5.8.1 Gestione di password, chiavi e certificati

Le password mantenute dall'applicazione o le chiavi private dei certificati devono essere conservate in forma cifrata. Le informazioni sulle password e le chiavi devono risiedere in container (aree del filesystem, tabelle del database, ecc.) differenti rispetto ai dati dell'applicazione.

5.8.2 Trasmissione delle password in rete

Utilizzare protocolli crittografici, come TLS (Transport Layer Security) o SSH (Secure Socket Shell), che impiegano algoritmi standard di derivazione delle chiavi basata su password (Password-based Key Derivation/key stretching) detti anche algoritmi di slow hashing, come PBKDF2, scrypt o bcrypt, i quali, rallentando di molto la funzione di hashing, rendono inefficaci eventuali attacchi di forza bruta per il password cracking.
Prevedere, inoltre, l'aggiunta di una chiave segreta alla hash, in modo tale da consentire la convalida della password solo a coloro che la conoscono. Ciò si può fare cifrando l'hash con algoritmo AES oppure includendo la chiave segreta nell'hash utilizzando poi un algoritmo di hashing come HMAC.
È sconsigliato l'utilizzo di funzioni di hash crittografico veloce come MD5, SHA-1, SHA-256, SHA-512, RipeMD, WHIRLPOOL, SHA-3.

5.8.3 Generazione/conservazione delle password nel filesystem/DB

Le password memorizzate nel filesystem o nel DB sotto forma di hash (esempio MD5/SHA-1 etc.), devono prevedere l'introduzione di un ulteriore fattore randomico (salt) durante la loro generazione.

5.8.4 Batch Job dell'applicazione

Le informazioni, i dati o gli allegati trasmessi tramite i batch job dell'applicazione (ad esempio sessioni ftp o altri protocolli di rete non cifrati o proprietari), devono utilizzare canali di comunicazione sicuri come SSL o TLS, in cui le chiavi di cifratura simmetriche vengono scambiate all'interno di una comunicazione protetta attraverso algoritmo crittografico asimmetrico (Ad esempio RSA con dimensione delle chiavi uguale o superiore a 1024 bit).

5.8.5 Storage dei dati applicativi

I dati dell'applicazione memorizzati nel database o nel filesystem devono essere cifrati tramite algoritmi simmetrici con chiave pari almeno a 192 bit (inclusi i bit di parità).

5.8.6 Integrità delle informazioni

Tutti i dati di natura critica conservati e mantenuti dall'applicazione, oltre che cifrati, devono prevedere l'utilizzo di algoritmi di hashing o firma digitale per poterne vagliare l'integrità/autenticità.

5.8.7 Meccanismi di autenticazione

L'applicazione sviluppata non deve impiegare meccanismi di autenticazione con chiave condivisa (altrimenti detti pre-shared secret).

5.8.8 Non ripudio delle sessioni

Tutte le sessioni riconducibili all'applicazione, svolte dalle utenze operative/amministrative, devono essere, oltre che supportate da meccanismi di tracciamento idonei, anche cifrate con algoritmi crittografici. In questo modo si garantisce il non ripudio delle singole sessioni. Deve cioè essere possibile determinare con esattezza se un evento si è verificato o meno.

5.8.9 Schemi di sicurezza e crittografici

Gli schemi di sicurezza devono essere semplici e ben documentati. È vietata la predisposizione di schemi di autenticazione , crittografia e/o gestione delle chiavi non-standard, oppure fatta in proprio ("hand-made")..