Allgemein

- Foliennummer 16;
- Confidentiality (Vertraulichkeit),Integrity (Integrität),Availability (Verfügbarkeit)
- Komplexität von SOAP/REST-Webservice lässt sich anhand von WSDL/WADL Files erkennen.
- Wenn in ein bestehendes XML-File externer XML-Code/file eingeschleust werden kann, nennt man das XXE(XML external Entity Injection.
- Billion laughs Attake ist ein DDos Angriff mit vielen LOL ´s die an einen Parser geschickt werden.
- Bei Clickjacking wird eine Webseite so präperiert, das der Nutzer nicht sieht worauf er tatsächlich klickt. (Bsp.: 2 Frames übereinander, man klickt auf email senden, es wird aber code ausgeführt der eine Zahlung veranlasst.)
- SQL-Injection (UNION, Mächtigkeit der SELECTs) –'; ((–) OR # in MYSQL)
- Bool'sche Muster
- http-only und secure flag in Session-Id Cookie setzen!
- neue Session-ID bei login (Zustandsänderung = Änderung in der Session ID)
- indexing auf Sererseite Abschalten
- Alogrithmus zum ver/entschlüsseln muss auch in Hardware langsam sein (FPGA´s)

OWASP Top 10

A1 Injection

Hier geht es um einschleusen von Code über Eingabefelder. Meist wird ein zusätzliches Kommando dazu genutzt, um Daten vom Server zu lesen, schreiben oder zu verändern ohne das dies von der Anwendung kontrolliert wird. Unterarten von Injection

- SQL
- XML
- shell

A2 Fehler in Authentifizierungs und Session-Management

- Session-Management und ID sind falsch implementiert,
- Session hijacking,
- Session klau,
- ID berechenbar,
- Passwörter nicht gehasht,
- SessionID läuft nicht ab,
- keine Transportverschlüsselung

A3 Cross-Site Scripting

Die vom User in den Browser eingegebenen Daten werde nicht validiert bzw. die Daten die an den Server Server geschickt werden. Hier hilft meist escapen und testen der Anwendung (manuelle pentest, reviews usw.)

A4 Unsichere direkte Objektreferenzen

- ID 1 im Browser = ID 1 in der DB => erratbar
- Zugriff muss auch auf Ressourcen Ebene vom Server überprüft werden (id 1 darf nur daten von id 1 sehen)

A5 Sicherheitsrelevante Fehlkonfiguration

- veraltete Softwarekomponenten
- nicht benötigte Komponenten aktiv oder installiert
- Standardkonten mit initial PW´s aktiv
- Fehlermeldungen, Stack Traces geben zuviel Informationen über das System raus
- Framework Einstellung sind nicht sicher,

A6 Verlust der Vertraulichkeit sensibler Daten

- Daten werden in Klartext gespeichert
- Daten in Klartext übertragen
- schwache/alte Krypto Verfahren
- schwache Schlüssel oder falsches Verwalten der Schlüssel
- Sicherheitsdirektiven und Header werden nicht genutzt

A7 Fehlerhafte Autorisierung auf Anwendungsebene

- Links zu Funktionen werden angezeigt obwohl die Rechte dazu fehlen
- serverseitige Prüfung von Authentisierung und Autorisierung wird nicht durchgeführt
- serverseitige Prüfung nur mit Daten vom Anwender

A8 Cross-Site Request Forgery

- geheimer Token bei jeder Anfrage/Link/Formular wird nicht mitgeschickt
- Dem User wird meistens ein Request untergeschoben womit ohne Benutzereingabe was gemacht wird

A9 Nutzung von Komponenten mit bekannten Schwachstellen

Ein oder mehrere kleine Lücken (auch hintereinander in unterschiedlichen Programmen) können ausgenutzt werden um an die Server/Daten zu kommen

A 10 Ungeprüfte Um- und Weiterleitungen

- Umleiten sollte vermieden werden
- Benutzer kann auf Angreiferwebseite weiter geleitet werden (Phising)
- Benutzer informieren wenn er umgeleitet wird