

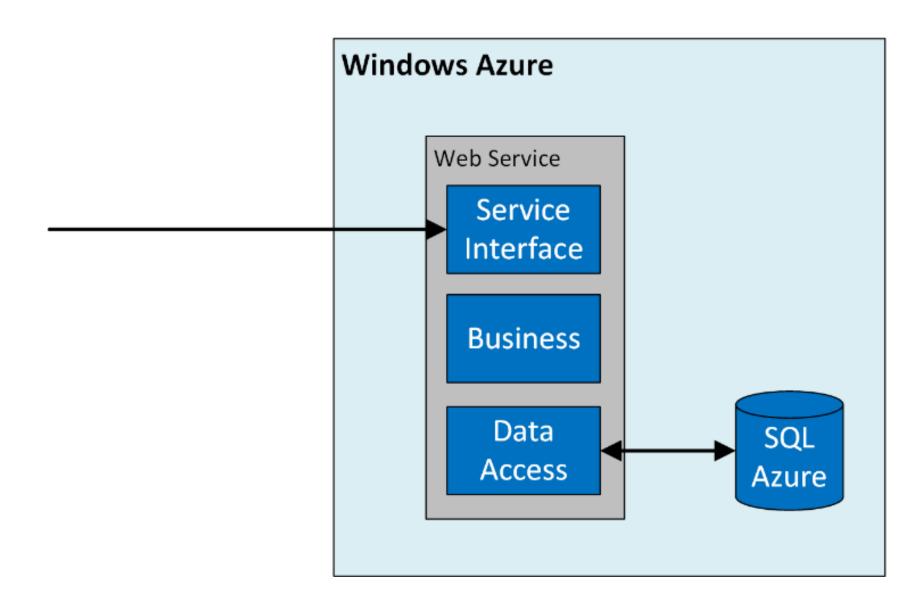
OWASP with .NET 5 and Angular

Robert Rozas navarro
Senior Customer Engineer rorozasn@microsoft.com

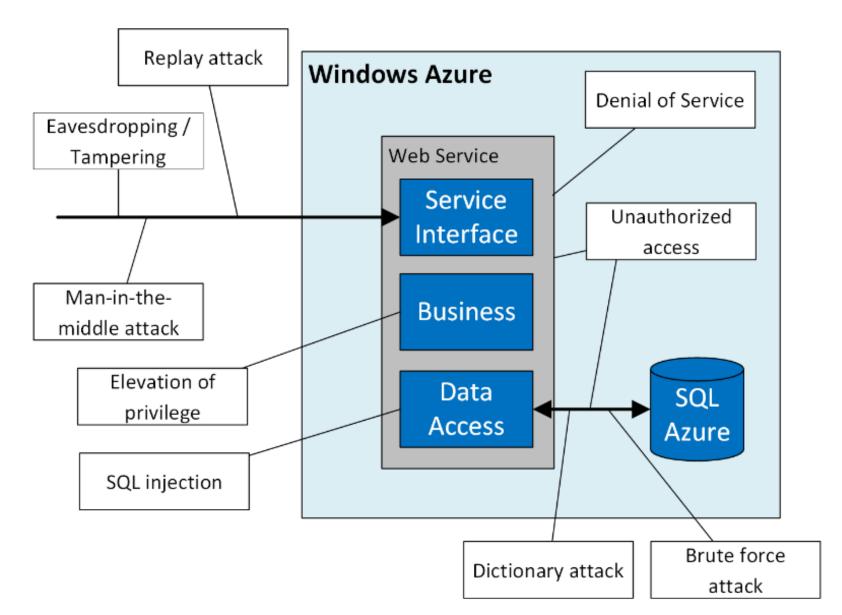
Agenda

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

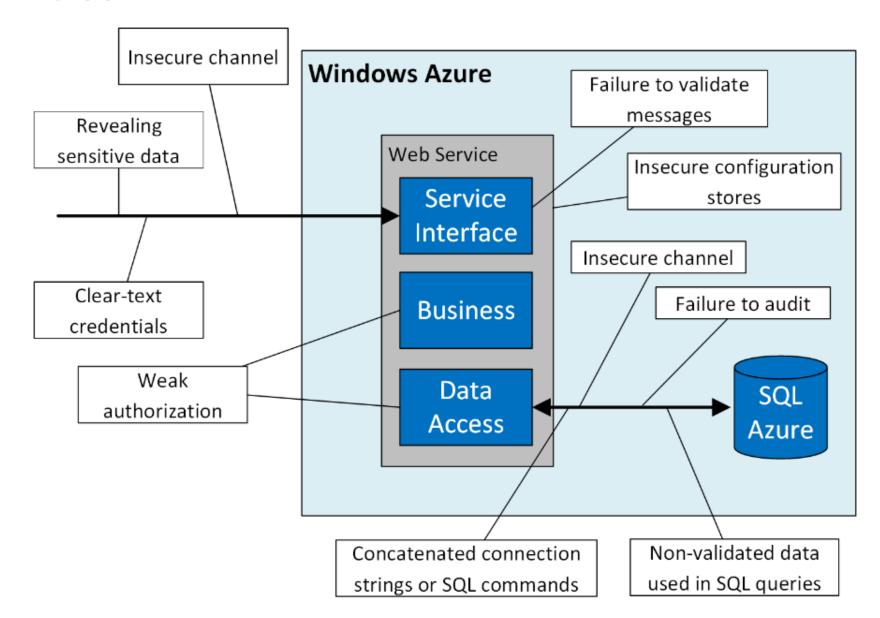
Scenario



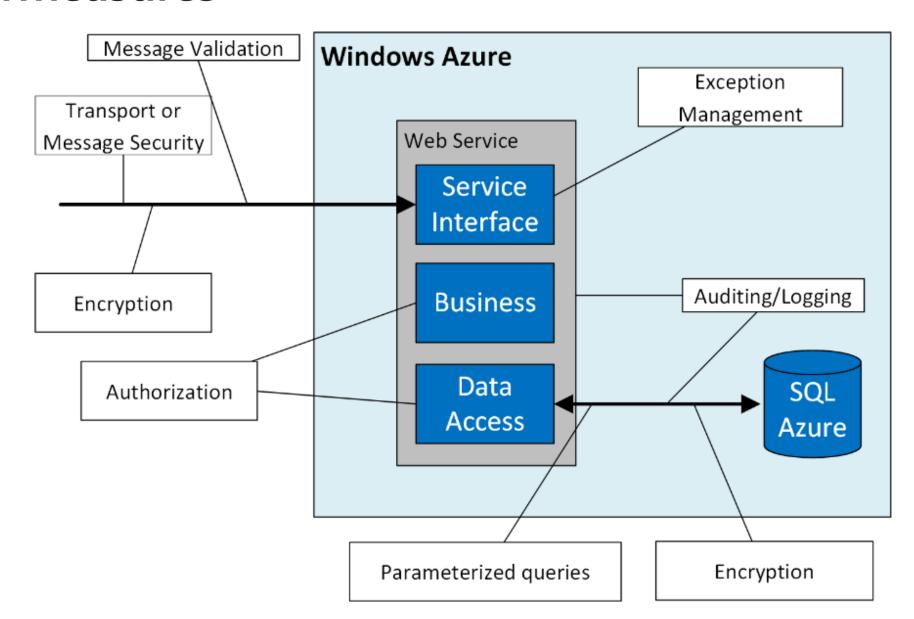
Threats / Attacks



Vulnerabilities



