



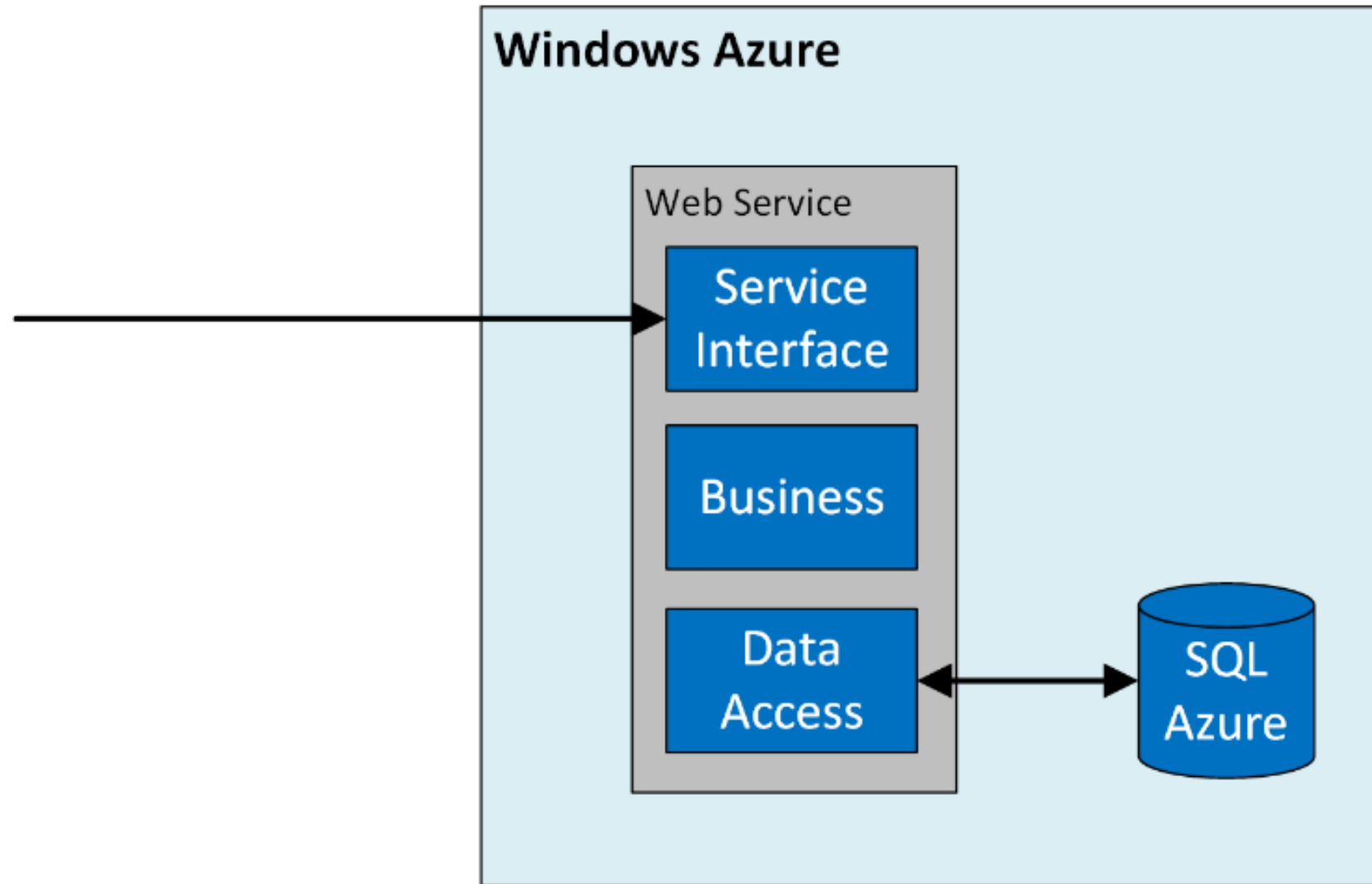
OWASP with .NET 5 and Angular

Robert Rozas navarro
Senior Customer Engineer
rorozasn@microsoft.com

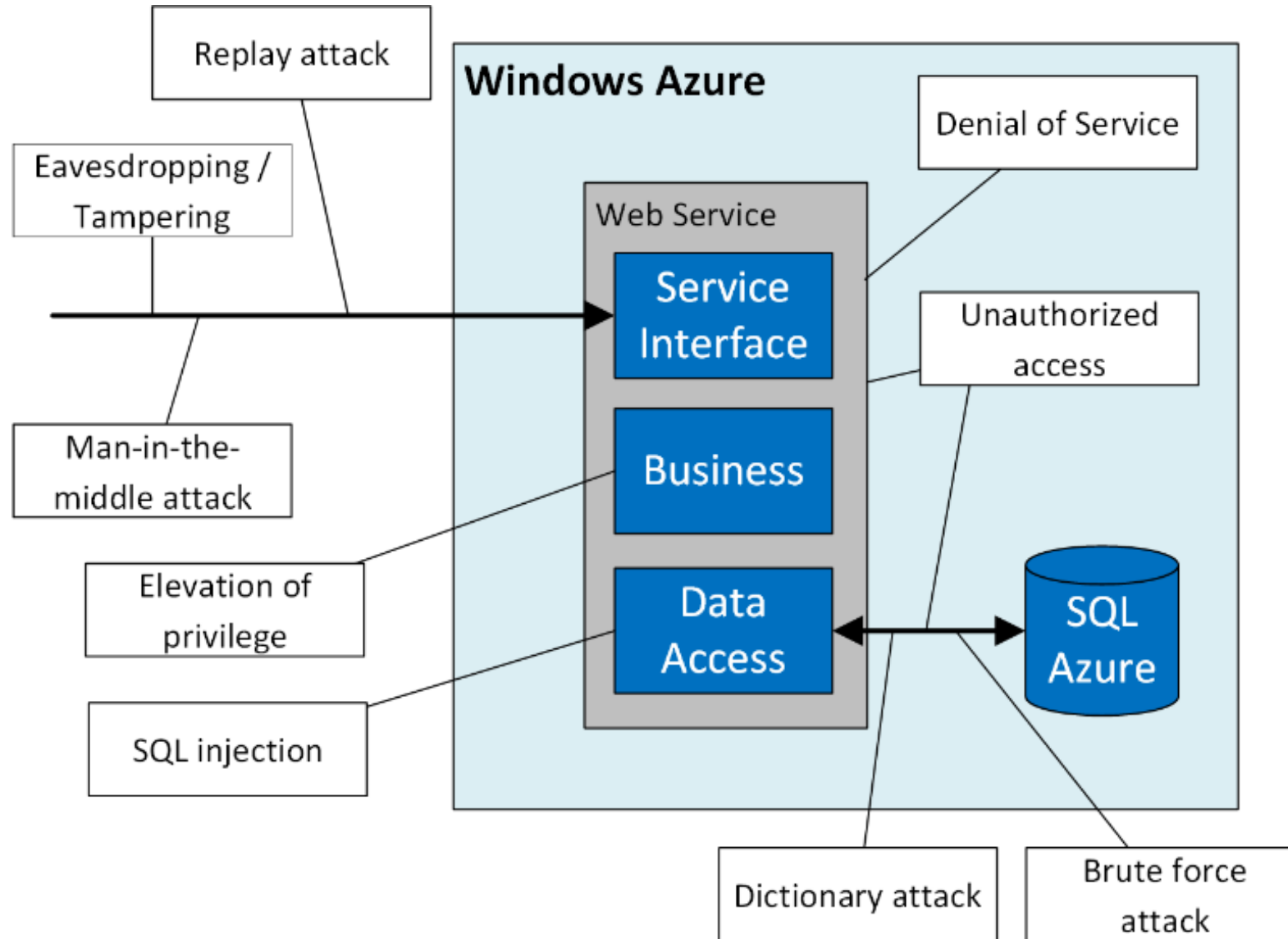
Agenda

1. Introduction
2. OWASP Top 10
3. .NET Demo

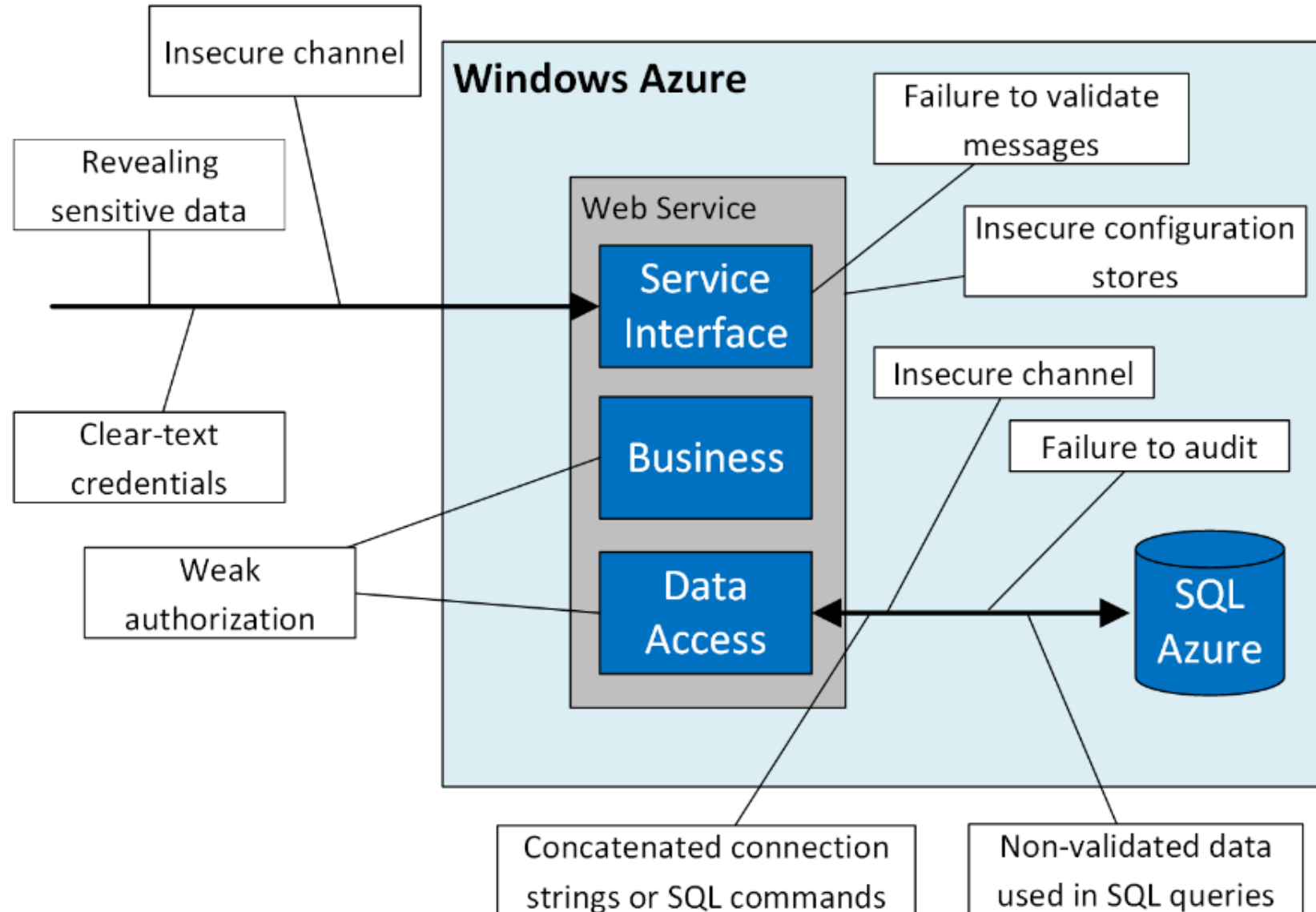
Scenario



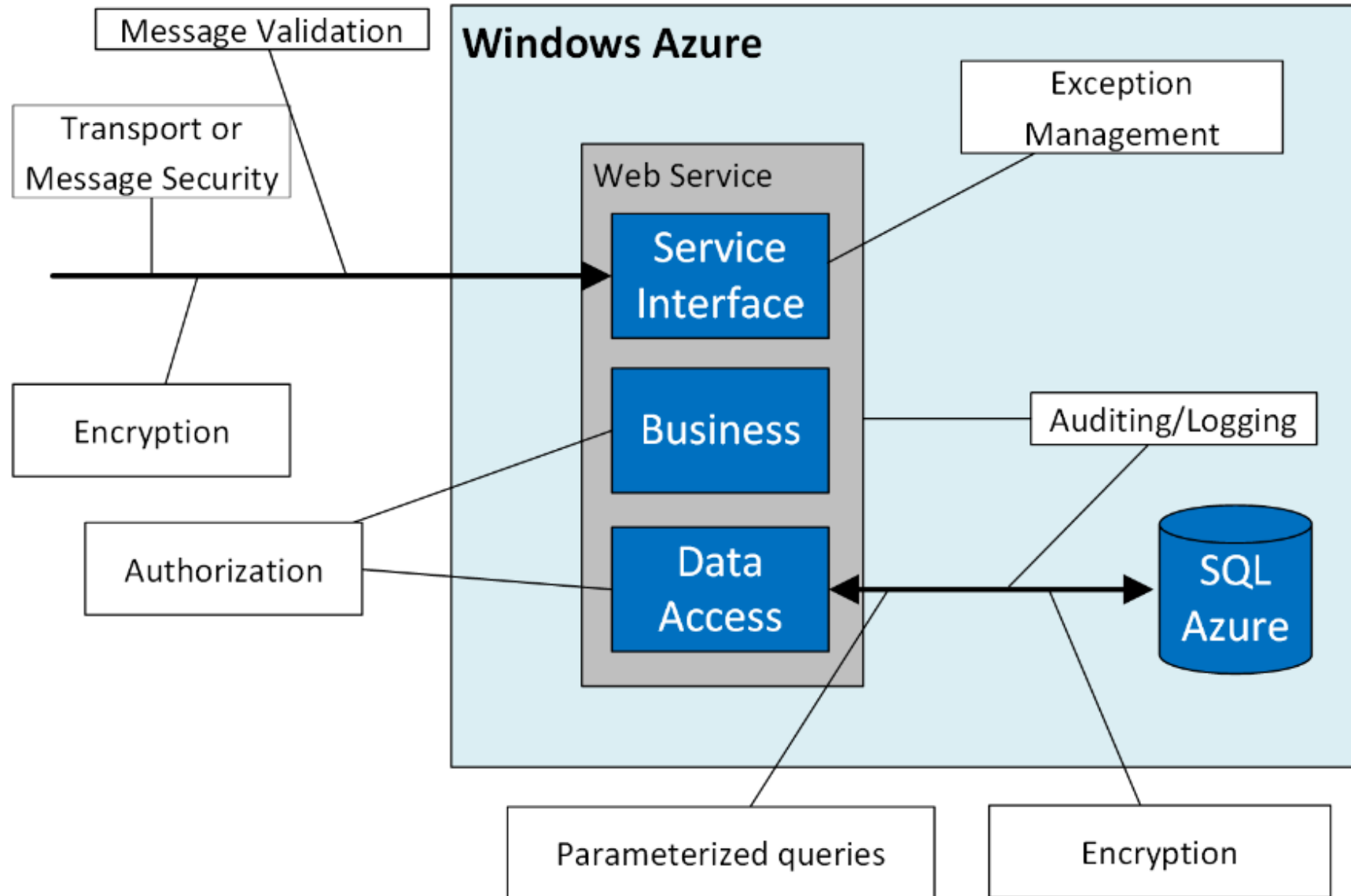
Threats / Attacks



Vulnerabilities



