服务器设置禁止直接访问目录或文件，可以避免服务器文件直接暴露，导致平台信息泄露。以下是Nginx、Apache、IIS的配置方法：

Nginx

1. 修改 Nginx 的配置文件，linux可通过命令：`find / -name nginx.conf` 来查找配置文件路径。

2. 在 http 块下添加以下配置代码：

```
location /Logs/ {

return 403;

}
```

如宝塔：

3. 保存并关闭文件。

4. 使用命令nginx -s reload 重载Nginx配置，使配置生效。

Apache

1. 修改Apache 的配置文件， httpd.conf

2. 加入以下配置代码

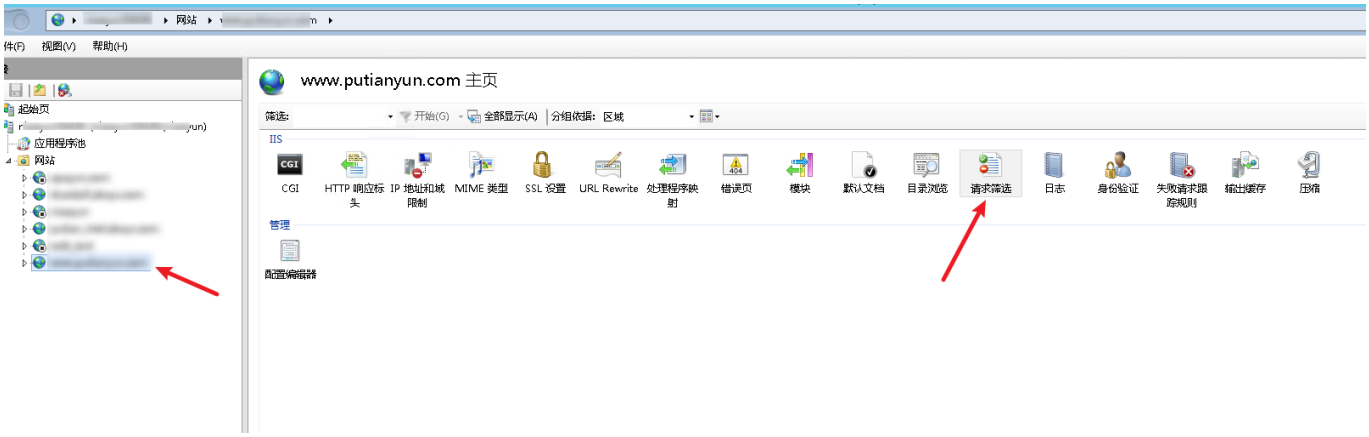
```
<Location /Logs/>
    Order allow,deny
    Deny from all
</Location>
```

3. 保存并关闭文件。

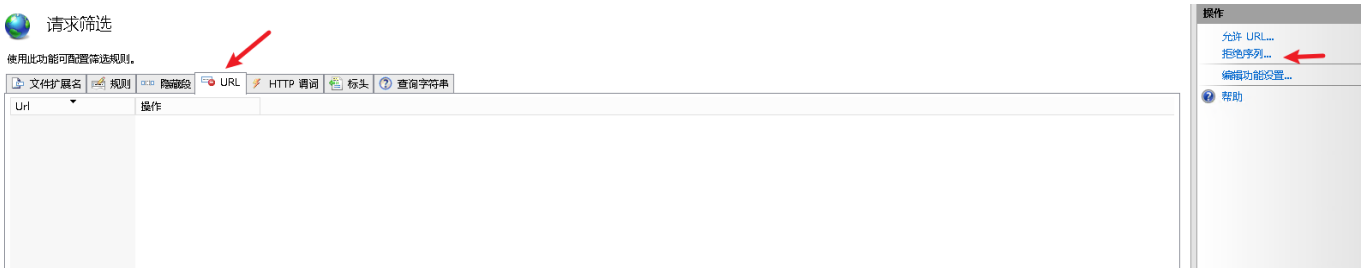
4. 重启httpd服务。

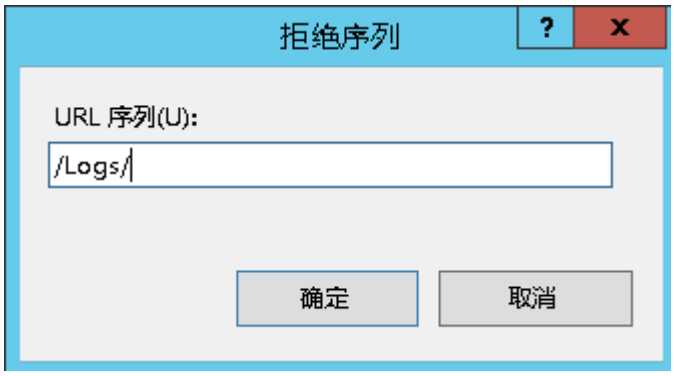
IIS

1. 打开IIS管理器，添加请求筛选设置



2.URL模块添加【拒绝序列】





- 重启IIS