Homework 2025:

1) OpenSSL:
   Generare chiavi simmetriche e usarle con diversi algoritmi simmetrici
   Generare chiavi asimmetriche e usarle per crittare, firmare e firmare certificati
   Generare certificati secondo lo standard x.509 v3
   Conservare la chiave privata in p12 e in keytool (e in Vault successivamente)
2) Java Cryptography Architecture
   Stessi esercizi di openssl e gestione certificati
   Emettere certificati x.509 e una catena di certificati
   Firmare e verificare
   Estrarre campi da un certificato (nome, chiave, validità, key usage,....)
3) Configurazione Apache/Tomcat con https
   Generare certificati per https
   Configurare in sicurezza apache (configurare ssl e, successivamente, seguire linee guida di configurazione sicura di un web server per eliminare le vulnerabilità note), analizzare, e possibilmente mitigare, le vulnerabilità della versione installata, guardando le vulnerabilità note su cataloghi open (MITRE, CWE, OWASP,….)
4) Configurazione di un meccanismo di Identity Management e Access Control
   Utilizzo Keycloack e openID per configurare una semplice applicazione web con un database, con un meccanismo di autenticazione OAUTH, un meccanismo di autorizzazione basato su policy e attributi/ruoli, sicurezza delle comunicazioni tra i vari componenti architetturali. Le tecnologie per l'implementazione dell'applicazione web based sono a vostra scelta (Container, Apache/Tomcat/ Java spring boot/ Flask,……). Per l'architettura scelta vanno inoltre documentate:
   - analisi delle minacce degli asset scelti
   - analisi delle contromisure secondo lo standard NIST (controlli e sotto-controlli da scegliere, dettaglio implementazione e configurazione per mitigare la minaccia specifica)
   - (opzionale) analisi dinamica con tool di penetration testing (tipo zap)

5) Protezione delle credenziali dei vari asset con un meccanismo di credential management (Vault) per arricchire l'esercitazione del punto (4)

Per gruppi di 3 persone sono previsti componenti di sicurezza aggiuntivi, contattare la docente del corso.

Homework 2024:

1) OpenSSL
2) Java Cryptography Architecture: creare certificati e chiavi, provarli con algoritmi simmetrici ed asimmetrici, firmare digitalmente e verificare la firma, estrarre campi dal certificato.
3) Configurazione Apache/Tomcat/Flask con https
4) Protezioni di credenziali private con Vault (studiare funzionalità e architettura di sicurezza di vault)
5) Semplice Webapp protetta con XACML + LDAP (per XACML: a) ci sono sicuramente librerie disponibili con SpringBoot, da verificare per altri AS, per Flask, verificare VAKT)
6) Semplice Webapp protetta con KeyCloack e OpenID
7) Modellazione dei Threat di una WebApp (integrando HomeWorks 3,4 e 5 oppure 3,4 e 6) com Microsft Threat Modelling Tool (before and after the application of security controls) con discussione di possibili mitigazioni e miglioramenti a valle dei risultati.
8) Assessment delle applicazioni e dei controlli di cui al punto 7 con il NIST 800-53, vedere foglio excel (**in alternativa** potete usare l'excel ed il framework nazionale italiano).