**4. Egy webalapú szoftvert többfelhasználós működésre kell kialakítani. Tervezze meg a webalapú szoftver többfelhasználós működését, definiálja a működéshez szükséges komponenseket, és alakítsa ki a szükséges biztonsági megoldásokat!**

* Ismertesse a webalapú rendszerek felhasználókezelési megoldásait és jellemzőit!
* Ismertesse a jelszókezelésre és tárolásra vonatkozó alapelveket!
* Mutasson be ‒ egy webalapú szoftver esetében ‒egy teljes körű felhasználókezelési megoldást!
* Ismertesse a leggyakoribb felhasználói fiókok elleni támadási módszereket, és tegyen javaslatot az ellenük való védekezésre!

**A tételhez segédeszköz nem használható.**

**-------------------------------------------------------------------------------------**

Íme néhány javaslat egy webalapú szoftver többfelhasználós működésének megtervezéséhez:

* Határozza meg a szoftver követelményeit és céljait, beleértve a felhasználók számát, szerepkörüket és jogosultságaikat, a megosztandó adatokat és erőforrásokat, valamint a teljesítmény- és biztonsági korlátozásokat.
* Tervezze meg a szoftver architektúráját úgy, hogy az támogassa a több felhasználót, és lehetővé tegye számukra az együttműködést és a megosztott erőforrásokhoz való biztonságos és hatékony hozzáférést. Ez magában foglalhatja az ügyfél-kiszolgáló modell, a mikroszolgáltatási architektúra vagy a kettő kombinációjának használatát.
* Válassza ki a megfelelő technológiákat és keretrendszereket a szoftver megvalósításához, például webszerver, adatbázis-kezelő rendszer, valamint programozási nyelv és futásidejű környezet.
* Fejlessze ki a szükséges biztonsági megoldásokat, hogy megvédje a szoftvert és felhasználóit az olyan fenyegetésekkel szemben, mint a jogosulatlan hozzáférés, az adatok megsértése és a rosszindulatú szoftverek támadásai. Ez magában foglalhatja hitelesítési és engedélyezési mechanizmusok, titkosítási és biztonságos kommunikációs protokollok, valamint rendszeres biztonsági frissítések és tesztelések végrehajtását.
* A szoftver tesztelése és telepítése egy termelési környezetbe, például egy felhőplatformra vagy egy dedikált szerverre, valamint teljesítményének és biztonságának figyelemmel kísérése annak biztosítása érdekében, hogy a szoftver megfeleljen a felhasználók igényeinek.

A webalapú szoftver működéséhez szükséges néhány komponens a következő lehet:

* Webszerver: Ez az összetevő felelős a felhasználók webböngészőitől érkező kérések fogadásáért és megválaszolásáért, a szükséges weboldalak és erőforrások kiszolgálásáért, valamint az ügyfelek és a kiszolgáló közötti kapcsolat kezeléséért.
* Adatbázis: Ez a komponens tárolja és kezeli a szoftver által használt adatokat, beleértve a felhasználói fiókokat, jogosultságokat és egyéb alkalmazásspecifikus adatokat. A szoftver követelményeitől függően relációs vagy nem relációs adatbázis-kezelő rendszert használhat.
* Alkalmazási logika: Ez a komponens valósítja meg a szoftver üzleti logikáját és funkcióit, például a felhasználói hitelesítést, az adatfeldolgozást és a felhasználói felület interakcióit. Írható programozási nyelven, például Java, Python vagy C# nyelven, és használhat webes keretrendszert, például ASP.NET vagy Flask.
* Biztonsági megoldások: Ez az összetevő biztosítja a szükséges biztonsági intézkedéseket a szoftver és a felhasználók fenyegetésekkel szembeni védelméhez, például hitelesítési és engedélyezési mechanizmusokat, titkosítást, valamint rendszeres biztonsági frissítéseket és tesztelést. Olyan technológiákat használhat, mint a HTTPS, a nyilvános kulcsú infrastruktúra és a behatolásérzékelő és -megelőző rendszerek.

A webalapú rendszerek felhasználókezelési megoldásait és funkcióit úgy tervezték, hogy támogassák a felhasználói fiókok létrehozását, kezelését és hitelesítését egy webalapú alkalmazásban. Néhány gyakori felhasználókezelési megoldás és funkció a következő:

* Felhasználói regisztráció: Ez lehetővé teszi az új felhasználók számára, hogy személyes adataik, például nevük, e-mail címük és jelszavuk megadásával fiókot hozzanak létre a rendszerben.
* Felhasználói bejelentkezés: Ez lehetővé teszi a regisztrált felhasználók számára, hogy felhasználónevük vagy e-mail címük és jelszavuk segítségével bejelentkezzenek a rendszerbe, és hozzáférjenek az alkalmazás funkcióihoz és erőforrásaihoz.
* Jelszó-visszaállítás: Ez lehetővé teszi a felhasználók számára, hogy e-mail címük megadásával vagy biztonsági kérdések megválaszolásával visszaállítsák jelszavukat, ha elfelejtették azt.
* Felhasználói szerepek és jogosultságok: Ez lehetővé teszi, hogy az alkalmazás különböző szerepköröket határozzon meg a felhasználók számára, például rendszergazda, moderátor vagy normál felhasználó, és az egyes szerepkörökhöz különböző jogosultságokat rendeljen. Ez lehetővé teszi az alkalmazás számára, hogy szabályozza, mely felhasználók milyen funkciókhoz és erőforrásokhoz férhetnek hozzá.
* Felhasználói profilok: Ez lehetővé teszi a felhasználók számára, hogy megtekintsék és frissítsék személyes adataikat és beállításaikat, például nevüket, e-mail címüket és profilképüket.
* Felhasználói tevékenységi naplók: Ez lehetővé teszi az alkalmazás számára, hogy nyomon kövesse és naplózza a felhasználók tevékenységeit, például azt, hogy mikor jelentkeztek be, milyen erőforrásokhoz fértek hozzá, és milyen változtatásokat hajtottak végre a rendszerben. Ez biztonsági és ellenőrzési célokra használható.
* Összességében a felhasználókezelési megoldások és funkciók elengedhetetlenek azon webalapú rendszerek számára, amelyeknek több felhasználót kell támogatniuk, és biztonságos és személyre szabott élményt kell nyújtaniuk számukra.