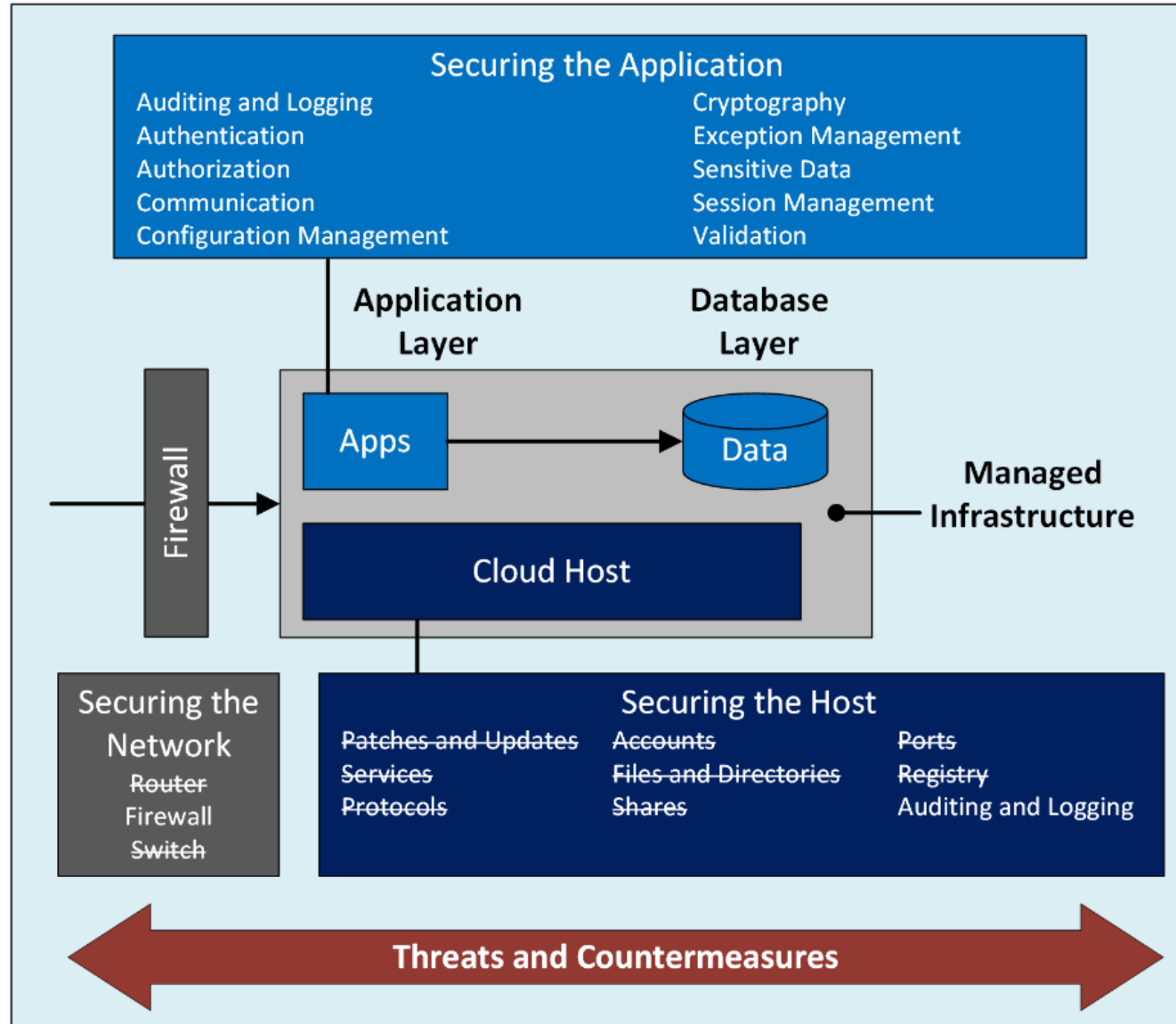
Countermeasures



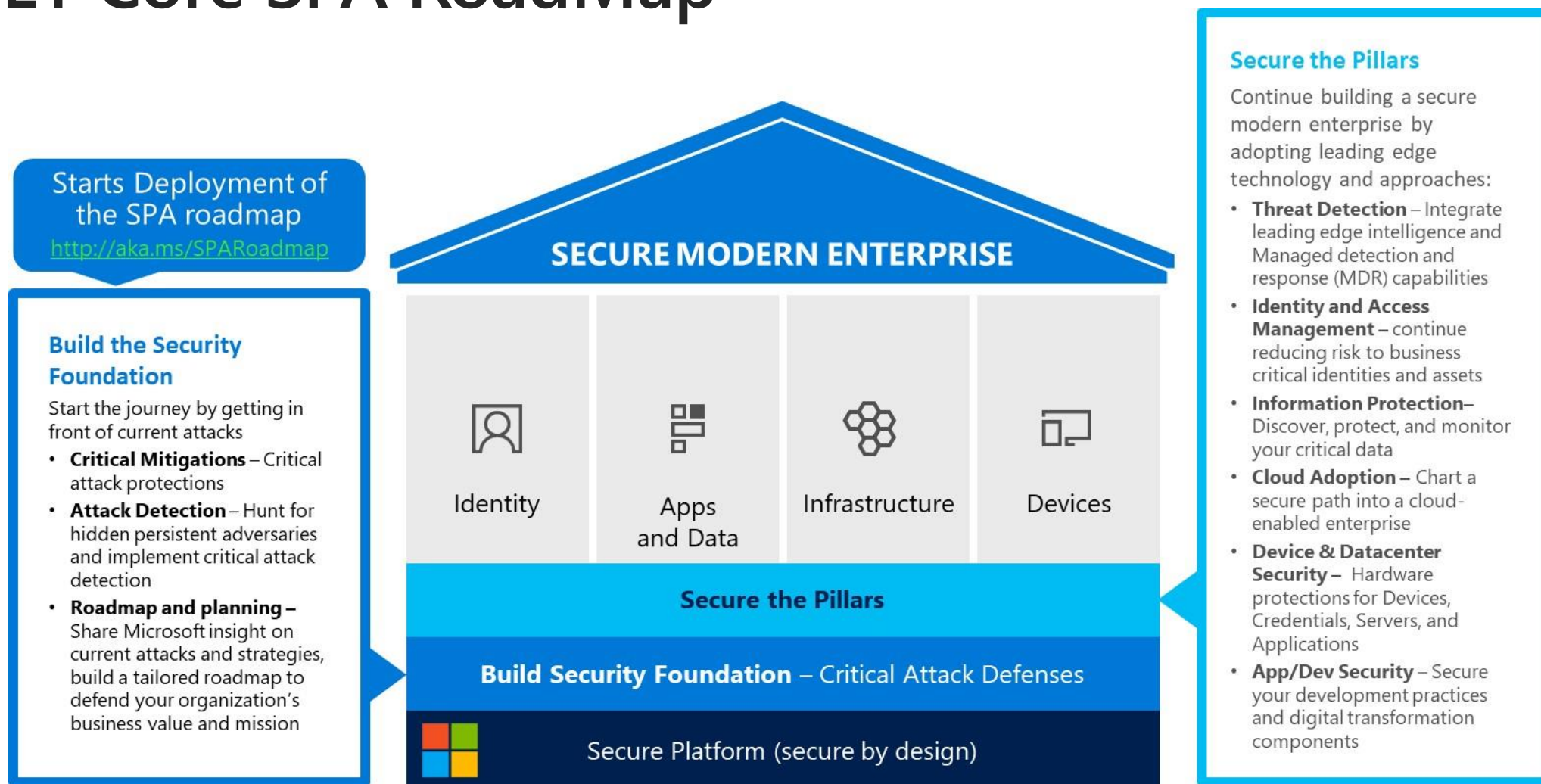
Security Frame

Category	Notes
Auditing and Logging	How security-related events are recorded, monitored, and audited.
Authentication	The process of proving identity, typically through credentials, such as a user name and password
Authorization	How your application provides access controls for roles, resources and operations.
Communication	How data is transmitted over the wire. Transport security versus message encryption is covered here.
Configuration Management	How your application handles configuration and administration of your applications from a security perspective.
Cryptography	How your application enforces confidentiality and integrity.
Exception Management	How you handle applications errors and exceptions.
Sensitive Data	How your application handles any data that must be protected either in memory, over the network, or in persistent stores
Session Management	A session refers to a series of related interactions between a user and your application.
Validation	How your application filters, scrubs, or rejects input before additional processing, or how it sanitizes output.

