# 三、ReWrite语法

last – 基本上都用这个Flag。

break – 中止Rewirte，不在继续匹配

redirect – 返回临时重定向的HTTP状态302

permanent – 返回永久重定向的HTTP状态301

1、下面是可以用来判断的表达式：

-f和!-f用来判断是否存在文件

-d和!-d用来判断是否存在目录

-e和!-e用来判断是否存在文件或目录

-x和!-x用来判断文件是否可执行

2、下面是可以用作判断的全局变量

例：http://localhost:88/test1/test2/test.php

$host：localhost

$server\_port：88

$request\_uri：http://localhost:88/test1/test2/test.php

$document\_uri：/test1/test2/test.php

$document\_root：D:\nginx/html

$request\_filename：D:\nginx/html/test1/test2/test.php

# 一些常用的配置

## 1、普通的（静态的）http服务器

这样如果访问http://localhost 就会默认访问到/home/wwwroot目录下面的index.html，如果一个网站只是静态页面的话，那么就可以通过这种方式来实现部署。

server {

    listen       80;

    server\_name  localhost;

    client\_max\_body\_size 1024M;

    location / {

           root   /home/wwwroot; //思路：通过/将所有的请求，转发给root处理

           index  index.html;

       }

}

## 2、反向代理

localhost的时候，就相当于访问localhost:8080了

server {

    listen       80;

    server\_name  localhost;

    client\_max\_body\_size 1024M;

    location / {

        proxy\_pass http://localhost:8080;

        proxy\_set\_header Host $host:$server\_port;    //思路：通过/，将所有的请求，转发给第3方处理

    }

}

既然服务器可以直接HTTP访问，为什么要在中间加上一个反向代理，不是多此一举吗？反向代理有什么作用？

负载均衡、虚拟主机等，都基于反向代理实现，当然反向代理的功能也不仅仅是这些

## 3、Redirect（重定向）语法

server {

    listen 80;

    server\_name start.igrow.cn;

    index index.html index.php;

    root html;

    if ($http\_host !~ "^star\.igrow\.cn$" {

        rewrite ^(.\*) http://star.igrow.cn$1 redirect;

    }

}

## 4、防盗链



location ~\* \.(gif|jpg|png|bmp)$ {

    valid\_referers none blocked \*.ttlsa.com server\_names ~\.google\. ~\.baidu\.;

    if ($invalid\_referer) {

        return 403;

        #rewrite ^/ http://www.ttlsa.com/403.jpg;

    }

}

## 5、根据文件类型设置过期时间

location ~\* \.(js|css|jpg|jpeg|gif|png|swf)$ {

    if (-f $request\_filename) {     //只能是文件，因为这用-f判断了

        expires 1h;

        break;

    }

}

## 6、设置图片缓存（过期）时间







## 7、禁止访问某个目录

location ~\* \.(txt|doc)${

root /data/www/wwwroot/linuxtone/test;  #所有用户都禁止访问这个目录

deny all;

}

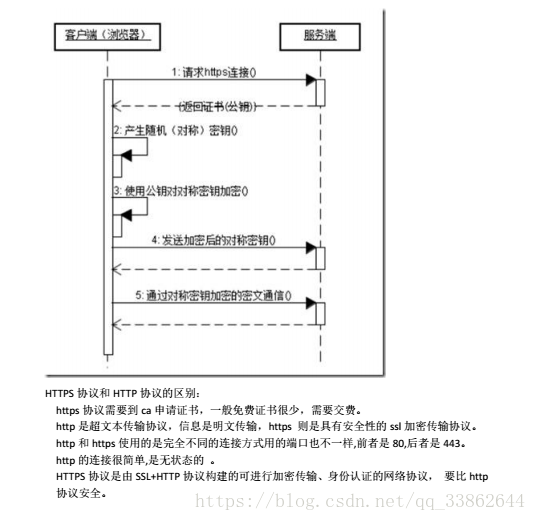
## 8、隐藏版本号的作用

通过你所用的版本，找其漏洞，进行攻击你

在http中添加该配置：server\_tokens off;



## 9、配置https (如当前文件夹下的 https-443.conf)



1、去阿里云/腾讯云申请免费的

2、下载证书

3、证书放到/usr/local/nginx目录下（就是和conf同级，nginx.conf默认的配置文件的上一级）

4、在vhost目录下加入配置文件

server {

 listen 443;

 server\_name lampol.edu0532.cn; #改域名

 ssl on;

 root /home/www/xcxtp5/public; #改项目路径

 ssl\_certificate ../certbo/1523694051089.pem;    #改证书路径

 ssl\_certificate\_key ../certbo/1523694051089.key; #改私钥路径

 ssl\_session\_timeout 5m;

 ssl\_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4;

 ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

 ssl\_prefer\_server\_ciphers on;

        location / {

            index  index.html index.htm index.php;

            autoindex  on;

            # 伪静态配置

            if (!-e $request\_filename) {

                rewrite  ^(.\*)$  /index.php?s=$1  last;

                break;

            }

        }

        location ~ \.php$ {

            fastcgi\_pass   127.0.0.1:9000;

            fastcgi\_index  index.php;

            include        fastcgi.conf;

        }

}

## 10、动静分离

思路：动、静态的文件，请求时匹配不同的目录

当访问gif,jpeg时 直接访问e:wwwroot;,正则自行配置

server {

  listen       80;

  server\_name  localhost;

  location / {

      root   e:wwwroot;

      index  index.html;

  }

  # 所有静态请求都由nginx处理，存放目录为html

  location ~ .(gif|jpg|jpeg|png|bmp|swf|css|js)$ {

      root    e:wwwroot;

  }

  # 所有动态请求都转发给tomcat处理

  location ~ .(jsp|do)$ {

      proxy\_pass  http://test;

  }

  error\_page   500 502 503 504  /50x.html;

  location = /50x.html {

      root   e:wwwroot;

  }

}