PROTOCOLE HARDERING - HTTP // HTTPS

Pourquoi on ne laisse pas la porte ouverte ?....2
Philosophie : Ego vs Standards....2
La "Défense en Profondeur" (Defense in Depth)....2
Pourquoi au niveau du Reverse Proxy (Traefik) ?....2
Les Standards (RFCs)....2
Les Juges : Outils d'Audit....3
SecurityHeaders.com....3
Mozilla Observatory....3
L'Implémentation : La Méthode "Traefik Middleware"....4
Anatomie des En-têtes (Détails Techniques)....4
Troubleshooting (Quand ça casse)....5
Le Syndrome de la Page Blanche....5
Le Piège YAML (Docker)....5

Pourquoi on ne laisse pas la porte ouverte ?

Par défaut, un serveur web (Nginx, Apache) est poli : il répond à tout le monde, accepte d'être affiché dans une frame, et laisse les navigateurs deviner le type de fichiers. C'est sympa, mais en sécurité, **la politesse est une faille**.

L'objectif du **Hardening HTTP** est d'envoyer des instructions strictes (Headers) au navigateur du client pour transformer ce dernier en allié de la sécurité.

> **Note :** Un serveur sans *Security Headers*, c'est comme laisser les clés de sa voiture sur le contact à Gotham City. Vous *allez* avoir des problèmes.

Philosophie : Ego vs Standards

Pourquoi nous battons-nous pour ces en-têtes ? Est-ce pour flatter l'ego de l'administrateur avec un "A+" ? Non. Le score n'est qu'un indicateur de conformité à des standards industriels ouverts.

La "Défense en Profondeur" (Defense in Depth)

La sécurité ne repose pas uniquement sur le pare-feu. En injectant ces en-têtes, nous utilisons le navigateur du client comme une seconde ligne de défense. Si le pare-feu tombe, le navigateur refuse d'exécuter l'attaque.

Pourquoi au niveau du Reverse Proxy (Traefik) ?

C'est une "Best Practice" architecturale appelée **Security at the Edge**.

- **Découplage :** Le serveur d'application (Nginx/App) ne doit se soucier que de servir le contenu.
- **Sécurité :** Le Reverse Proxy (Traefik) agit comme un douanier. Il tamponne chaque réponse sortante avec les règles de sécurité. Si on change de serveur web demain (Apache, Caddy), la sécurité reste active.

Les Standards (RFCs)

Ces configurations ne sont pas des inventions de Mozilla, mais des applications strictes des protocoles Internet (IETF & W3C) :

En-tête	Standard de Référence	Le Concept Réel
HSTS	RFC 6797	Empêche l'attaque **SSL Stripping**. Même si l'utilisateur tape http://, le navigateur force le https:// avant même d'envoyer le premier paquet.
CSP	W3C Recommendation	Luttre contre les **XSS (Cross Site Scripting)**. C'est une liste blanche : "N'exécute que ce que je connais". C'est l'en-tête le plus complexe mais le plus robuste.
X-Frame	RFC 7034	Empêche le **Clickjacking**. Interdit à un site tiers d'afficher votre site dans une fenêtre invisible pour voler des clics.
Referrer	W3C Candidate	Protection de la **Vie Privée**. Limite les fuites d'informations (URL complètes, tokens en GET) vers les sites externes (Analytics, Pubs).

Les Juges : Outils d'Audit

Avant de corriger, il faut mesurer. Nous utilisons deux références mondiales.

SecurityHeaders.com

- **C'est quoi ?** Un scanner rapide créé par Scott Helme.
- **Le verdict :** Il note de **F** (Passoire) à **A+** (Forteresse).
- **Utilité :** Vérifier la présence des en-têtes de base. C'est le "Contrôle Technique" de votre site.

Mozilla Observatory

- **C'est quoi ?** L'outil d'analyse de la fondation Mozilla (Firefox).
- **Le verdict :** Une note sur 100.
- **Particularité :** Il est impitoyable (le "Dark Souls" du scan web). Il pénalise sévèrement l'usage de scripts "inline" (code JS mélangé au HTML).
- **Objectif Réaliste :** Viser le **B+** pour un site statique standard est excellent. Le **A+** nécessite une architecture complexe.

L'Implémentation : La Méthode "Traefik Middleware"

Plutôt que de modifier la configuration de chaque conteneur Nginx (nginx.conf), nous appliquons la sécurité au niveau du **Reverse Proxy (Traefik)**.

Avantage : Centralisation. On définit le bouclier une fois, on l'applique partout.

