programma per sottomettere la propria richiesta HTTP o può utilizzare un proxy liberamente disponibile che gli consente di modificare facilmente qualsiasi dato inviato dall'applicazione web.

5.5.4.1.1.3 Indirizzamento della repudiation

Indirizzare la repudiation in genere significa garantire che il sistema venga progettato prevedendo il tracciamento e la registrazione delle operazioni svolte (logging), garantendo inoltre che, tali registrazioni vengano protette e preservate. Alcuni di questi registri possono essere gestiti utilizzando un trasporto affidabile specifico. In questo senso, il syslog su UDP presenta forti lacune in termini di sicurezza; il syslog su TCP / SSL invece è notevolmente migliore.
La Tabella seguente mostra in elenco gli obiettivi di repudiation, le strategie di mitigazione per indirizzare la repudiation e le tecniche per attuare tali mitigazioni:

OBIETTIVO DELLA MINACCIA	STRATEGIA DI MITIGAZIONE	TECNICA DI MITIGAZIONE
Non utilizzare un meccanismo di log vuol dire non poter provare nulla.	Log	Assicurarsi di tracciare tutte le informazioni rilevanti dal punto di vista della sicurezza.
Esposizione dei Logs a eventuali attacchi	Proteggere i logs	• syslog su TCP/SSL; • ACL.
Il Log come canale di attacco	Informazioni dettagliate sul log	Documentare la progettazione del log sin dall'inizio del processo di sviluppo.

Tabella 13 - STRIDE: Indirizzamento della repudiation

Non avere un log significa non poter provare nulla. Prevedere e mantenere i log, significa, poter investigare su quanto accaduto, al fine di acquisire un valido riscontro, nel momento in cui qualcuno nega di aver ottenuto o fatto qualcosa.
Esposizione del log a possibili attacchi. Eventuali aggressori faranno del tutto per invalidare le informazioni contenute nel log, contrastando a volte l'operazione stessa di scrittura o forzando il "roll over" del log, con il fine di rendere difficile l'individuazione dell'attacco. Questi inoltre, possono agire in modo tale da disattivare gli allarmi, facendo sì che, il vero attacco non venga alla luce.
Il log come canale di attacco. Da progettazione, è possibile che vengono raccolti dati provenienti da sorgenti 'malevoli' fuori dal nostro controllo, fornendo poi gli stessi dati a persone o sistemi che hanno dei privilegi di sicurezza. Un esempio di questa tipologia di attacco potrebbe essere l'invio di una e-mail indirizzata a "</html> destinatario@dominio.com", che causa problemi a quegli strumenti web-based che non prevedono l'HTML inline.
È possibile rendere il tutto più semplice scrivendo codice sicuro nell'elaborazione dei dati di log, dando chiara evidenza di ciò che questi non possono contenere, ad esempio "I dati di log sono tutti in chiaro, ed eventuali aggressori potrebbero inserire ciò che vogliono" oppure "I campi da 1 a 5 del tracciato del log sono sotto stretto controllo da parte del nostro software, mentre i campi da 6 a 9 sono facilmente iniettabili. Il campo 1 è un campo time GMT. I campi 2 e 3 sono indirizzi IP (v4 o v6) ... ".