.NET Securing the Application



.NET Core SPA RoadMap



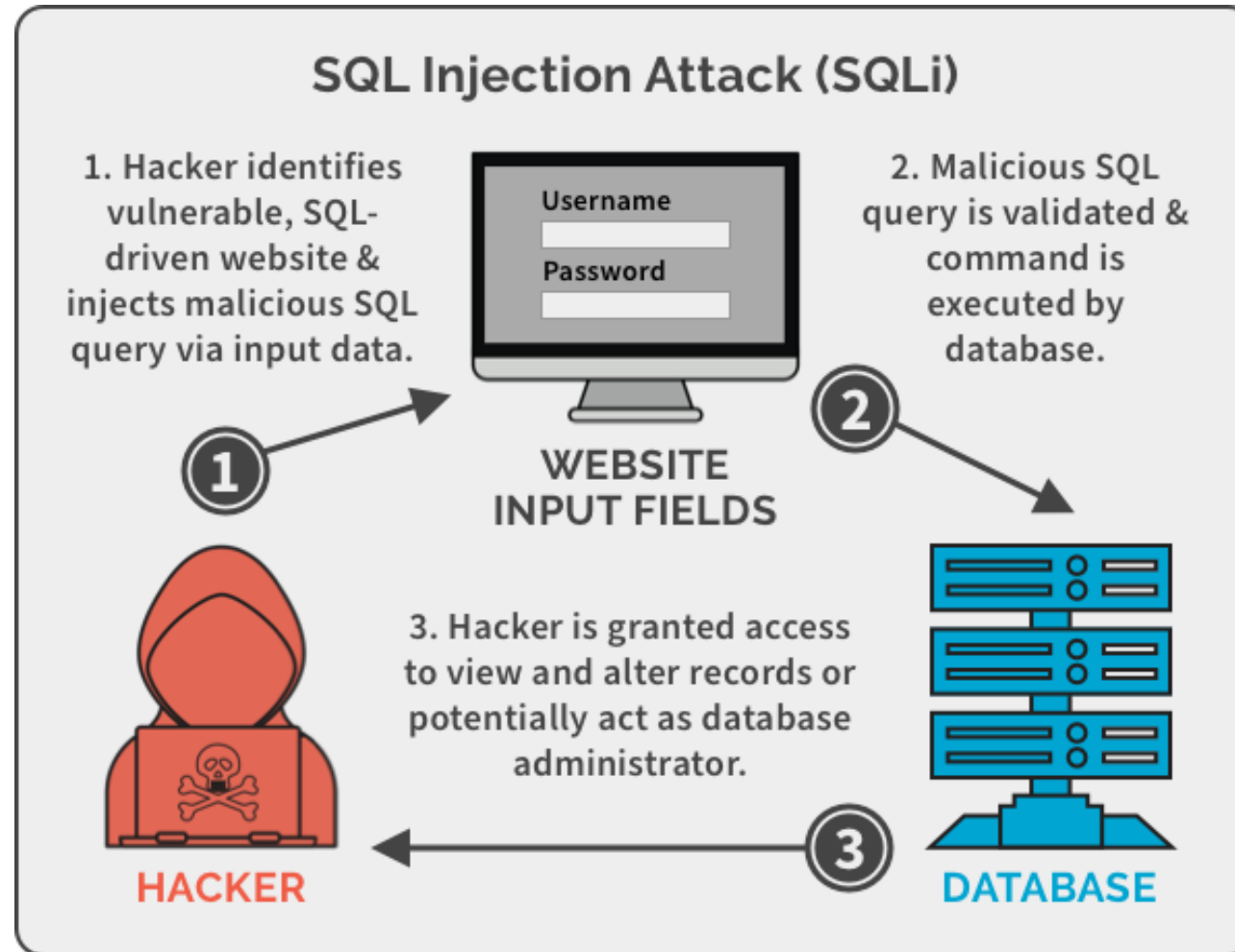
<https://aka.ms/SPARoadmap>

OWASP Top Ten

OWASP Top 10 – 2013	→	OWASP Top 10 – 2017
A1 – Injection	➔	A1:2017-Injection
A2 – Broken Authentication and Session Management	➔	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	➔	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	➔	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	➔	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	➔	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

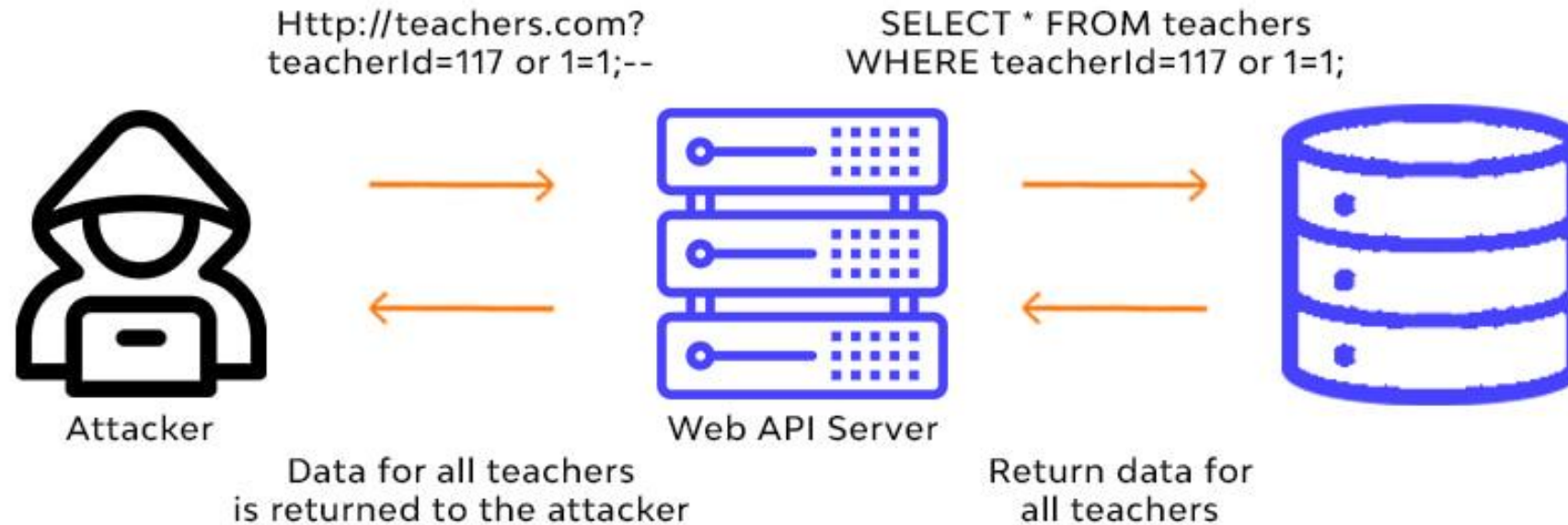
<https://owasp.org/www-project-top-ten/>

