8.3.4 Web Server to SQL Database:

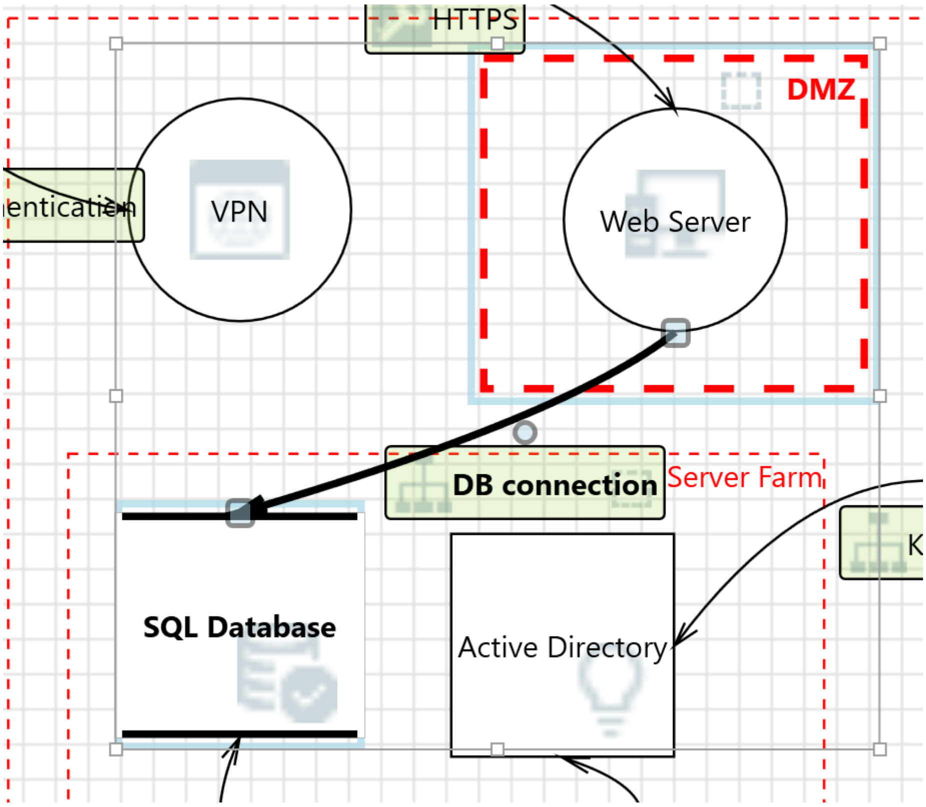

Figure 9: Web server to SQL Database

In Figure 9, Web server access to SQL DB is depicted. Listed below are potential threats and corresponding measures to mitigate them.

Spoofing the Web Server Process

Category:	Spoofing
Description:	Web Server may be spoofed by an attacker, and this may lead to unauthorised access to SQL Database. Consider using a standard authentication mechanism to identify the source process.
Mitigation:	User authentication will be done through Single Sign On (SSO) with MFA enabled for all external connections (Grassi et al., 2017).

Potential SQL Injection Vulnerability for SQL Database

Category:	Tampering
Description:	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any

	procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.
Mitigation:	Access to the Web Server will be protected with Web Application Firewall. A WAF can inspect the input data from user requests and apply strict validation rules. It checks for suspicious or malicious content, such as JavaScript code or HTML tags, and blocks or sanitises them to prevent SQL injection attacks.

The SQL Database Data Store Could Be Corrupted

Category:	Tampering
Description:	Data flowing across the DB connection may be tampered with by an attacker. This may lead to the corruption of SQL Database. Ensure the integrity of the data flow to the data store.
Mitigation:	Access to the Web Server will be protected with Web Application Firewall. A WAF can inspect the input data from user requests and apply strict validation rules. It checks for suspicious or malicious content, such as JavaScript code or HTML tags, and blocks or sanitises them to prevent code injection attacks.

Potential Excessive Resource Consumption for Web Server or SQL Database

Category:	Denial Of Service
Description:	Does Web Server or SQL Database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.
Mitigation:	Implementing rate-limiting mechanisms within the application code will prevent excessive requests from consuming resources. Additionally, validating and sanitising all incoming requests to prevent attacks that exploit vulnerabilities, such as buffer overflows or injection attacks.