La seguente tabella riporta le vulnerabilità della Top 10 OWASP 2017[21] riconducibili alle minacce di repudiation e per ciascuna vulnerabilità indicata, le relative pratiche[22] e requisiti[23] di sicurezza consigliati da OWASP:

OWASP TOP-10 2017 (Rischi di sicurezza delle applicazioni)	OWASP Proactive Controls 2018 v 3.0 (Pratiche di sicurezza proattive)	OWASP ASVS 3.0 (Requisiti di sicurezza applicative)
A10 – Insufficient Logging & Monitoring	C9 - Implement Security Logging and Monitoring	V8 - Error Handling and Logging

Tabella 14 - Rischi di sicurezza OWASP relativi alla Repudiation

Alcuni esempi di minacce di repudiation:

- Potenziali debolezze nella protezione dei dati di audit: E' buona norma considerare cosa accade quando il meccanismo di audit viene attaccato, compresi eventuali tentativi di distruggere i log o i programmi di analisi dei log a supporto del processo di indagine sugli attacchi. E' opportuno assicurarsi costantemente che l'accesso al log sia strettamente monitorato e che esiste e venga utilizzato un meccanismo efficace capace di controllare la lettura e la scrittura separata su log.
- Auditing insufficiente: Il log deve raccoglie dati sufficienti per comprendere cosa è accaduto in passato. Questo deve acquisire dati sufficienti per essere in grado successivamente di riconoscere un possibile incidente di sicurezza. Tale acquisizione deve essere sufficientemente contenuta da poter essere lasciata sempre attiva. Si deve sempre disporre di dati sufficienti per gestire eventuali richieste di ripudio. Dunque è importante assicurarsi di loggare i dati sufficienti e appropriati per gestire eventuali controversie. Assicurarsi inoltre di tenere sempre in considerazione gli aspetti relativi alla privacy dei dati durante la verifica dei log.
- Dati di log provenienti da una fonte sconosciuta o da soggetti poco affidabili: Trattasi di dati di log provenienti da utenti o sistemi sconosciuti o debolmente autenticati. Un'altra entità presente al di fuori del più esterno confine di fiducia è stato autorizzato a scrivere su log. Di norma è buona pratica identificare e autenticare la fonte dei log prima che questi vengano accettati e consentire l'accesso al log solo da codice fidato.

5.5.4.1.1.4 Indirizzamento dell'information disclosure

La Tabella seguente mostra in elenco gli obiettivi dell'information disclosure, le strategie di mitigazione per indirizzare l'information disclosure e le tecniche per attuare tali mitigazioni:

OBIETTIVO DELLA MINACCIA	STRATEGIA DI MITIGAZIONE	TECNICA DI MITIGAZIONE
Monitoraggio della rete	Crittografia	• HTTPS/SSL; • IPsec.
Directory o nomi di file (per esempio "lettere-di-licenziamento/" o "NomeCognome.docx")	Sfruttare le funzionalità messe a disposizione dal Sistema Operativo	ACLs.
Contenuti di un file	Sfruttare le funzionalità messe a disposizione dal Sistema Operativo	ACLs.

21 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project

22 https://www.owasp.org/index.php/OWASP_Proactive_Controls

23 https://github.com/OWASP/ASVS