OWASP Top Ten

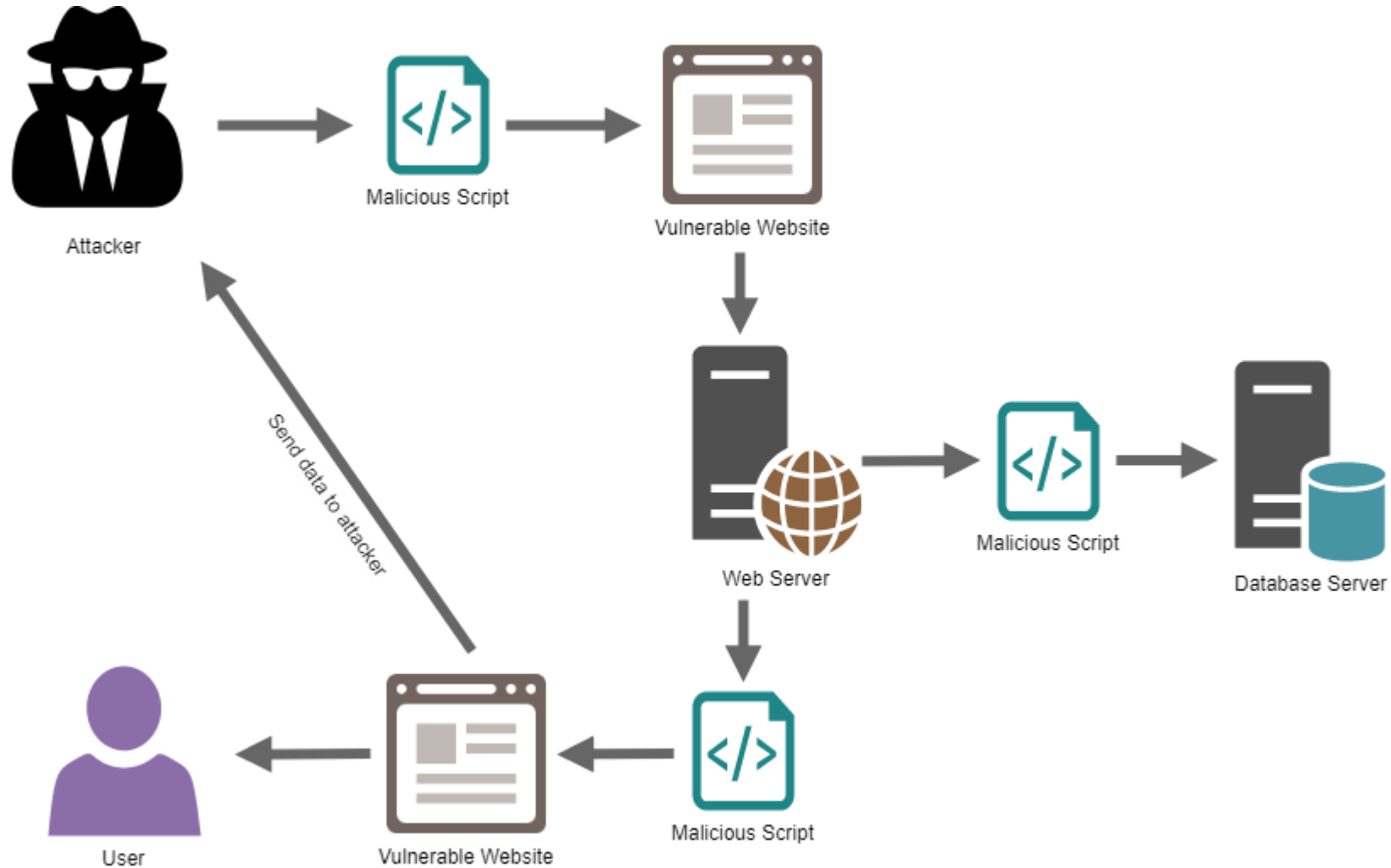


OWASP Top Ten

SQL Injection

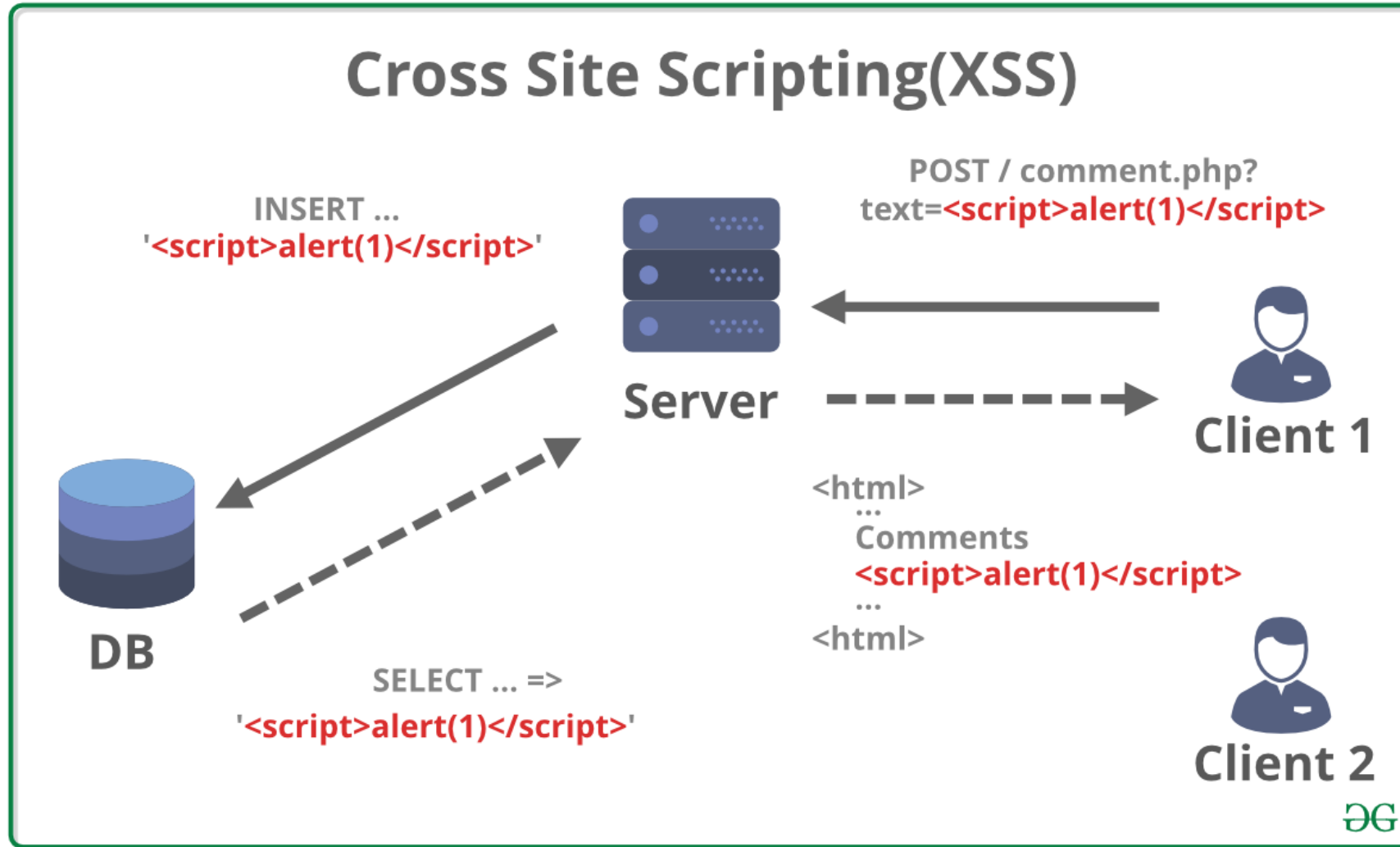


OWASP Top Ten



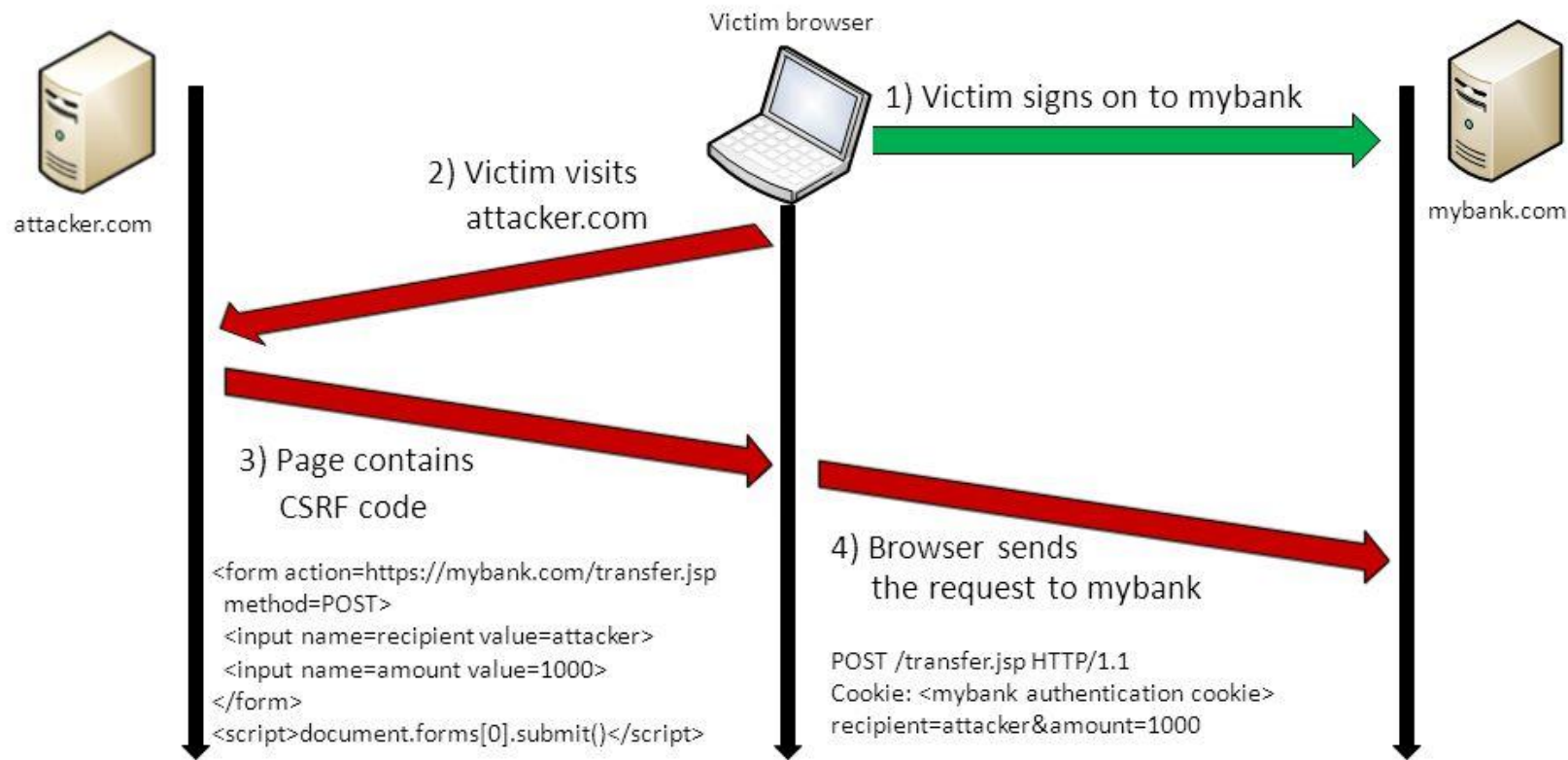
