Sécurité des Applications

Janvier 2021 | **Serie 8**

Stéphane Küng

1 Administratif

Ce travail **individuel** doit être rendu avant la date indiquée sur le ScoreBoard au format **PDF** sur CyberLearn.

1.1 Clarification

Dans vos rapports d'exercices, faites attention à bien inclure:

- Captures d'écran de réussite
- Payload utilisés
- Tout **code source** utilisé ou créé (ou en annexe)
- Nom des outils utilisés
- Configuration

1.2 Password 1

Pour cet exercice, implémentez un système de login simple[1] avec une `fonction de dérivation de mot de passe`[2]. Les hashs peuvent être stoqués dans un fichier texte, une base `SQLite`, ou autre...

Les charactères **unicodes** comme les Emoji, Accents, et caractères exotiques doivent être acceptés

Cette serie d'exercice peut être réalisée soit au travers d'une application standalone (`C#`, `C`, `Java`, `Python`, ...) en mode fenêtré ou console, soit au travers d'une Application WEB (`PHP`, `Node`, `Python`, `Ruby`, ...).

1.3 Password 2

Ajouter à votre système de login une authentification avec `OpenID Connect` avec un fournisseur publique comme `Github`, `Google`, `Twitter`, `Yahoo`, `OpenID`, ou autre.

1.4 Password 3

Si vous avez opté pour une application WEB :

Ajouter à votre système de login une authentification avec `SAML`. Il vous faut pour ça un `Identity Provider` (`IdP`), la page ici en propose un certain nombre utilisable gratuitement ou en mode démo comme `Azure`, `Gluu`, `miniOrange`, `Okta`, `Ping Identity`, `samlidp.io`.

Si vous avez opté pour une application Standalone :

Ajouter à votre système de login une authentification avec `PKCE` avec un fournisseur publique de votre choix.

[1] `Lyra2`, `Balloon`, `Argon2`, `bcrypt`, `scrypt`, `PBKDF`, ...
[2] Pas besoin d'implémenter un cookie de session, de timeout, de gestion de droits, ...