Nginx基线检查

一、server_tokens基线

server_tokens指令负责在错误页面和ServerHTTP响应头字段中显示NGINX版本号和操作系统版本。不应显示此信息。

操作方法

在 nginx 配置文件中的 http 块配置 server_tokens off;

二、 Nginx是否禁止隐藏文件的访问

禁用隐藏文件是一种深度防御机制，有助于防止意外泄露敏感信息。

操作方法

编辑nginx配置文件，添加以下配置：

```
location ~ /\. {
deny all;
}
```

三、Nginx是否禁用autoindex功能

Nginx autoindex 指令用于配置 Nginx 的目录浏览功能，开启目录浏览可能会导致信息泄露。

操作方法

编辑 Nginx 配置文件，将配置文件中的 autoindex 设置为 off

四、是否隐藏Nginx后端服务X-Powered-By头

x-powered-By 表示网站是用什么技术开发的，它会泄漏开发语言、版本号和框架等信息,有安全隐患，需要隐藏掉。

操作方法

在配置文件的 http 块下配置如下内容

```
proxy_hide_header X-Powered-By;
proxy_hide_header Server;
```

五、是否限制Nginx账户登录系统

Nginx帐户不应该具有登录的能力，防止Nginx账户被恶意利用。

操作方法

修改 /etc/passwd 配置文件中 nginx 用户的登录 Shell 字段，设置为：/usr/sbin/nologin（debian，ubuntu）或 /sbin/nologin（centos），可以使用下列命令修改。

```
chsh -s /sbin/nologin nginx
```

六、 Nginx配置文件权限配置是否合适

nginx 配置文件的所有者和所属组应为 root，且权限不宜过高

操作方法

设置 nginx 配置文件的用户和用户组为 root，权限为 644

```
chown root:root /etc/nginx/nginx.conf /etc/nginx/conf.d/*.conf
/etc/nginx/default.d/*.conf

chmod 644 /etc/nginx/nginx.conf /etc/nginx/conf.d/*.conf
/etc/nginx/default.d/*.conf
```

七、Nginx的WEB访问日志是否记录

应为每个站点启用 access_log 。

操作方法

编辑 Nginx 配置文件，在http下参考如下格式配置 access_log

```
access_log logs/access.log main;
```