<https://owasp.org/www-project-top-ten/>

OWASP Top Ten

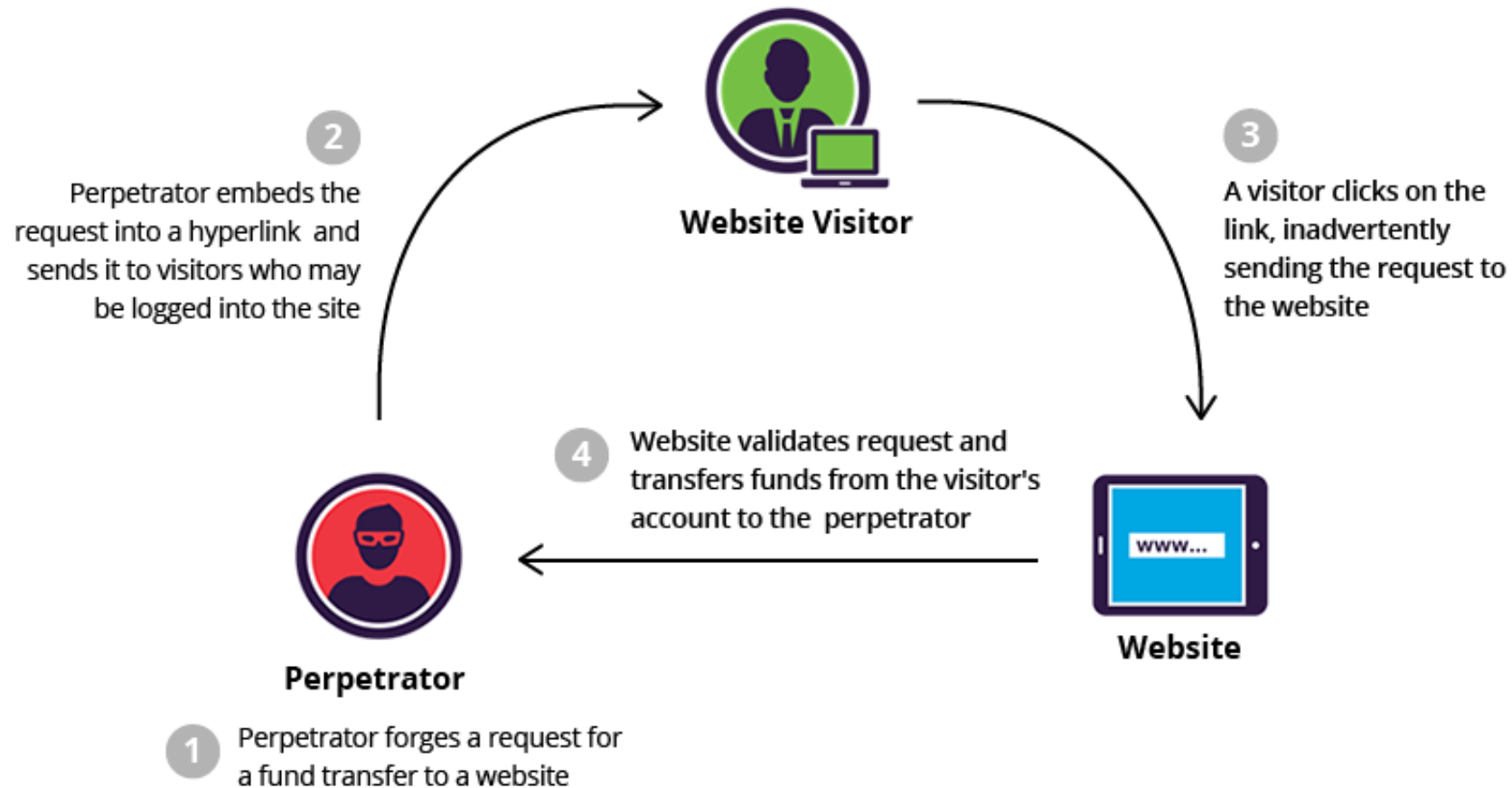


OWASP Top Ten




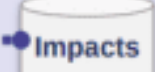
Cross-Site Request Forgery (CSRF)



