:!LOW:!SSLv2:!MD5:!RC4

3. 拦截垃圾信息

HTTP Referrer Spam 是垃圾信息发送者用来提高他们正在尝试推广的网站的互联网搜索引擎排名一种技术，如果他们的垃圾信息链接显示在访问日志中，并且这些日志被搜索引擎扫描，则会对网站排名产生不利影响。

加固方法：
在 nginx.conf 文件中添加：

```
if ( $http_referer ~*
(babes|forsale|girl|jewelry|love|nudit|organic|poker|porn|sex|teen) )
{
# return 404;
return 403;
}
```

4. 禁用 WebDAV

Nginx 支持 webdav，虽然默认情况下不会编译。如果使用 webdav，则应该在 Nginx 策略中禁用此规则。

加固方法：
nginx.conf 文件中 dav_methods 应设置为：off

5. 禁用 Nginx 状态模块

当访问一个特制的 URL 时，如"../nginx.status"，stub_status 模块提供一个简短的 Nginx 服务器状态摘要。大多数情况下不应启用此模块。

加固方法：
nginx.conf 文件中 stub_status 不应设置为：on

6. 关闭默认错误页上的 Nginx 版本号

如果在浏览器中出现 Nginx 自动生成的错误消息，默认情况下会包含 Nginx 的版本号。 这些信息可以被攻击者用来帮助他们发现服务器的潜在漏洞。

加固方法：
nginx.conf 文件中 server_tokens 应设置为：off

7. 设置 client_body_timeout 超时

client_body_timeout 设置请求体（request body）的读超时时间。仅当在一次 readstep 中，没有得到请求体，就会设为超时。超时后，Nginx 返回 HTTP 状态码 408(Request timed out)。

加固方法：
nginx.conf 文件中 client_body_timeout 应设置为：10

8. 设置 client_header_timeout

client_header_timeout 设置等待 client 发送一个请求头的超时时间（例如：GET / HTTP/1.1）。仅当在一次 read 中，没有收到请求头，才会设为超时。超时后，Nginx 返回 HTTP 状态码 408(Request timed out)。

加固方法：
nginx.conf 文件中 client_header_timeout 应设置为：10

9. 设置 keepalive_timeout 超时

keepalive_timeout 设置与 client 的 keep-alive 连接超时时间。服务器将会在这个时间后关闭连接。

加固方法：
nginx.conf 文件中 keepalive_timeout 应设置为：55

10. 设置 send_timeout 超时

send_timeout 设置客户端的响应超时时间。这个设置不会用于整个转发器，而是在两次客户端读取操作之间。如果在这段时间内，客户端没有读取任何数据，Nginx 就会关闭连接。

加固方法：
nginx.conf 文件中 send_timeout 应设置为：10

11. Nginx 可用的方法应限制为 GET, HEAD, POST

GET 和 POST 是 Internet 上最常用的方法。Web 服务器方法在 RFC 2616 中定义。Web 服务器应禁用不需要实现的可用方法。

加固方法：
nginx.conf 文件中应存在：

```
if ($request_method !~ ^(GET|HEAD|POST)$ )
```

12. 控制并发连接 limit_zone slimits

limit_zone 配置项限制来自客户端的同时连接数。通过此模块，可以从一个地址限制分配会话的同时连接数量或特殊情况。

加固方法：
nginx.conf 文件中 limit_zone 应设置为：slimits $binary_remote_addr 5m

13. 控制并发连接 limit_conn slimits

limit_conn 配置项控制一个会话同时连接的最大数量，即限制来自单个 IP 地址的连接数量。

加固方法：
nginx.conf 文件中 limit_conn 应设置为：slimits 5

0x03 总结

对 Nginx 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，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