REX AWS Lambda@Edge & HTTP Security Headers

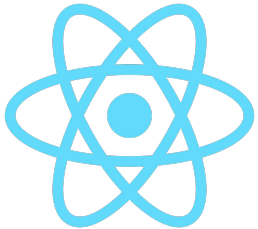
OWASP Paris — 23 Juin 2020

Antoine TANZILLI — OCTO

Archi AWS SPA React

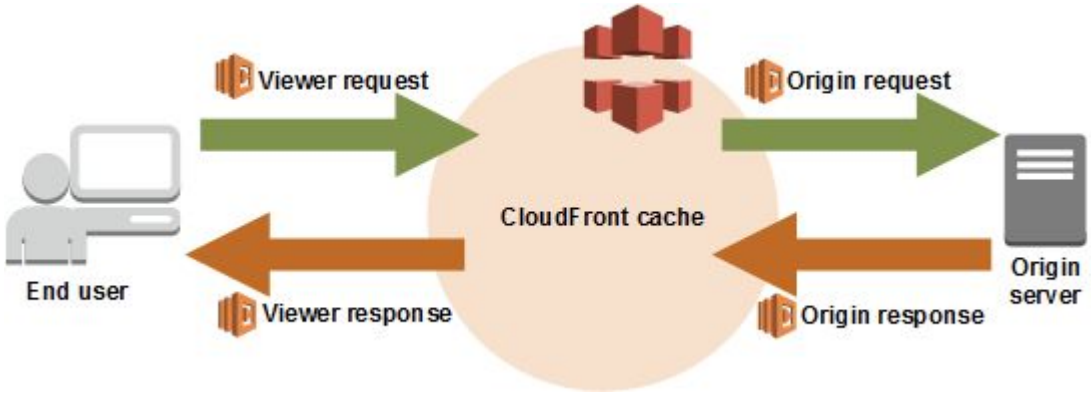
CDN (Cloudfront)

Storage (S3)



SPA React

Lambda@Edge

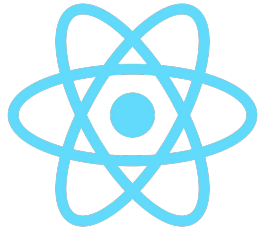


Archi AWS SPA React avec Lambda@Edge

CDN (Cloudfront)

Lambda@Edge

Storage (S3)



SPA React

Exemple Lambda@Edge

```
"use strict";

const contentSecurityPolicies = [
  "form-action 'self' https://secure.ogone.com https://ogone.test.v-psp.com",
  "frame-ancestors https://auth.example.com https://example.og4.me",
];

exports.handler = async (event) => {
  const response = event.Records[0].cf.response;
  const headers = response.headers;

  headers["Content-Security-Policy"] = [
       {
       key: "Content-Security-Policy",
       value: contentSecurityPolicies.join("; "),
       },
  ];

  return response;
};
```

Next steps

- Gestion de la configuration
  - pas de support de variables d'environnement, comment fait-on ?
- Réduire la boucle de feedback
  - écrire des tests -> exemple
  - autres solutions ?
- Génération et injection d'un *nonce* pour les scripts *inline* dans les CSP
  - pour Google Tag Manager, etc