	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

	altre reti esterne all'organizzazione, verso il layer dati che ospita i DBMS.

Firewall per il server di database	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	I sistemi critici come i DBMS devono essere protetti da firewall opportunamente configurati. Per tali sistemi vale quanto segue: - Il server del database deve essere posizionato dietro un firewall le cui regole predefinite sono impostate per negare tutto il traffico. - Il firewall del server del database deve essere aperto solo a specifiche applicazioni o server web, e le regole del firewall non devono consentire l'accesso diretto da parte dei client. Se l'ambiente di sviluppo non può soddisfare tale requisito, in tal caso quei dati con particolari restrizioni non devono essere memorizzati nel server del database di sviluppo utilizzando in sostituzione dati falsi. La scelta di offuscare eventualmente i dati reali di produzione non sarebbe sufficiente, pertanto viene sconsigliata. - Adottare le opportune procedure di controllo riguardo le modifiche apportate alle regole dei firewall notificando le modifiche alle regole agli amministratori di sistema (SA) e agli amministratori di database (DBA). - Le regole Firewall per i server di database devono essere regolarmente manutenute e revisionate dai SA e dai DBA. Tali regole devono essere regolarmente riesaminate anche dall'Ufficio per la sicurezza delle informazioni. - Verificare regolarmente i criteri di hardening delle macchine e le regole dei firewall tramite scansioni di rete, o consentendo scansioni da parte dell'ufficio per la sicurezza delle informazioni attraverso il firewall.

Failover	
Minaccia	Negazione dei servizi.
Contromisure	Prevedere meccanismi di failover del sistema DB per i database più critici dal punto di vista della disponibilità del servizio. In tali casi, è necessario utilizzare architetture DBMS in cluster applicativi, scegliendo se possibile i sistemi di clustering nativi dello specifico prodotto piuttosto che soluzioni di terze parti. Quando un DBMS del cluster va in fault, un processo di controllo (watchdog) deve rilevare il problema, generare un alert verso i sistemi di monitoraggio e ripartire il carico di lavoro sui sistemi restanti, eventualmente attivando sistemi di riserva posti in configurazione "hot-standby". Il cluster deve essere in grado di salvaguardare l'integrità dei dati dal punto di vista delle transazioni, attraverso opportuni meccanismi di replica in grado di avere i dati sempre coerenti rispetto all'ultima operazione di "commit" eseguita.

Controllo del traffico dati	
Minaccia	- Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	Attivare, a livello perimetrale, un dispositivo di sicurezza intelligente di tipo IDS (Intrusion Detection System) o IPS (Intrusion Prevention System) per individuare (IDS) la presenza di codice malevolo e bloccare (IPS) le intrusioni.