OWASP Top Ten

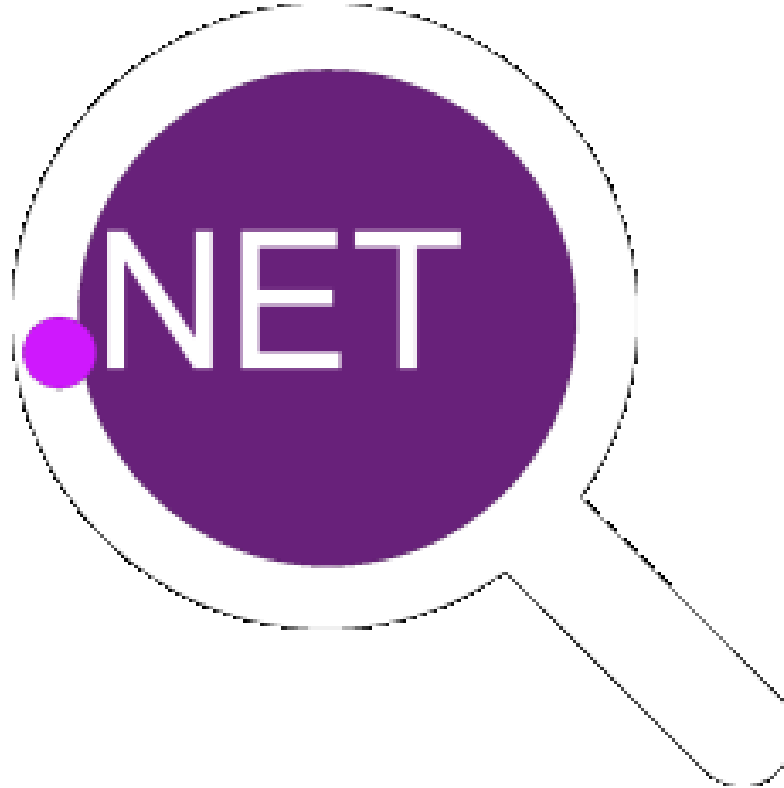


OWASP Top Ten

RISK	 Threat Agents	 Attack Vectors	 Security Weakness		 Impacts		Score
		Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY ③	COMMON ②	EASY ③	SEVERE ③	App Specific	8.0
A2:2017-Authentication	App Specific	EASY ③	COMMON ②	AVERAGE ②	SEVERE ③	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE ②	WIDESPREAD ③	AVERAGE ②	SEVERE ③	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE ②	COMMON ②	EASY ③	SEVERE ③	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE ②	COMMON ②	AVERAGE ②	SEVERE ③	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY ③	WIDESPREAD ③	EASY ③	MODERATE ②	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY ③	WIDESPREAD ③	EASY ③	MODERATE ②	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT ①	COMMON ②	AVERAGE ②	SEVERE ③	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE ②	WIDESPREAD ③	AVERAGE ②	MODERATE ②	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE ②	WIDESPREAD ③	DIFFICULT ①	MODERATE ②	App Specific	4.0

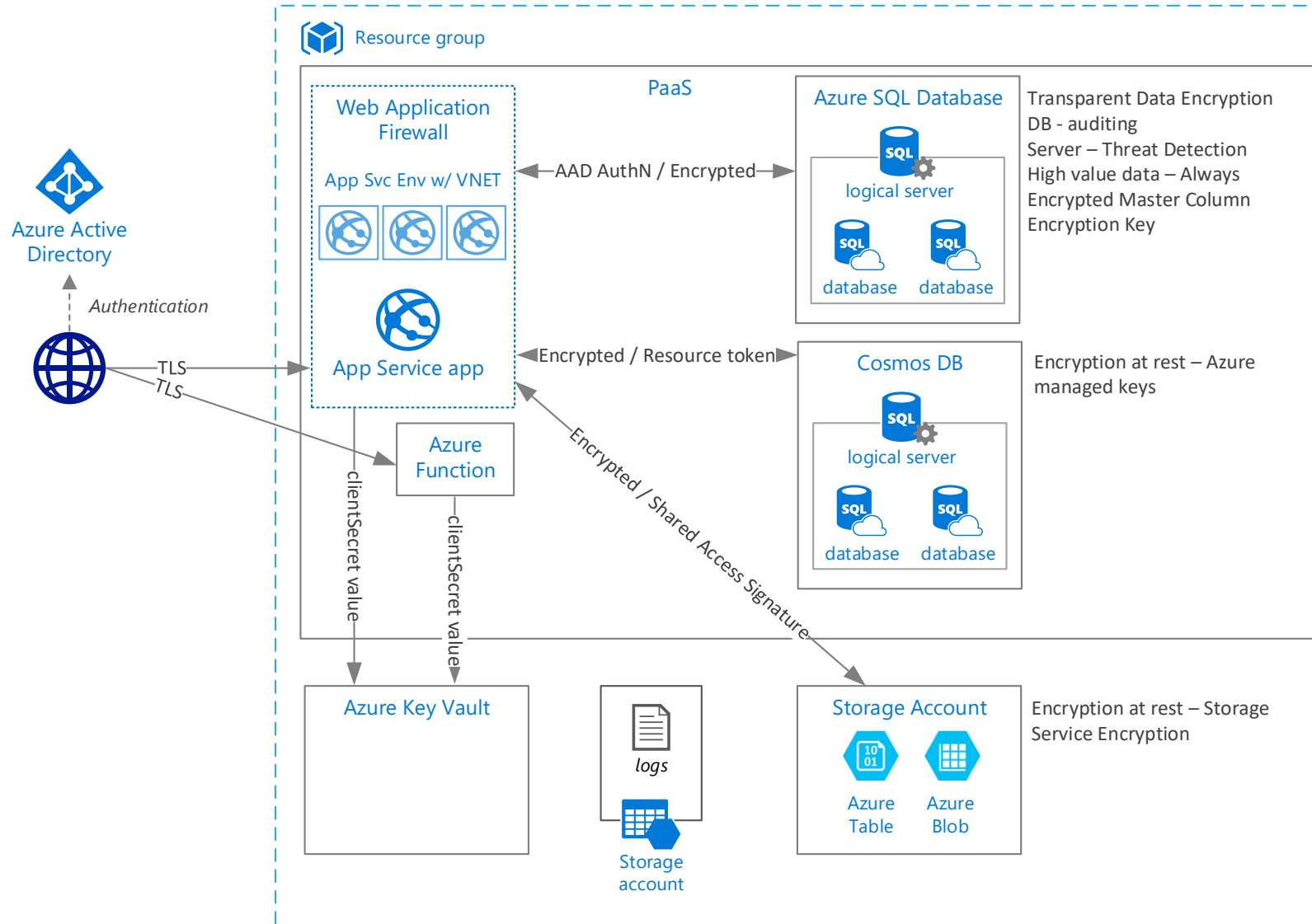
<https://owasp.org/www-project-top-ten/>

.NET Security Cheat Sheet



https://cheatsheetseries.owasp.org/cheatsheets/DotNet_Security_Cheat_Sheet.html

Recommended Architecture





OWASP with .NET 5 and Angular

Robert Rozas navarro
Senior Customer Engineer
rorozasn@microsoft.com

Thank you!