

java代码审计 深度解析

第一课 点击劫持

ALLOW-FROM URI

页面自能被指定的Uri嵌入到iframe或frame中。

1.3.2 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"

1.3.3 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";

```
server {  
    listen      80;  
    server_name localhost;  
    server_tokens off;  
    add_header X-Frame-Options "SAMEORIGIN";  
}
```

重启Nginx服务。

1.3.4 IIS配置X-FRAME-OPTIONS

在web站点的web.config中配置：





谢谢观赏