

Projet Sécurité: CTF



GROUPE	BACKDOOR	SCENARIO 21/10
PHASE 1	DEVELOPPEMENT CTF	WEB
NIVEAU	MOYEN	



Le Blog de John

Les participants se retrouvent sur le site web officiel de l'entreprise X, où ils découvrent un blog personnel prétendument appartenant à John, l'un des employés de l'entreprise. Le site a une page d'accueil avec des articles et des informations sur John, mais il y a aussi des éléments cachés et des indices disséminés dans le site.

Temps estimé: 30 mins

Etapes:

1/Blog de John :

Pour obtenir le premier flag, il faut trouver le nom d'utilisateur et le mot de passe de John. Les indices se trouvent sur le blog, y compris son âge, sa date de naissance, le nom de son poisson de compagnie, etc. il faut ensuite utiliser ces informations pour bruteforcer la connexion au compte de John, où le nom d'utilisateur est simplement "john" et le mot de passe est la combinaison des informations disponibles.

2/Code Source :

Le deuxième flag est caché dans le code source de la page. On peut y accéder en inspectant la page. On y trouve une chaîne de caractères encodée en base64. Après un premier décodage, on obtient une autre chaîne de caractères en base64. Le deuxième flag se trouve après un deuxième décodage de cette chaîne.

3/Soumission :

Pour le troisième flag, on doit revenir à la page principale du blog de John, où on se retrouve avec une case de texte et un bouton "Submit". Il suffit d'entrer le premier flag (la combinaison de données personnelles de John) dans la case, puis cliquer sur le bouton "Submit". Après avoir soumis le bon premier flag, le troisième flag s'affichera.