此页面由社区从英文翻译而来。了解更多并加入 MDN Web Docs 社区。

X-Frame-Options

`X-Frame-Options` HTTP 响应头是用来给浏览器指示允许一个页面可否在 `<frame>`、`<iframe>`、`<embed>` 或者 `<object>` 中展现的标记。站点可以通过确保网站没有被嵌入到别人的站点里面，从而避免点击劫持攻击。

仅当访问文档的用户使用支持 `X-Frame-Options` 的浏览器时，此附加的安全性才会被提供。

> **备注：** `Content-Security-Policy` HTTP 响应头有一个 `frame-ancestors` 指令，支持这一指令的浏览器已经废弃 了 `X-Frame-Options` 响应头。

首部类型	响应首部
禁止修改的消息首部	否

语法

`X-Frame-Options` 有两个可能的值：

```
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
```

指南

如果设置为 `DENY`，不光在别人的网站 frame 嵌入时会无法加载，在同域名页面中同样会无法加载。另一方面，如果设置为 `SAMEORIGIN`，那么页面就可以在同域名页面的 frame 中嵌套。

`DENY`

表示该页面不允许在 frame 中展示，即便是在相同域名的页面中嵌套也不允许。

`SAMEORIGIN`

表示该页面可以在相同域名页面的 frame 中展示。规范让浏览器厂商决定此选项是否应用于顶层、父级或整个链，有人认为该选项不是很有用，除非所有的祖先页面都属于同一来源（origin）（见 bug 725490 ）。参见浏览器兼容性以获取详细的兼容性信息。

`ALLOW-FROM uri`

这是一个被弃用的指令，不再适用于现代浏览器，请不要使用它。在支持旧版浏览器时，页面可以在指定来源的 frame 中展示。请注意，在旧版 Firefox 上，它会遇到与 `SAMEORIGIN` 相同的问题——它不会检查 frame 所有的祖先页面来确定他们是否是同一来源。`Content-Security-Policy` HTTP 首部有一个 `frame-ancestors` 指令，你可以使用这一指令来代替。

示例

> **备注：** 使用 `<meta>` 标签来设置 `X-Frame-Options` 是无效的！例如 `<meta http-equiv="X-Frame-Options" content="deny">` 没有任何效果。不要这样用！只有当像下面示例那样设置 HTTP 头 `X-Frame-Options` 才会生效。

配置 Apache

配置 Apache 在所有页面上发送 `X-Frame-Options` 响应头，需要把下面这行添加到 'site' 的配置中：

```
Header always set X-Frame-Options "SAMEORIGIN"
```

要将 Apache 的配置 `X-Frame-Options` 设置成 `DENY` ，按如下配置去设置你的站点：

```
Header set X-Frame-Options "DENY"
```

配置 Nginx

配置 Nginx 发送 `X-Frame-Options` 响应头，把下面这行添加到 'http', 'server' 或者 'location' 的配置中：

```
add_header X-Frame-Options SAMEORIGIN always;
```

配置 IIS

配置 IIS 发送 `X-Frame-Options` 响应头，添加下面的配置到 `Web.config` 文件中：

```
<system.webServer>
  ...

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

  ...
</system.webServer>
```

参见 Microsoft 关于使用 IIS Manager 来修改这一配置的支持文章 用户界面。

配置 HAProxy

配置 HAProxy 发送 `X-Frame-Options` 响应头，添加这些到你的前端、监听（listen），或者后端的配置里面：

```
rspadd X-Frame-Options:\ SAMEORIGIN
```

或者，在较新的版本中：

```
http-response set-header X-Frame-Options SAMEORIGIN
```

配置 Express

要配置 Express 以发送 `X-Frame-Options` 响应头，你可以使用借助了 frameguard 的 helmet 来设置首部。在你的服务器配置里面添加：

```
const helmet = require('helmet');
const app = express();
app.use(helmet.frameguard({ action: 'SAMEORIGIN' }));
```

或者，你也可以直接用 frameguard：

```
const frameguard = require('frameguard')
app.use(frameguard({ action: 'SAMEORIGIN' }))
```

规范

Specification

HTTP Header Field X-Frame-Options

section-2

浏览器兼容性

Report problems with this compatibility data on GitHub

	Chrome	Edge	Firefox	Internet Explorer	Opera	Safari	WebView Android	Chrome Android	Firefox for Android
`X-Frame-Options`	Chrome 4	Edge 12	Firefox 4	Internet Explorer 8	Opera 10.5	Safari 4	WebView Android Yes	Chrome Android Yes	Firefox for Android Y
ALLOW-FROM	Chrome No	Edge 12–79	Firefox 18–70	Internet Explorer 8	Opera No	Safari No	WebView Android No	Chrome Android No	Firefox for Android
SAMEORIGIN	Chrome Yes	Edge 12	Firefox Yes	Internet Explorer 8	Opera Yes	Safari Yes	WebView Android Yes	Chrome Android Yes	Firefox for Android Ye

Full support No support Compatibility unknown See implementation notes.

参见

- `Content-Security-Policy` 的 `frame-ancestors` 指令
- HTTP Header Field X-Frame-Options - RFC 7034
- ClickJacking Defenses - IEBlog
- Combating ClickJacking with X-Frame-Options - IEInternals

Last modified: 2022年4月26日, by MDN contributors