X-FORWARDED-FOR

I. Qu'est-ce que X-Forwarded-For ?

L'en-tête HTTP X-Forwarded-For (XFF) est utilisé pour identifier l'adresse IP du client d'origine lorsqu'une requête passe par un proxy, un équilibreur de charge ou un autre intermédiaire.

II. Format de l'en-tête

L'en-tête X-Forwarded-For suit généralement ce format :

X-Forwarded-For: client_IP, proxy1_IP, proxy2_IP, ...

- **client_IP** : L'adresse IP de l'utilisateur final.
- **proxy1_IP** : L'adresse IP du premier proxy traversé.
- **proxy2_IP** : L'adresse IP du second proxy, et ainsi de suite.

Le dernier proxy ajoute sa propre adresse IP à la fin de la liste avant de transmettre la requête au serveur suivant.

III. Utilisation et sécurité

Cas d'utilisation

- **Journalisation** : Enregistrer l'IP réelle du client dans les logs.
- **Restrictions d'accès** : Appliquer des règles basées sur l'IP du client.
- **Analyse de trafic** : Identifier la source des connexions.

Problèmes de sécurité

L'en-tête X-Forwarded-For peut être falsifié par un client malveillant. Pour éviter cela :

- **Utiliser un proxy de confiance** pour ajouter et valider l'en-tête.
- **Vérifier la liste des IPs** pour détecter d'éventuelles falsifications.
- **Configurer un pare-feu applicatif (WAF)** pour gérer les adresses IP de manière sécurisée.

X-FORWARDED-FOR

IV. Configuration dans les serveurs web

Nginx

Ajoutez cette directive pour extraire l'IP du client réel :

set_real_ip_from 0.0.0.0/0;

real_ip_header X-Forwarded-For;

real_ip_recursive on;

Apache

Activez le module mod_remoteip et configurez-le comme suit :

RemoteIPHeader X-Forwarded-For

RemoteIPTrustedProxy 192.168.1.1

V. Conclusion

X-Forwarded-For est un en-tête HTTP essentiel pour identifier l'adresse IP des clients derrière un proxy. Son utilisation doit être sécurisée pour éviter toute manipulation frauduleuse des adresses IP.