	sia intuitivo (ad es., solo digitando l'url corretto). Mascherare il percorso dei file documentali memorizzati nelle applicazioni web (ad esempio, con la conversione in hash dei nomi dei file o la visualizzazione del percorso con sequenze di lettere e numeri) provvedendo ad inserirli all'interno di specifici repository, utilizzando percorsi di tipo semantico complessi non facilmente riproducibili nell'url.

Convalida dell'input	
Minaccia	Negazione dei servizi.
Contromisure	- Validare l'input proveniente dal browser web attraverso l'uso di white list. - Valutare accuratamente tutti i dati di input sul server. - Gestire le eccezioni nel codice dell'applicazione.

Personalizzazione dei messaggi di errore del web server	
Minaccia	Divulgazione di informazioni riservate (Attacchi che rivelano dettagli implementativi).
Contromisure	Gestire le eccezioni nel codice dell'applicazione. Codificare e registrare le eccezioni che possono essere propagate all'esterno dell'applicazione. In caso di eccezione, restituire al client messaggi di errore generici (ad es., 404 Not Found, 408 Request Timeout) e/o codificati che non rivelino dettagli interni del sistema.

Password in memoria RAM	
Minaccia	Divulgazione di informazioni riservate (Memory dump attack).
Contromisure	Il Web Server deve utilizzare le password hash invece di memorizzare il testo delle password in chiaro. Il Web Server può utilizzare la Tokenizzazione in modo che solo i dati rappresentativi saranno in memoria mentre i dati sensibili vengono memorizzati altrove; I Web Server basati su .NET e su Java possono utilizzare il tipo SecureString/GuardedString per limitare il tempo in cui le password non crittografate sono disponibili in memoria.

5.6 Sicurezza dei DBMS/Database Server

5.6.1 Architettura

Isolamento dei sistemi critici	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	I sistemi critici come i DBMS devono avere un ambiente di elaborazione dedicato, strettamente controllato e monitorato. Per tali sistemi vale quanto segue: - Devono essere posti su un sistema dedicato che ospita solo il DB (e non ad es. un Web Server, un Application Server, un Directory Server e o altri servizi importanti). - Devono essere posti su un "layer dati" (segmento) di rete diverso da quello dei sistemi di front-end e da quello delle postazioni di lavoro client. - I diversi layer di rete devono essere posti su interfacce diverse di un firewall - Il firewall deve consentire unicamente le comunicazioni strettamente necessarie da e per i DB rispetto agli altri sistemi (Web Server, Application Server, client interni). - Non deve essere consentita dai firewall nessuna connessione diretta da internet o