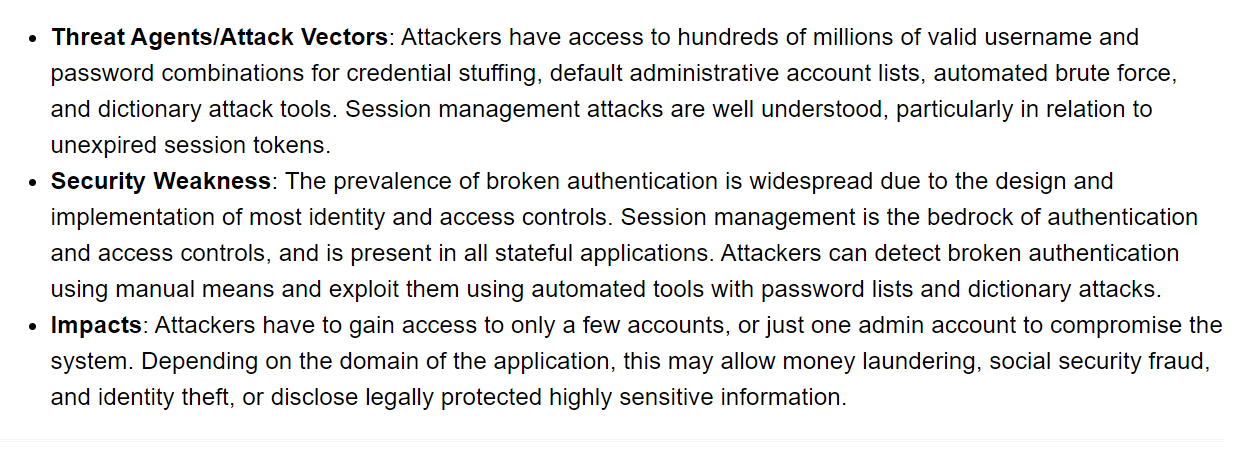
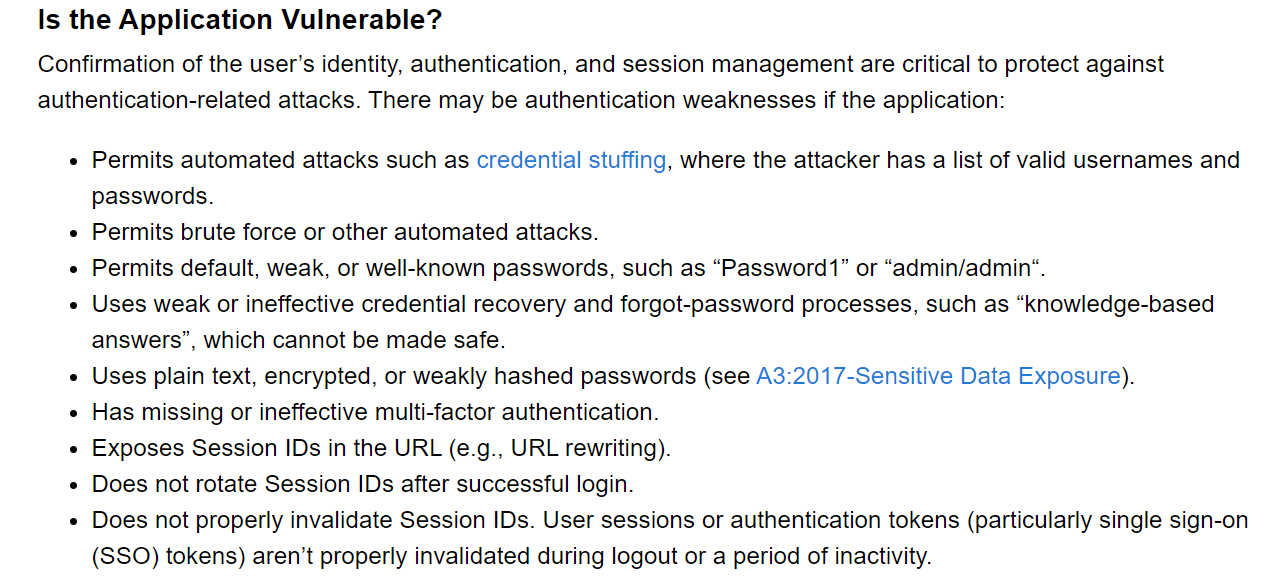
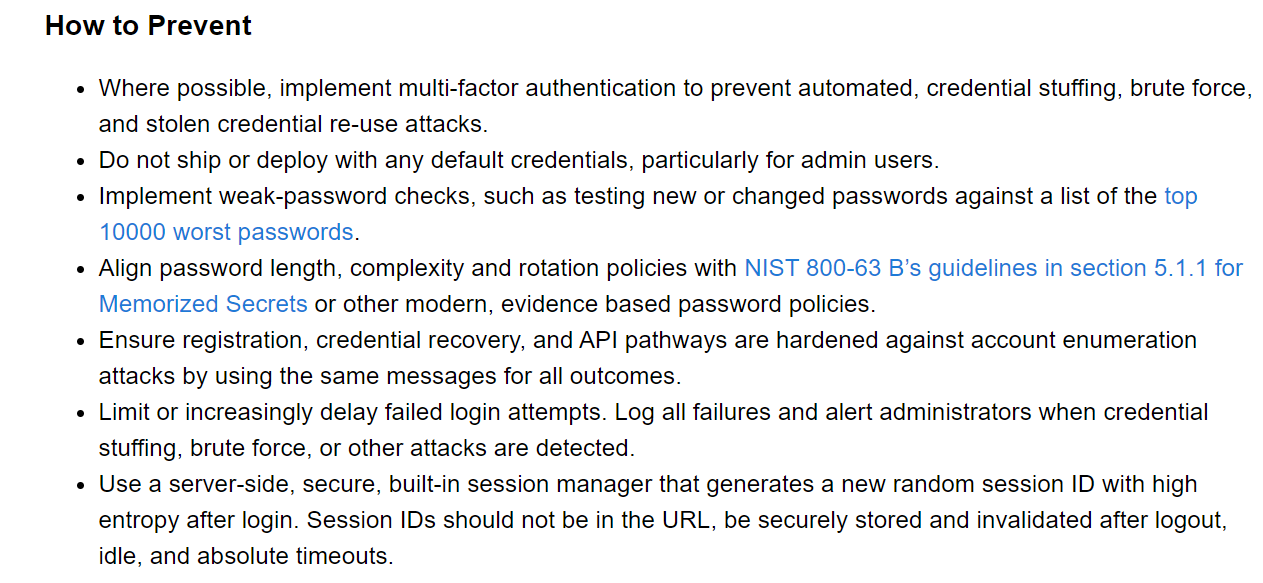
**A2 – Broken Authentication**









