A6 - Security Misconfiguration	C10 - Handle All Errors and Exceptions	V19 - Configuration
A9 - Using Components with Known Vulnerabilities	C3 - Secure Database Access	V13 - Malicious Controls

Tabella 18 - Rischi di sicurezza OWASP relativi al Denial Of Service

Alcuni esempi di minacce di denial of service:

- Ping of Death: Il comando ping viene solitamente utilizzato per verificare la disponibilità di una risorsa di rete. Il principio di funzionamento si basa sull'invio di piccoli pacchetti di dati alla risorsa di rete target. Il ping of death sfrutta tale principio e invia pacchetti di dati superando il limite massimo (65.536 byte) consentito dal TCP/IP. La frammentazione TCP/IP esegue una scomposizione in blocchi più piccoli che vengono poi inviati al server. A causa di questa tipologia di attacco, poiché i pacchetti di dati inviati sono più grandi di quelli che il server può gestire, il server può bloccarsi, riavviarsi o può andare in crash.
- Smurf: Questo tipo di attacco utilizza grandi quantità di traffico di tipo Internet Control Message Protocol (ICMP) nei confronti di un indirizzo Internet Broadcast. L'indirizzo IP di richiesta viene contraffatto con l'indirizzo IP della vittima. Ne consegue che tutte le risposte vengono inviate alla vittima piuttosto che all'IP utilizzato in origine dal ping. Poiché un singolo indirizzo Internet Broadcast Address può supportare un massimo di 255 host, un attacco smurf amplifica di 255 volte un singolo ping. L'effetto risultante è quello di rallentare la rete a un punto tale da rendere la rete stessa inutilizzabile.
- Buffer overflow: Un buffer è una area di memoria temporanea presente nella RAM che viene utilizzata per contenere dati che possono essere elaborati dalla CPU prima che questi vengano scritti su disco. I buffer hanno un limite di dimensione. Questo tipo di attacco sovraccarica il buffer con un numero di dati maggiore di quanto ne può contenere. In tal modo il buffer si riempie oltre il limite corrompendo i dati presenti in memoria e determinando conseguentemente un instabilità nel sistema.
- Teardrop: Questo tipo di attacco utilizza pacchetti di dati di grandi dimensioni. Il TCP/IP li scompone in frammenti che vengono poi assemblati sull'host ricevente. L'attaccante manipola questi pacchetti man mano che vengono inviati in modo tale da sovrapporli. Ciò può causare l'arresto anomalo dell'host vittima durante la fase di riassemblamento.
- Syn attack: SYN è una forma abbreviata di Synchronize. Questo tipo di attacco sfrutta le tre modalità di handshake (negoziazione iniziale) per stabilire una comunicazione TCP. L'attacco SYN funziona inondando la vittima con messaggi SYN incompleti. Ciò fa sì che l'host vittima assegni risorse di memoria che normalmente non vengono mai utilizzate negando conseguentemente l'accesso agli utenti legittimi per mancanza delle necessarie risorse.

5.5.4.1.1.6 Indirizzamento dell'elevation of privilege

La Tabella seguente mostra in elenco gli obiettivi dell'Elevation Of Privilege, le strategie di mitigazione per indirizzare l'Elevation Of Privilege e le tecniche per attuare tali mitigazioni.

OBIETTIVO DELLA MINACCIA	STRATEGIA DI MITIGAZIONE	TECNICA DI MITIGAZIONE
Confusione tra dati/codice	Adottare strumenti e architetture che inducono a separare i dati dal codice.	• Prepared Statement o Stored procedure per l'SQL; • Separatori chiari con forme canoniche; • Validare i dati prima di passarli al consumer.
Attacchi di compromissione del	Utilizzare un linguaggio di programmazione sicuro	L'utilizzo di un linguaggio di programmazione sicura nella stesura