Le Code (docker-compose.yml), voici le bloc labels standard à intégrer dans la définition du service Web.

```
labels:
  # ... (Configuration du routage standard) ...

  # --- DÉFINITION DU BOUCLIER (Middleware: sec-headers) ---

  # 1. HSTS (Strict-Transport-Security)
  # "Tu ne me parles qu'en HTTPS pendant 1 an. Pas de HTTP clair."
  traefik.http.middlewares.sec-headers.headers.stsSeconds: "31536000"
  traefik.http.middlewares.sec-headers.headers.stsIncludeSubdomains: "true"
  traefik.http.middlewares.sec-headers.headers.stsPreload: "true"
  traefik.http.middlewares.sec-headers.headers.forceSTSHeader: "true"

  # 2. Anti-Clickjacking (X-Frame-Options)
  # "Interdiction de m'afficher dans une <iframe> sur un autre site."
  traefik.http.middlewares.sec-headers.headers.frameDeny: "true"

  # 3. Anti-Mime-Sniffing (X-Content-Type-Options)
  # "Si je dis que c'est une image, c'est une image. N'essaie pas d'exécuter le code dedans."
  traefik.http.middlewares.sec-headers.headers.contentTypeNosniff: "true"

  # 4. Protection XSS Basique
  traefik.http.middlewares.sec-headers.headers.browserXssFilter: "true"

  # 5. Politique de Référent (Referrer-Policy)
  # "Ne dis pas aux sites externes d'où je viens exactement."
  traefik.http.middlewares.sec-headers.headers.referrerPolicy: "strict-origin-when-cross-origin"

  # 6. Content Security Policy (CSP) - LE GARDIEN
  # "Je n'autorise que les scripts et images venant de MOI-MÊME ('self')."
  # Note : 'unsafe-inline' est toléré ici pour les scripts JS internes simples.
  traefik.http.middlewares.sec-headers.headers.contentSecurityPolicy: "default-src 'self'; script-src 'self'
'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self';"

  # 7. Permissions Policy (Le petit nouveau)
  # "Non, je n'ai pas besoin de ta caméra ni de ton micro."
  traefik.http.middlewares.sec-headers.headers.permissionsPolicy: "camera=(), microphone=(), geolocation=(),
payment=()"

  # --- ACTIVATION DU BOUCLIER ---
  # Application sur le routeur principal
  traefik.http.routers.mon-service-secure.middlewares: "sec-headers"

  # Application sur le routeur de redirection (CRITIQUE pour le A+)
  traefik.http.routers.mon-service-redirect.middlewares: "force-canonical,sec-headers"
```

Anatomie des En-têtes (Détails Techniques)

En-tête	Fonction	Risque Contré
HSTS	**Le Pacte de Sang.** "Une fois qu'on s'est vu en sécurisé, on ne revient jamais en arrière."	**Downgrade Attack** (Force le hacker à décrypter, ce qu'il ne peut pas faire).
X-Frame-Options	**L'Identité Unique.** Empêche un site malveillant de superposer votre site transparent sur le sien pour voler des clics.	**Clickjacking** (Détournement de clic).
CSP	**Le Videur de Boîte.** Il a une liste VIP. Si ton script n'est pas sur la liste (ou ne vient pas de la maison), il ne rentre pas. C'est le header le plus puissant.	**XSS** (Cross-Site Scripting) et Injection de code.
Permissions-Policy	**Le Mode Parano.** Désactive proactivement les API du navigateur (Micro, Caméra, USB) inutilement exposées.	**Spyware / Abus de confiance** via le navigateur.
Referrer-Policy	**L'Agent Secret.** Quand tu quittes le site, on ne dit pas à la destination quelle page précise tu visitais.	**Fuite de données** (Privacy).

Troubleshooting (Quand ça casse)

Le Syndrome de la Page Blanche

Si après déploiement, le site charge mais sans style (moche) ou sans script (boutons inactifs), c'est la **CSP** qui est trop stricte.

- **Diagnostic :** Ouvrir la console du navigateur (F12 > Console). Vous verrez des messages rouges : *"Refused to load... because it violates the Content Security Policy"*.
- **Solution :** Si vous utilisez Google Fonts ou un CDN externe, il faut l'ajouter dans la règle contentSecurityPolicy.
    - *Exemple :* style-src 'self' 'unsafe-inline' https://fonts.googleapis.com;

Le Piège YAML (Docker)

Docker Compose est capricieux.

- **Erreur :** labels must be a mapping ou must be a list.
- **Règle d'Or :**
    - Si vous utilisez des deux-points (:) comme séparateur, NE METTEZ PAS de tiret (-) au début de la ligne.
    - Si vous utilisez des tirets (-), utilisez le signe égal (=) comme séparateur. **Ne mélangez jamais les deux styles.**