ASIX2 - PHP: M9UF1

UF1 - Entrega #1

Gener de 2024

Versió 3.0

Professor: David González Roldán / Josep Mª Ruiz Rios

Control de Versions

Versió	Comentaris	Professor	Curs	Data
1.0	Primera versió	David González	Alumnes DAM2/ASIX2	08/01/2021
2.0	Pràctica revisada al nou curs i adaptada exclusivament per ASIX2	David González	Alumnes ASIX2	08/12/2021
3.0	Pràctica revisada per al nou curs.	Josep Ruiz	Alumnes ASIX2	25/01/2024

ÍNDEX

1 Pràctica #1 – Registre Bàsic d'Usuaris i Login de EduHacks

1.1 Enunciat

Has arribat fins aquí i no ha estat fàcil, però, ara bé, la prova de foc i on ja començarem a tastar el camp de batalla real, la nostra missió serà unificar tots els coneixements rebuts fins ara i crear les primeres estructures d'una futura plataforma de CTF pública al més pur estil root.me i que hem batejat amb el nom en clau "**EduHacks**".

Ara per ara, però, n'hi haurà prou amb crear les estructures requerides per suportar el sistema de registre i login d'usuaris.

1.2 Requeriments

Amb relació a la BDs

- El script de BDs haurà de ser compatible amb MySQL/MariaDB
- La BDs s'anomenarà "eduhacks" i usarà per defecte codificació UTF-8 MB4 case sensitive.
- Contindrà una taula anomenada "users" amb els següents camps:
    - **iduser** (PK): Integer (Autoincrementable)
    - **mail**: Varchar(40) (Unique)
    - **username**: Varchar(16) (Unique)
    - **passHash**: Varchar(60)
    - **userFirstName**: Varchar(60)
    - **userLastName:** Varchar(120)
    - **creationDate:** Datetime
    - **removeDate:** Datetime
    - **lastSignIn:** Datetime
    - **active:** TinyInt(1)

Amb relació al portal web:

- Cal que el portal sigui web responsive (ho haureu de verificar).

- Mostrar el logo de la nostra marca “EduHacks”
    - Pot ser tan sols un text, però sigueu creatius i utilitzeu per exemple Google Fonts o similars https://fonts.google.com/
- Escollir una imatge de fons per representar “EduHacks”.
    - https://pixabay.com/es/
    - https://www.pexels.com/ca-es/
    - https://unsplash.com/
    - https://www.freeimages.com/es
- Considerar l’ús de fontawesome si voleu afegir icones gràfiques/logos a la vostra web (opcional): https://fontawesome.com/
- Cal que la web d’entrada (index.php) sigui directament el formulari de Login
    - Únicament 2 camps d’entrada (obligatoris) i el botó de Sign In:
        - Username / Mail (s’admetrà com a login vàlid l’ús del email o del username).
        - Password
- Addicionalment cal mostrar una secció secundària del tipus “Don’t have an account yet? Sign Up”
    - Al fer click a signup, caldrà obrir el fitxer register.php amb el formulari de registre
        - Username (Obligatori)
        - Email (Obligatori)
        - First Name (Opcional)
        - Last Name (Opcional)
        - Password (Obligatori)
        - Verify Password (Obligatori)
- Cal elaborar un web principal anomenat home.php que únicament serà accessible per usuaris loginats i que sols ha de contenir una imatge de fons i un text donant la benvinguda a l’usuari que pertoqui i un botó per fer logout i tancar la sessió (logout.php).

Amb relació a la lògica de negoci del Login:

- A l'enviar-se el formulari cal verificar que el username/email es correspon efectivament amb un username/email donat d'alta a la taula "users" i amb valor "1" al camp "active".

- Si s'ha verificat que existeix un usuari actiu es comprovarà el password introduït per l'usuari amb el valor de hash desat a la BDs (camp "passHash").
- Si s'ha verificat la parella usuari/password i aquest està actiu anirem a parar a la pantalla "home.php" on se'ns donarà la benvinguda fent ús de les nostres dades, en cas contrari, cal mostrar un missatge d'error indicant que no és possible fer login amb les dades facilitades (important NO dir quin és el motiu exacte).
- Addicionalment, cada vegada que el Login sigui correcte, caldrà actualitzar el valor de data i hora que es desa en el camp "lastSignIn" de l'usuari afectat. Això ens permetrà detectar usuaris inactius més endavant i fer campanyes promocionals.
- El login implica la creació d'una sessió d'usuari i les cookies associades a aquesta.

Amb relació a la lògica de negoci del Registre:

- Al enviar-se el formulari cal verificar que el username/email no existeixen ja a la BDs, en cas de fer-ho, caldrà informar a l'usuari que no es possible utilitzar el nom d'usuari o mail introduït.
- Si el username i email efectivament no existeixen es procedirà a l'alta de l'usuari a la BDs amb les dades facilitades.
    - A la BDs mai desarem la password de l'usuari, sinó que en desarem el seu hash (veure consideracions addicionals).
    - Caldrà assignar el valor de la data i hora actuals al camp "creationDate".
    - Caldrà assignar el valor "1" al camp "active".
- Una vegada completat amb èxit el registre, caldrà informar de l'èxit de l'operació a la web principial (index.php).

Amb relació a la lògica de negoci de la pàgina Home.php:

- L'intent d'accedir a la mateixa sense tenir oberta una sessió d'usuari, comportarà una redirecció automàtica a la pàgina de login (index.php).
- Si un usuari que té una sessió oberta accedeix a index.php, serà automàticament redireccionat a home.php.
- Els usuaris podràn fer logout i, per tant, tancar la sessió i les cookies associades, fent ús del botó logout d'aquesta pàgina i que conduirà a "logout.php".

Amb relació a la lògica de negoci de la BDs:

- Cal fer ús de connexions persistents.
- Cal que l'operativa de connexió a la BDs es trobi separada amb un fitxer php específic.
- Cal implementar un o diversos fitxers a tall de llibreria d'accés a dades. Aquests fitxers són els que han d'implementar les funcions requerides amb relació a les consultes, inserts, updates, ...

Consideracions addicionals:

1. Cal que adoptis unes mínimes mesures de seguretat que evitin el XSS.
2. La validació del password es farà contra els valors de hash desats invocant la funció **password_verify()**: https://www.php.net/manual/es/function.password-verify.php
3. El valor a desar dels passwords es calcularà invocant a la funció **password_hash**(): https://www.php.net/manual/es/function.password-hash.php
4. **No es pot confiar en les entrades de dades**, assegura't de protegir les dades contra injeccions de codi.
5. Pots afegir les millores que estimis oportunes per millorar l'experiència d'usuari, per exemple amb validació a costat client via JavaScript.
6. Pots inspirar-te en les webs de Facebook o Instagram per agafar idees.

Recorda que aquesta entrega s'ampliarà posteriorment per anar-hi afegint noves funcionalitats, així que et recomano fer el codi mantenible i comentar-lo convenientment.

1.3 ENTREGA

Com a bon professional, una vegada completada la pràctica, pujaràs tots els fitxers necessaris a un repositori de GitHub públic i en facilitaràs l'enllaç al teu responsable a través del Moodle.

És important que hi sigui tot, o del contrari, quan baixem el repositori no ho podrem posar en funcionament!