SWRhapsody

CSP

于8月 3, 2019由**SWRhapsody**发布

Introduction

Content Security Policy (CSP)，中文内容安全策略，这是一个由 W3C 制定的一个标准，主要是用来防御 XSS。不过 CSP 作为一种安全策略并不能拦截所有的攻击，同时配置不当反而更危险。

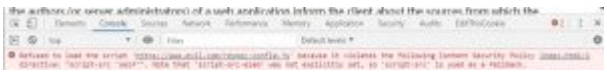
Code

CSP 工作原理

在浏览器发起请求后服务器返回带 `Content-Security-Policy` Header 的 Response，并在个这个请求头中设置安全策略

```
Content-Security-Policy: default-src 'self'https://apis.google.com; img-src *; media-src media1.com media2.com; script-src userscripts.example.com
```

这个HTTP Header 允许创建信任的内容的来源白名单，并指示浏览器仅执行或渲染来自这些来源的资源，比如说在这个例子中，浏览器只会渲染来自当前地址和 `apis.google.com` 的 Javascript，但是接受任何地址的图片。这样就算页面中有请求获取来自 `evil.com` 的脚本的代码也不会加载恶意代码。



关于 `Content-Security-Policy` 具体的各个指令可以看 [6]。CSP 在默认情况下阻止内联代码和 `eval()` 函数，如果需要需配置 `script-src 'unsafe-inline';style-src 'unsafe-inline'` 。

CSP 还具备报告的功能，通过配置可以向服务器返回某种通知以便在第一时间发现和制止允许恶意注入的错误

```
1 <span class="typ">Content</span><span class="pun">-</span><span class="typ">Security</span><spa
2 </span>
```

SWRhapsody

```
  </span><span class="str">"csp-report"</span><span class="pun">:</span><span class="pln"> </sp
    </span><span class="str">"document-uri"</span><span class="pun">:</span><span class="pln">
    </span><span class="str">"referrer"</span><span class="pun">:</span><span class="pln"> </sp
    </span><span class="str">"blocked-uri"</span><span class="pun">:</span><span class="pln"> <
    </span><span class="str">"violated-directive"</span><span class="pun">:</span><span class="
    </span><span class="str">"original-policy"</span><span class="pun">:</span><span class="pln
  </span><span class="pun">}</span><span class="pln">
</span><span class="pun">}</span>
```

不过根据 OWASP 的看法，CSP 不因该成为网站对抗 XSS 的第一道防线，它主要是用来缓减攻击，而不是输入过滤以及其他防御的替代品 [4]，google还有篇文章 [4] 说他们调查了很多网站结果发现这些网站不正确的配置使得CSP 很容易被绕过。

Reference

[1] https://en.wikipedia.org/wiki/Content_Security_Policy

[2] https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

[3] https://static.googleusercontent.com/media/research.google.com/zh-CN//pubs/archive/45542.pdf

[4] https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

[5] https://developers.google.com/web/fundamentals/security/csp/

[6] https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

分类: ARTICLE COLLECTION

SWRhapsody

电子邮件 *

网站

在想些什么?

发表评论

近期文章

携程Apollo YAML 反序列化

CVE-2020-5410

CodeQL部分源码简读

服务器与网关的不一致

CodeQL 部分使用记录

近期评论

文章归档

2020年8月

分类目录

SWRhapsody

Uncategorized

相关文章

ARTICLE COLLECTION

各种文章收集

DDOS CC攻击原理及防范方法: https://www.cnblo 阅读更多…

ARTICLE COLLECTION

XSS

Introduction 想写个对于各种漏洞的总结，这个是第一篇 XS 阅读更多…