

5.8.10 Weak Keys e Collision

Il processo di creazione/assegnazione delle chiavi di cifratura ai dati dell'applicazione, in base al cipher utilizzato, non deve generare weak keys (chiavi deboli) o, nel caso di algoritmi di hashing, alcuna collision (valori ripetuti).

5.8.11 URL cifrati

Le directory contenenti file o dati di natura personale, critici e sensibili, residenti nella document root del web server devono apparire cifrate nell'URL del client browser.

5.8.12 Normalizzazione dei dati cifrati

Nelle applicazioni web l'utilizzo della codifica *base64* è autorizzato solo per la normalizzazione dei dati, delle stringhe o degli URL cifrati.