HTTP - User-Agent

Description

Le User-Agent est une chaîne de caractères envoyée par le client (navigateur Web) dans les en-têtes du protocole HTTP à destination du serveur. Cette information est utilisée par ce dernier afin d'identifier le type du navigateur et la version utilisée par le client. Cette identification permet au serveur de potentiellement adapter le contenu de sa réponse.

Par exemple, si le serveur remarque l'utilisation d'un navigateur sur téléphone portable ou tablette, alors il pourra renvoyer la version “responsive” du site (version adaptée pour les écrans de petite taille).

Prérequis d'exploitation

Pour exploiter cette vulnérabilité, il est nécessaire d'avoir accès à une application se basant sur la valeur de l'en-tête “User-Agent” afin d'adapter les réponses aux différents clients de l'application.

Connaissances nécessaires

- Connaissance de base du fonctionnement du protocole HTTP ;
- Maîtrise de la notion d'en-têtes HTTP.

Outils nécessaires

- Utilisation d’outils de type Burp Suite ou curl pour la création/modification de requêtes HTTP.

Flux d'exécution

Explorer

L'en-tête “User-Agent” est un champ de la requête HTTP qui permet d'identifier le client qui envoie la requête au serveur. En envoyant différentes valeurs pour cet en-tête sur différentes pages de l'application, il est possible de détecter une ou plusieurs réponses différentes du serveur. Cette technique permet de vérifier si le serveur utilise bien la valeur du “User-Agent” pour adapter la réponse au client. Cela peut être utile pour détecter des vulnérabilités ou des comportements spécifiques du serveur en fonction de la valeur de cet en-tête.

Expérimenter

L'analyse des différentes réponses du serveur en fonction des différentes valeurs de “User-Agent” envoyées permet de tenter de tromper le serveur en lui envoyant la valeur attendue. Cette technique peut être utilisée pour contourner des mesures de sécurité mises en place par le serveur qui se basent sur la valeur de cet en-tête. Par exemple, certains serveurs peuvent bloquer les clients qui utilisent des valeurs de “User-Agent” suspectes ou qui ne correspondent pas à celles attendues. En modifiant la valeur de l'en-tête, il est possible de tromper le serveur et de contourner cette mesure de sécurité.

Exploiter

Conséquences potentielles

Une exploitation réussie de ce type de vulnérabilité peut permettre :

- L'accès à des pages sensibles ;
- L'accès à des fonctionnalités sensibles.

Contre-mesures

Les contre-mesures suivantes peuvent être mises en œuvre :

- Mettre en œuvre des contrôles de sécurité robustes pour vérifier la validité de ces en-têtes ;
- Ne pas accorder d'accès à des fonctionnalités sensibles basées uniquement sur la valeur de ces dernières ;
- Maintenir et mettre à jour régulièrement le serveur Web pour corriger les vulnérabilités connues.

Comment cela fonctionne

Les scénarios suivants peuvent être joués via l'exploitation de cette vulnérabilité :

- Utilisation d'un "User-Agent" lié à un navigateur obsolète pour tenter d'accéder à des fonctionnalités qui ne sont plus prises en charge par les navigateurs plus récents ;
- Utilisation d'un "User-Agent" ressemblant à celui d'un navigateur de confiance pour tenter de tromper un serveur.

Exemple 1

Voici un exemple de fichier robots.txt qui permet d'accéder à un endpoint "flag" avec le User-Agent "admin" :

```
User-agent: *
Disallow: /flag

User-agent: admin
Allow: /flag
```

Ce fichier indique qu'un utilisateur ne peut pas accéder à l'endpoint "flag" par défaut et que l'accès est possible seulement avec une valeur de l'en-tête User-Agent à "admin". Cela signifie que seuls les utilisateurs qui utilisent le User-Agent "admin" seront en mesure d'accéder à ce endpoint et aux ressources qui s'y trouvent.

Exemple 2

Il est possible de configurer un serveur Web pour forcer l'utilisation d'un User-Agent spécifique en utilisant une directive "User-Agent" dans le fichier de configuration du serveur. Voici un exemple de configuration pour le serveur Apache :

```
BrowserMatch "MySpecialUserAgent" force-response-1.0
RequestHeader set User-Agent "MySpecialUserAgent" env=force-response-1.0
```

Dans cet exemple, la directive "BrowserMatch" indique que toutes les requêtes qui incluent la chaîne de caractères "MySpecialUserAgent" doivent être marquées comme ayant la variable "force-response-1.0". La directive "RequestHeader" indique que si la variable "force-response-1.0" est présente, le serveur doit remplacer le User-Agent de la requête par "MySpecialUserAgent".

Cela forcera toutes les requêtes provenant du navigateur ou de l'application cliente avec la chaîne "MySpecialUserAgent" à utiliser cette chaîne comme User-Agent. Cela peut être utile dans des cas où une application ou un navigateur spécifique est nécessaire pour accéder à des ressources spécifiques, ou lorsque le serveur nécessite des informations spécifiques du User-Agent pour fonctionner correctement.

References

URL :

- https://developer.mozilla.org/fr/docs/Web/HTTP/Overview
- https://developer.mozilla.org/fr/docs/Web/HTTP/Overview#les_messages_http
- https://developer.mozilla.org/fr/docs/Web/HTTP/Headers
- https://portswigger.net/burp/documentation/desktop/tutorials/intercepting-http
- https://www.hostinger.fr/tutoriels/comment-utiliser-la-commande-curl-sous-linux

Retour fiches vulnérabilités

- Cyber fiches vulnérabilités