Elméleti kérdés

1. Miért fontos a hitelesítés két fél között? Milyen támadások és módszerek vannak a hitelesítés kijátszására?
2. Milyen tipikus gyengeségei vannak a hozzáférés vezérlésnek?
3. Miért kritikus a fájl feltöltés funkció és hogyan tudjuk a futtatható fájlok feltöltését szűrni és validálni?
4. Mi az obfuszkáció és milyen biztonsággal kapcsolatos veszélyei vannak a használatának?
5. Sorold fel az elméleti és a gyakorlati taxonómiákat! Részletesen mutass be egyet!

Gyakorlati kérdés

Gyakorlati megoldásoknál törekedjetek arra, hogy minél részletesebb legyen a válasz. Ahol lehet képernyőképekkel mutasd be, hogy jutottál el a megoldásig.

1. SQL injection támadással adja meg a products táblából az autók nevét, árát és a tulajdonos azonosítóját! Írja le az SQL parancsot!
2. Adjon meg egy XML XXE támadást az admin felhasználó nevében, ahol az autó neve legyen Tesla, ára 2000 és a támadás következményeként megjelenik a leírás részben az etc/passwd! Töltsd fel az xml-t és készíts egy képernyőképet az eredményről
3. Adja meg  [http://www.insecar.com/adm](%20http%3A//www.insecar.com/admf) oldal jelszavát. (Figyelj arra, hogy nem a hash érték kell) Mi lenne a jelszó ha a következő beégetett érték szerepelne: ce9e730864b828b56d23f93abb71571c29b0d1b8 ?
(plusz pont ha megtalálod az eredeti értéket, illetve jár a pluszpont ha nem találod meg az eredeti értéket de kifejted milyen okai lehetnek ennek)
4. Adja meg a script kódot, amellyel CSRF támadással lecseréli a bejelentkezett felhasználó adatait a saját nevére és az általad választott jelszóra az insecar oldalon.
5. Mutass be egy Reflected XSS támadást, amely az Insecar oldalon kiírja a neved és utána egy véletlen számot! Írd le a támadás kódját!