HTML - Code Source

Description

Le code source HTML peut contenir des commentaires sensibles qui sont insérés dans le code HTML d'une page web, mais qui ne sont pas visibles pour l'utilisateur final. Les commentaires sont généralement utilisés par les développeurs pour ajouter des notes ou des informations supplémentaires sur le code, mais ils peuvent également être utilisés pour cacher des informations sensibles comme des mots de passe ou des clés d'API.

Prérequis d'exploitation

Pour exploiter cette vulnérabilité, il est nécessaire d'avoir accès à une application qui comporte des commentaires HTML.

Connaissances nécessaires

- Reconnaître des commentaires HTML dans une page web.

Outils nécessaires

- Avoir accès à une console de navigateur (Firefox, Chrome).

Flux d'exécution

Explorer

Naviguer sur l'application pour récupérer les endpoints et/ou pages de l'application puis analyser le code HTML de chaque page.

Expérimenter

Tenter de trouver des commentaires en HTML cachés dans le code source de la page et analyser leur contenu.

Exploiter

Conséquences potentielles

Une exploitation réussie de ce type de vulnérabilité peut permettre :

- L'accès à des informations sensibles telles que des identifiants de connexion ;
- La recherche de vulnérabilités en énumérant le fonctionnement ou la/les version(s) des composants de l'application.

Contre-mesures

Les contre-mesures suivantes peuvent être mises en œuvre :

- Ne pas inclure d'informations sensibles dans les commentaires en HTML ;
- Utiliser des contrôles d'accès basés sur les rôles et les autorisations pour limiter l'accès aux pages web contenant des commentaires sensibles ;
- Utiliser un pare-feu applicatif pour bloquer les requêtes HTTP non autorisées ou suspectes.

Comment cela fonctionne

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

- L'utilisation d'informations confidentielles pour se connecter sur un espace protégé par un mot de passe ;

- L'énumération d'informations sensibles sur le serveur ou l'application afin de mener une attaque.

Exemple 1

Voici un exemple de page HTML simple contenant un commentaire qui fournit des identifiants en clair :

```
<!DOCTYPE html>
<html>
    <head>
        <title>Exemple de commentaire sensible</title>
    </head>
    <body>
        <h1>Bienvenue sur notre site web</h1>
        <!-- Identifiants: login: admin, mot de passe: secret -->
    </body>
</html>
```

Dans cet exemple, le commentaire HTML caché dans le code contient les identifiants de connexion (login: “admin”, mot de passe: “secret”). Si cette page est accessible à un attaquant, il peut facilement récupérer ces informations sensibles et les utiliser pour accéder au système.

Exemple 2

Voici un exemple de page HTML simple contenant un commentaire qui indique la présence d'une page de debug de l'application :

```
<!DOCTYPE html>
<html>
    <head>
        <title>Exemple de lien sensible</title>
    </head>
    <body>
        <h1>Bienvenue sur notre site web</h1>
        <!-- <a href="/utils/debug_dev.php">Debug</a>-->
    </body>
</html>
```

Dans cet exemple, le commentaire HTML caché dans le code contient un lien vers la page “/utils/debug_dev.php” qui semble être une page de debug à destination des équipes de développement.

CWEs

- CWE-200 : Exposure of Sensitive Information to an Unauthorized Actor
  - The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.
- CWE-540 : Inclusion of Sensitive Information in Source Code
  - Source code on a web server or repository often contains sensitive information and should generally not be accessible to users.
- CWE-615 : Inclusion of Sensitive Information in Source Code Comments
  - While adding general comments is very useful, some programmers tend to leave important data, such as: filenames related to the web application, old links or links which were not meant to be browsed by users, old code fragments, etc.

References

URL :

- https://dane.ac-reims.fr/images/enseigner/classes_virtuelles/PDF/Debuter_avec__html.pdf
- https://pedagogie.ac-toulouse.fr/informatique/sites/informatique.disciplines.ac-toulouse.fr/files/fichiers/web/3._lhtml_cor.pdf
- https://www.tutorialspoint.com/html/html_tutorial.pdf

https://lewebpedagogique.com/isneiffel/files/2017/06/Langage-HTML.pdf

Retour fiches vulnérabilités

- Cyber fiches vulnérabilités