Cryptanalyse - Encodage

Description

En informatique, l'encodage consiste à transformer des données en clair en une chaine de caractères encodée par un algorithme ou une table d'encodage. L'encodage peut avoir plusieurs avantages tels que la facilité de retranscription des caractères spéciaux (URL encodage) ou encore le transfert de données complexes (une image) au travers de médias ne supportant que des données textuelles.

Pré-requis d'exploitation

Pour exploiter cette méthode informatique, il est nécessaire d'avoir une connaissance approfondie de l'algorithme d'encodage utilisé, ainsi que des compétences en programmation pour pouvoir l'implémenter dans un logiciel ou un script. Il est également important de comprendre les limitations et les vulnérabilités potentielles de la méthode d'encodage en question, ainsi que les attaques courantes qui peuvent être utilisées pour la compromettre.

Connaissances nécessaires

- Connaissance des principes de base de la cryptographie et de l'encodage de données ;
- Connaissance des méthodes utilisées pour casser les codes.

Outils nécessaires

- Outils tels que des bibliothèques de cryptographie ou des outils en ligne permettant de chiffrer et de déchiffrer des données selon le type de code choisi (Dcode, Cyberchef).

Flux d'exécution

Explorer

Lire la chaine de caractère encodée, analyser sa taille, la base (décimal, hexadécimal, base64) et les caractères qu'elle comporte.

Expérimenter

Dans un premier temps, tenter de bruteforcer la chaine encodée avec des outils en ligne puis lancer des outils offline si besoin. Par la suite, tenter différentes méthodes (analyse de fréquence, brute force, guessing de caractère manquant, ...) en fonction du type d'encodage identifié.

Exploiter

Conséquences potentielles

Une exploitation réussie d’une vulnérabilité dans ce domaine peut permettre :

- La divulgation d'informations sensibles ;
- La compromission d'une base de données ou d'un serveur et des données des utilisateurs qu'ils contiennent.

Contre-mesures

Les contre-mesures suivantes peuvent être mises en œuvre :

- Utiliser des algorithmes de chiffrement sécurisés et reconnus ;
- Utiliser un pare-feu applicatif pour bloquer les requêtes excessives ou suspectes afin d’empêcher les attaques par brute force.

Comment cela fonctionne ?

Le scénario suivant peut être joué via l'exploitation de cette vulnérabilité :

- Un attaquant réussit à accéder à une base de données contenant des informations sur les utilisateurs, telles que leurs noms d'utilisateur et leurs mots de passe encodés en base64. Pour pouvoir récupérer les mots de passe en clair, l'attaquant peut alors facilement décoder la base64 en utilisant un outil en ligne par exemple. Il peut ainsi se connecter avec les identifiants de l'utilisateur qu'il a récupérés et potentiellement usurper son identité.

Exemple 1

Le chiffrement Base64 est une technique d'encodage largement utilisée qui permet de représenter des données binaires sous forme de texte ASCII. Elle consiste à diviser les données binaires en groupes de 3 octets (24 bits), puis à convertir chaque groupe en 4 caractères ASCII.

Voici un exemple de mot de passe encodé puis décodé en Base64 :

```
    Mot de passe : "motdepasse"
    Message encodé : "bW90ZGVwYXNzZQ=="
```

Explication de l'encodage : Le mot de passe **motdepasse** est divisé en groupes de 3 octets (24 bits) : **mot**, **dep**, **ass** et **e==**. Chaque groupe est ensuite converti en 4 caractères ASCII en utilisant une table de correspondance prédéfinie. Par exemple, le groupe **mot** est converti en **bW90**, le groupe **dep** en **ZGVw**, etc.

Explication du décodage : Pour décoder le message encodé en Base64, la technique inverse de codage est utilisée. Chaque groupe de 4 caractères ASCII est converti en son équivalent binaire de 24 bits, puis les groupes de 3 octets sont combinés pour reconstituer les données binaires d'origine. Par exemple, le groupe **bW90** est converti en **mot**, le groupe **ZGVw** en **dep**, etc.

CWEs

- CWE-261 : Weak Encoding for Password
    - Obscuring a password with a trivial encoding does not protect the password.

References

URL :

- https://www.zonensi.fr/NSI/Premiere/C02/CodageCaractere/CodageCaractere.pdf
- http://deptinfo.unice.fr/twiki/pub/Linfo/PlanningDesSoutenances20032004/blanc-degeorges.pdf
- https://perso.liris.cnrs.fr/nicolas.pronost/UCBL/CapesInfo/PrepaEcrit/AlgoProg/07-Chiffrement%20et%20cryptographie.pdf

Retour fiches vulnérabilités

- Cyber fiches vulnérabilités