contenuto e il significato. Gli attacchi di SQL injection possono leggere, modificare o eliminare informazioni riservate dal database e talvolta persino metterlo fuori uso o eseguire comandi arbitrari di sistema operativo.

Come difendersi

- In genere, la soluzione consiste nel fare affidamento su query parametriche, piuttosto che sulla concatenazione di stringhe. Questa tecnica fornisce un valido escaping dei caratteri pericolosi.
- Validare tutti gli input, indipendentemente dalla loro provenienza. La validazione dovrebbe essere basata su una white list: dovrebbero essere accettati solo i dati che adattano a una struttura specificata, scartando quelli che non rispettano la white list Occorre controllare il tipo del dato, la sua dimensione, l'intervallo di validità (range), il formato ed eventuali valori attesi (white list).
- Limitare l'accesso agli oggetti e alle funzionalità di database, in base al "Principle of Least Privilege" (non fornire agli utenti permessi più elevati di quelli strettamente necessari per svolgere il loro lavoro).

Esempio:
La query ottenuta dinamicamente tramite concatenazione di stringhe viene resa sicura effettuando un'encoding mirato del valore in input.

```
<%
        Function FixSQL(stringa)
         stringa = Replace(stringa, "'", "''")
         stringa = Replace(stringa, "%", "[%]")
         stringa = Replace(stringa, "[", "[[]")
         stringa = Replace(stringa, "]", "[]]")
         stringa = Replace(stringa, "_", "[_]")
         stringa = Replace(stringa, "#", "[#]")
         FixSQL = stringa
        End function

        SQL = "SELECT * FROM tabella WHERE ID = '" & FixSQL(Request("ID")) & "'"
%>
```

Per ulteriori informazioni si veda: http://cwe.mitre.org/data/definitions/89.html,
CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

7.8 ASP.NET

ASP.NET è un insieme di tecnologie di sviluppo di software per il web, commercializzate da Microsoft. Utilizzando queste tecnologie gli sviluppatori possono realizzare applicazioni Web e servizi Web (Web Service). Sebbene il nome ASP.NET derivi da ASP (Active Server Pages), la vecchia tecnologia per lo sviluppo web di Microsoft, esistono sostanziali differenze fra le due. Infatti ASP.NET si basa, come tutte le applicazioni della famiglia Microsoft .NET, sul CLR (Common Language Runtime).

Vengono di seguito analizzate le principali vulnerabilità e relative contromisure da adottare.

7.8.1 Cross-site scripting (XSS)

Come riconoscerla

Il Cross Site Scripting consiste nella possibilità che un attaccante possa inserire nella pagina dell'applicazione, quindi nel codice HTML, script che, una volta eseguiti, possano trarre in inganno i legittimi utenti, trafugare informazioni e predisporre nuovi attacchi.
Questa minaccia, enormemente diffusa, è dovuta allo scarso controllo dell'input da parte delle web application.