Sikkerhedsmæssige Problemstillinger

Error Handling

En sikkerhedsmæssig problemstilling vi allerede har taget os af, men stadig er værd at nævne er errorhandling. Før vi fik vores error handling på plads printede vores hjemmeside bare en lang error message på selve siden, og problemet med dette var at det gjorde hjemmesiden sårbar over for hacking. Vi løste dette via error-logging og dermed også en error-handler, således at fejl beskeden på bruger siden ikke gav nogen følsom information væk.

Injection Flaws (SQL)

SQL Injection fungerer ved at sende en data forespørgsel til en SQL database som giver et udslag der ikke er efter original intention. For eksempel kan der sendes SQL kommandoer vha. af en login funktion der tjekker authentication informationer imod databasen, hvis der ikke er implementeret funktioner der begrænser hvad databasen kan modtage. Derfor er det vigtigt at definere/begrænse hvad der kan sendes til databasen vha. applikationen. Denne type angreb kan eksempelvis fungere ved at foretage direkte kommandoer til databasen der kan slette eller udtrække sensitivt data.

Korrekt autorisering af bruger-sessions

Hjemmesider benytte ofte cookies etc til validering af aktive sessions, som kan indeholde sensitive brugerinformationer. Ved hensigtsmæssig håndtering af sessions bør sessions’ ID invalideres ved lukning af browser eller bruger logger ud. Hvis dette ikke er situationen kan e.g aktive cookies stadig benyttes ondskabsfuldt.

Hashing af f.eks. Passwords

Ved hashing af passwords bruger vi en algoritme, der “scrambler” brugerens kodeord, sådan at databasen ikke indeholder brugerens kodeord, men indeholder den hashede kode. Et yderligere problem ved dette er at hashing algoritmer er offentligt kendte, og derfor ville man stadig kunne lave et automatiseret angreb, så snart angriberen har fundet ud af hvilken algoritme, som er brugt.

Løsningen til dette er at man tilføjer “salt” til sin hashing. Salt er en, unik for hver kode, tilfældig tilføjelse til kodeordet inden dette bliver hashet. Så kan angriberen ikke længere bare bruge et automatiseret angreb, og han må derfor manuelt sidde og kæmpe sig igennem hvert et password. Derudover kunne vi også tilføje en pepper, som er samme tankegang som med salt, bortset fra at pepperet ikke er gemt på samme lokation, og pepperet vil være én global “kode” for alle brugere. Pepper bliver dog ofte set som overkill.