57. CSP（内容安全策略）介绍：如何防止注入类攻击

1. 核心概念 (Core Concept)

CSP（Content Security Policy）是一种安全特性，它允许网站管理员通过 HTTP 头或 meta 元素定义一系列受信任的内容源，从而限制浏览器可以加载的脚本、样式、图片等资源的来源，有效缓解跨站脚本（XSS）等注入类攻击。

2. 为什么需要它？ (The "Why")

- **防止 XSS 攻击：** 限制可执行脚本的来源，阻止攻击者注入恶意脚本并执行。
- **限制其他攻击：** 除了脚本，还可以限制样式表、字体、图片、媒体文件等的加载源，进一步增强安全性，例如防止攻击者加载恶意 CSS 进行钓鱼。
- **提升安全性感知：** 通过明确定义允许的资源来源，网站管理员对页面加载的内容有更强的控制力。

3. API 与用法 (API & Usage)

CSP 主要通过 HTTP 响应头 `Content-Security-Policy` 或 `Content-Security-Policy-Report-Only`，或者 `<meta>` 标签来配置。

常用指令 (Directives):

- `default-src <source>`: 为所有未显式指定源的指令设置默认源。
- `script-src <source>`: 限制 JavaScript 的来源。
- `style-src <source>`: 限制样式表的来源。
- `img-src <source>`: 限制图片的来源。
- `connect-src <source>`: 限制通过 XMLHttpRequest, WebSocket 等连接的来源。
- `font-src <source>`: 限制字体的来源。
- `object-src <source>`: 限制 `<object>`, `<embed>`, `<applet>` 标签的来源。
- `media-src <source>`: 限制 `<audio>`, `<video>` 标签的来源。
- `frame-src <source>`: 限制 `<frame>`, `<iframe>`, `<frameset>` 标签的来源。
- `child-src <source>`: 限制 worker 或 frame 的来源（逐渐取代 frame-src 和 worker-src）。
- `manifest-src <source>`: 限制 Web 应用 manifest 文件的来源。
- `report-uri <uri>/report-to <endpoint>`: 浏览器违反 CSP 时向指定 URI/端点发送违规报告。
- `upgrade-insecure-requests`: 指示用户代理将 HTTP 请求重写为 HTTPS。
- `block-all-mixed-content`: 阻止在 HTTPS 页面中加载任何通过 HTTP 加载的资源。

信源值 (Source Value):

- `'none'`：禁止从任何源加载。
- `'self'`：只允许从当前域加载（协议、域名、端口必须完全一致）。
- `<scheme>://<host>:<port>`：允许从指定的协议、主机和端口加载。
- `*.example.com`：允许从 example.com 的所有子域加载。
- `example.com:*`：允许从 example.com 的任何端口加载。
- `'unsafe-inline'`：允许使用内联脚本和样式（**强烈不推荐，降低 CSP 防御 XSS 能力**）。
- `'unsafe-eval'`：允许使用 `eval()` 等方法（**强烈不推荐，降低 CSP 防御 XSS 能力**）。
- `'nonce-<base64-value>'`：只允许加载带有匹配 nonce 值的脚本或样式标签。

  ```
  <script nonce="random123">...</script>
  ```

- `'<hash-algorithm>-<base64-value>'`：只允许加载与指定哈希匹配的内联脚本或样式块。

  ```
  <script>alert('Hello!');</script>
  ```

  哈希值（例如 SHA256）可以通过工具计算。

代码示例 (HTTP Header):

```
Content-Security-Policy: default-src 'self'; script-src 'self'
https://cdnjs.cloudflare.com; style-src 'self' 'unsafe-inline'; img-src *;
report-uri /csp-reporting
```

说明：
这个策略允许：

- 所有资源默认只允许从当前域加载 (`default-src 'self'`)。
- JavaScript 可以从当前域或 Cloudflare CDN 加载 (`script-src 'self' https://cdnjs.cloudflare.com`)。
- 样式可以从当前域加载，并允许使用内联样式（`'unsafe-inline