**1. APACHE配置X-FRAME-OPTIONS**

在站点配置文件httpd.conf中添加如下配置，限制只有站点内的页面才可以嵌入iframe。

**Header always append X-Frame-Options SAMEORIGIN**

配置之后重启apache使其生效。该配置方式对IBM HTTP Server同样适用。

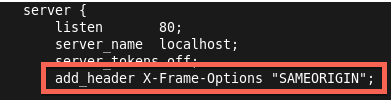
如果同一apache服务器上有多个站点，只想针对一个站点进行配置，可以修改.htaccess文件，添加如下内容：

**Header append X-FRAME-OPTIONS "SAMEORIGIN"**

**2. NGINX 配置X-FRAME-OPTIONS**

到 nginx/conf文件夹下，修改nginx.conf ，添加如下内容：

**add\_header X-Frame-Options "SAMEORIGIN";**



重启Nginx服务。

**3. IIS配置X-FRAME-OPTIONS**

在web站点的web.config中配置：

**<system.webServer>**

**...**

**<httpProtocol>**

**<customHeaders>**

**<add name="X-Frame-Options" value="SAMEORIGIN" />**

**</customHeaders>**

**</httpProtocol>**

**...**

**</system.webServer>**

**4. TOMCAT配置X-FRAME-OPTIONS**

将[ClickjackFilter.jar](http://localhost:8081/issues_lib/ClickjackFilter.jar)添加到lib目录下。

然后，打开webapps\ROOT\WEB-INF\web.xml添加以下过滤器：

**<filter>**

**<filter-name>ClickjackFilterDeny</filter-name>**

**<filter-class>org.owasp.filters.ClickjackFilter</filter-class>**

**<init-param>**

**<param-name>mode</param-name>**

**<param-value>DENY</param-value>**

**</init-param>**

**</filter>**

**<filter-mapping>**

**<filter-name>ClickjackFilterDeny</filter-name>**

**<url-pattern>/\*</url-pattern>**

**</filter-mapping>**