Faille de Sécurité

Projet de Synthèse Master 2 SSI - 2014

Sommaire

1. Type de faille

Il s'agit d'une faille qui ne concerne pas une partie du code et ne nécessite pas de compétences particulières.
Dans notre cas, il suffit de faire comme beaucoup de hackers font, à savoir du social engineering.

2. Qu'est-ce que le social engineering ?

Le social engineering consiste pour l'attaquant à prendre connaissance des habitudes de l'utilisateur. Il peut également prendre en compte les diverses informations personnelles de lui présent sur internet. Ces informations sont facilement accessibles grâce à l'explosion des réseaux sociaux et de l'indexation plus que puissante de Google.
Ainsi il peut récolter les habitudes, le nom des animaux, des loisirs, la date de naissance, le nom des enfants de la cible etc. Cela va lui permettre de dresser une liste de mots, qu'il va ensuite pouvoir assembler afin de trouver un mot de passe, lui donnant ainsi accès à des informations confidentielles.

C'est cet aspect de la sécurité que nous avons voulu mettre en avant.
En effet, beaucoup de développeurs font très attention à la sécurité de leur code en échappant les caractères spéciaux des formulaires, en mettant en place nombre de firewalls et de procédures de sécurité. Mais face à toutes ces mesures, nombre sont ceux qui utilisent des mots de passe jugés trop faibles et reprenant des informations les concernant.

3. Exploitation de notre faille

Dans notre cas, le social engineering est réalisable en associant les différents noms et prénoms des membres de notre groupe.
Cette recherche permet d'accéder par exemple à l'administration du wiki. En effet, le compte root du mediawiki est facilement trouvable.

Il en va de même pour le mot de passe de la base de données qui est composé de la même manière.

4. Conclusion

Le social engineering concerne une nouvelle partie des piratages. On peut voir qu'il est très facile d'exploiter cette erreur humaine.
Les fuites des mots de passes Adobe ou encore les dernières statistiques concernant les mots de passe les plus utilisés le prouvent bien. Les personnes en utilisent des trop faibles et il est donc simple de les récupérer.
Il faut donc prendre en compte ce point de sécurité en obligeant les utilisateurs (et nous même) à utiliser des mots de passe forts n'ayant de surcroît aucun rapport avec notre vie privée et nos habitudes.