**Fishing:**

Ex. (Spearfishing)

Hackeren får adgang til din email.

Hackeren udgiver sig for at være dig og skriver til en i din tætte omgangskreds. Han skriver en hastemail om at du står i en nødsituation og skal bruge 10.000 kr, men du har ikke nok på din konto, hackeren spørger din ven om de 10.000 kr, og din ven overfører dem. Dette kan også en metode at franarre folks personlige oplysninger såsom CPR.

Ex (Fishing)

Hackeren sender en invitation ud til en grillfest til alle Kurts venner på facebook.

Kurts ven Wonnegut trykker på linket I meddelsen, Wonnegut downloader nu en ondsindet fil.

**Credential Stuffing:**

Hackere har lister med gyldige brugernavn – Password kombinationer (Par) som via software bliver automatisk injected på alverdens hjemmesider.

**Hvordan forhindrer man et ”Brute Force Attack”:**

* Stærke passwords (feks min 12 char med 3 forkellige tegn og min et tal) (Good Luck Hacker).
* Lukke Account/Brugeren der bliver angrebet efter x antal forkerte log in forsøg.
* Monitor Serverlogs (Alarm til server admin efter x antal forkerte log in).
* Two factor authentication(Something you have, something you know).
* Captcha(feks marker alle billeder med lyskryds).

**Account enumeration:**

Hjemmesiden man prøver at logge ind på sender et response tilbage med en meddelelse om at dit password er forkert men brugernavnet er rigtigt (den siger forkert password). Dette hjælper hackeren idet han kan gætte indtil brugernavnet er rigtigt og så koncentrere sig om password i stedet for. I stedet skal hjemmesiden sige ingenting.