A jelszavak kezelése és tárolása kritikus szempont az online fiókok és személyes adatok biztonságának fenntartásában. Fontos, hogy erős és egyedi jelszavakat használjon minden egyes fiókjához, és ezeket a jelszavakat biztonságos módon tárolja. Ennek egyik módja a jelszókezelő használata, amely egy olyan eszköz, amely segít létrehozni és tárolni az erős, egyedi jelszavakat az összes online fiókjához. Így csak egyetlen fő jelszót kell megjegyeznie, a jelszókezelő pedig minden egyes fiókjához kitölti a megfelelő jelszót, amikor be kell jelentkeznie. Ez segíthet megvédeni Önt a hackerek és más fenyegetések ellen, és megkönnyíti a jelszavak kezelését.

Az alábbiakban röviden áttekintjük egy webalapú szoftver lehetséges felhasználókezelési megoldását:

* Először is, a szoftvernek rendelkeznie kell egy biztonságos és megbízható hitelesítési rendszerrel, amely lehetővé teszi a felhasználók számára, hogy fiókokat hozzanak létre és bejelentkezzenek a rendszerbe. Ez erős jelszószabályok alkalmazásával, valamint kétfaktoros hitelesítés vagy más, a felhasználó személyazonosságát igazoló módszerek bevezetésével érhető el.
* Miután a felhasználók bejelentkeztek, képesnek kell lenniük saját fiókbeállításaik kezelésére, például jelszavuk, személyes adataik és preferenciáik frissítésére. A rendszernek lehetővé kell tennie a felhasználók számára, hogy saját jogosultságaikat és hozzáférési szintjeiket kezeljék a szoftveren belül, hogy csak az általuk engedélyezett funkciókhoz és funkciókhoz férhessenek hozzá.
* A rendszernek emellett lehetőséget kell biztosítania a rendszergazdák számára, hogy a szoftveren belül valamennyi felhasználó fiókjait és jogosultságait kezelhessék. Ez magában foglalhatja új fiókok létrehozását, a felhasználói adatok frissítését, valamint az egyes funkciókhoz vagy funkciókhoz való hozzáférés hozzárendelését vagy visszavonását.
* Összességében egy jó felhasználókezelési megoldásnak lehetőséget kell biztosítania a felhasználók számára, hogy biztonságosan hozzáférjenek saját fiókjaikhoz és kezeljék azokat, ugyanakkor a rendszergazdáknak is meg kell adniuk a szükséges eszközöket a rendszeren belüli összes felhasználó fiókjának kezeléséhez.

A felhasználói fiókok megtámadásának néhány gyakori módszere a következő:

* A támadó a karakterek sokféle kombinációjának kipróbálásával próbálja kitalálni a felhasználó jelszavát.
* Szótári támadások, amelyek során a támadó a gyakori szavak és kifejezések előre kiszámított listáját használja a felhasználó jelszavának kitalálására.
* Adathalász-támadások, amelyek során a támadó úgy próbálja rávenni a felhasználót a jelszava elárulására, hogy hamis e-mailt vagy üzenetet küld neki, amely legitim forrásnak tűnik.
* Rosszindulatú támadások, amelyek során a támadó vírussal vagy más rosszindulatú szoftverrel fertőzi meg a felhasználó számítógépét, hogy hozzáférjen a fiókjaihoz.
* Fontos, hogy erős, egyedi jelszavak használatával és azzal, hogy senkinek sem adja ki a jelszavát, biztonságban tartsa fiókjait. Használjon kétfaktoros hitelesítést is, ha az elérhető a fiókjaihoz, mivel ez segíthet megvédeni azokat még akkor is, ha a jelszava veszélybe kerül.

A támadások ellen a következő lépésekkel védekezhet:

* Használjon erős, egyedi jelszavakat minden egyes fiókjához. Kerülje, hogy ugyanazt a jelszót használja több fiókhoz, és győződjön meg arról, hogy jelszavai hosszúak és összetettek.
* Használjon kétfaktoros hitelesítést (2FA), ha az elérhető a fiókjaihoz. Ez egy plusz biztonsági szintet jelent, mivel a bejelentkezéskor a jelszaván kívül egy egyszeri kódot is meg kell adnia.
* Vigyázzon, hogy ne adja ki jelszavát senkinek, és kerülje a gyanús e-mailekből vagy üzenetekből származó linkekre való kattintást vagy mellékletek letöltését.
* Tartsa naprakészen szoftvereit, beleértve az operációs rendszert és a telepített biztonsági szoftvereket is. Ez segíthet megvédeni a rosszindulatú szoftverek támadásai ellen.
* Fontolja meg egy jelszókezelő használatát, amely segít erős, egyedi jelszavakat létrehozni és tárolni az összes fiókjához. Ez megkönnyítheti az erős jelszavak használatát anélkül, hogy mindet megjegyeznie kellene.