Les entêtes HTTP

1. Présentation

Lorsqu'on lance une requête vers un serveur, la requête et la réponse comportent des en-têtes qui fournissent des informations utiles aux serveurs et aux navigateurs.

2. Les principales informations contenues dans l'entête

Entête	Signification et exemple
Accept	Spécifie les types de contenu que le client accepte Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, image/apng, */*;q=0.8
Accept-Charset	Spécifie les jeux de caractères que le client accepte Accept-Charset: utf-8, iso-8859-1;q=0.5, *;q=0.1
Accept-Encoding	Spécifie les types de compression que le client accepte Accept-Encoding: gzip, deflate
Cache-Control	Spécifie les directives de mise en cache pour la ressource demandée Cache-Control: max-age=3600, public
Connection	Spécifie le type de connexion que le client souhaite utiliser Connection: close (fermeture de la connexion après l'envoi de la requête Connextion : Keep-Alive (laisser la connexion ouverte après l'envoi de la requête) timeout : 300 (si précisé définit le temps de conservation de la connexion)
Content-Length	Spécifie la longueur du contenu de la demande Content-Length: 1024
Content-Type	Spécifie le type de contenu de la demande Content-Type: application/json
Cookie	Transmet des informations au serveur Cookie: foo=bar
Host	Spécifie le nom de domaine et le numéro de port du serveur auquel la requête est adressée Host: example.com
Referer	Spécifie l'URL de la page Web qui a fourni un lien vers la page actuelle Referer: https://example.com/page1.html
Upgrade	Spécifie le type de protocole que le client souhaite utiliser Upgrade: websocket
User-Agent	Spécifie le type de client qui effectue la requête User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36

3. Strict-Transport-Security (HSTS)

L'en-tête HTTP Strict-Transport-Security (HSTS) est utilisé pour indiquer aux navigateurs de toujours utiliser une connexion sécurisée (HTTPS) pour interagir avec un site web spécifique. Cela renforce la sécurité en protégeant les utilisateurs contre les attaques telles que les attaques de type Man-in-the-Middle (MITM) qui pourraient tenter de les rediriger vers des versions non sécurisées d'un site.

Lorsque le serveur envoie l'en-tête Strict-Transport-Security dans la réponse HTTP, il spécifie une période de temps (exprimée en secondes) pendant laquelle le navigateur doit forcer l'utilisation de HTTPS. Pendant cette période, le navigateur mémorise cette directive et ne se connecte au site qu'à travers HTTPS, même si l'utilisateur entre une URL avec le protocole HTTP.

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

4. X-Frame-Options

L'en-tête HTTP X-Frame-Options est utilisé pour contrôler si une page web peut être affichée dans un cadre (frame ou iframe). Son objectif principal est de protéger les sites web contre les attaques de clickjacking, où un attaquant tente de tromper l'utilisateur en cliquant sur quelque chose d'apparemment sûr sur une page, alors qu'en réalité, il interagit avec une autre page placée dans un cadre invisible.

Il existe trois directives principales que vous pouvez définir pour l'en-tête X-Frame-Options :

DENY	la page ne peut pas être affichée dans un cadre
SAMEORIGIN	la page peut être affichée dans un cadre uniquement si la demande provient de la même origine (même domaine).
ALLOW-FROM	la page peut être affichée dans un cadre si la demande provient d'une source spécifique (l'URI spécifié).

5. X-Forwarded-For

L'entête HTTP X-Forwarded-For est utilisée pour indiquer l'adresse IP réelle de l'utilisateur lorsque la requête HTTP traverse un ou plusieurs proxys ou serveurs intermédiaires. Cela peut être utile dans les environnements où plusieurs serveurs ou proxys sont impliqués dans la gestion des requêtes et où il est important de connaître l'adresse IP d'origine de la demande.

Lorsqu'un client envoie une requête HTTP à travers un réseau de serveurs, chaque serveur ajoute son adresse IP à l'entête X-Forwarded-For. Ainsi, l'entête peut contenir une liste d'adresses IP, où la première adresse IP dans la liste est celle du client d'origine.

Par exemple, si un client A envoie une requête à un serveur B, qui transmet ensuite la requête à un serveur C, l'entête X-Forwarded-For sur le serveur C pourrait ressembler à ceci :

```
X-Forwarded-For: client_A_IP, server_B_IP
```

Dans cet exemple, client_A_IP est l'adresse IP du client d'origine, et server_B_IP est l'adresse IP du serveur B qui a transféré la requête.

L'entête X-Forwarded-For est souvent utilisée par les applications web pour récupérer l'adresse IP du client réel, en particulier lorsque celles-ci sont derrière des équilibreurs de charge ou des proxys. Cependant, il est important de noter que cet entête peut être falsifiée par un client malveillant, et donc elle ne doit pas être utilisée comme la seule source de confiance pour l'identification des adresses IP.