**A2 Broken Authentication & Session Management**

* **Leicht verwundbar, wenn**
  + die Anmeldedaten beim Speichern unzureichend geschützt/verschlüsselt sind.
  + die Anmeldedaten durch schwache Kontoverwaltungsfunktionen (Kontoerstellung, Kennwortänderung, etc.) leicht zu erraten oder zu überschreiben sind.
  + die Session ID aus der URL auslesbar ist.
  + Session IDs keine Zeitüberschreitung besitzen oder Benutzersitzungen nicht ungültig werden während der Abmeldung.
  + Passwörter und Session IDs über unverschlüsselte Verbindungen gesendet werden.
* **Beispiel Attacken:**
  + Bei unverschlüsselten Verbindungen kann jeder den Datentransfer beobachten und die Anmeldedaten abfangen z.B. durch Man in The Middle.
  + Person nutzt öffentlichen Computer und vergisst sich mit seinem Account abzumelden. Ohne eine Zeitüberschreitung der Session ID kann der nächste Nutzer durch einfaches Betreten der zuletzt besuchten Seiten Zugriff auf den Account beschaffen.
* **Wie es verhindert werden kann:**
  + Nur starke Passwörter erlauben
  + Anmeldedaten sollten neben einer starken Verschlüsselung zusätzlich gehasht werden
  + Session IDs sollten eine Zeitüberschreitung besitzen
  + Sensible Daten sollten im Body Part einer POST Anfrage gesendet werden