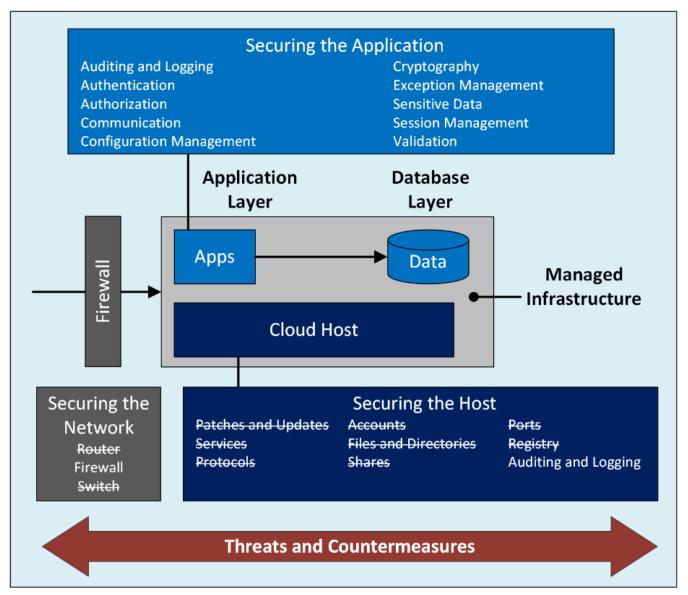
Countermeasures



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

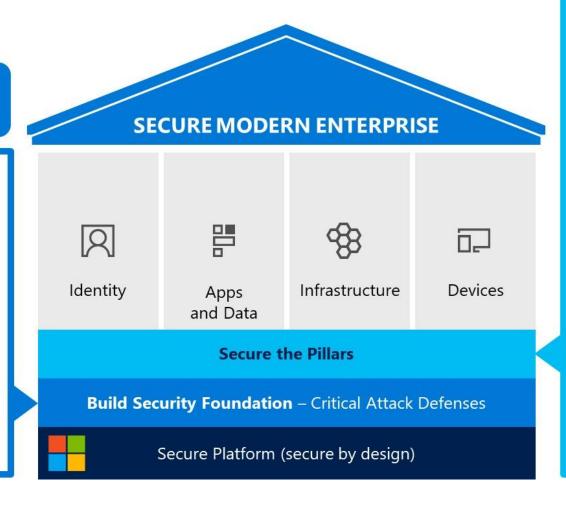
Starts Deployment of the SPA roadmap

http://aka.ms/SPARoadmap

Build the Security Foundation

Start the journey by getting in front of current attacks

- Critical Mitigations Critical attack protections
- Attack Detection Hunt for hidden persistent adversaries and implement critical attack detection
- Roadmap and planning –
 Share Microsoft insight on current attacks and strategies, build a tailored roadmap to defend your organization's business value and mission

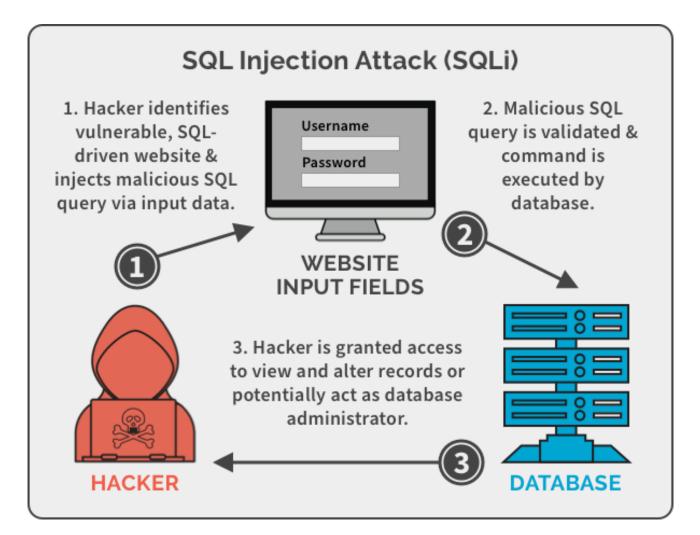


Secure the Pillars

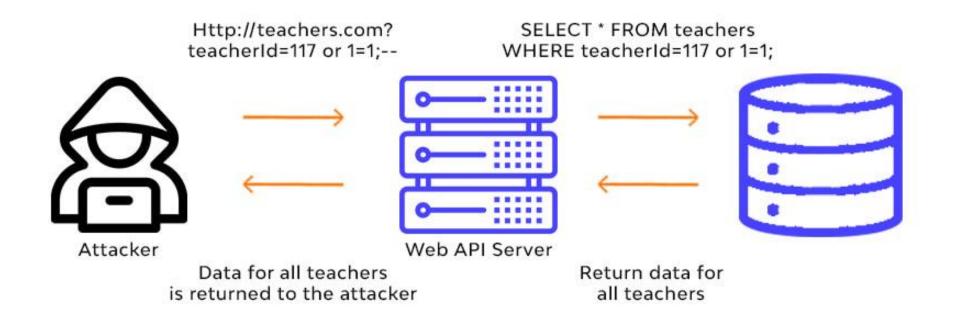
Continue building a secure modern enterprise by adopting leading edge technology and approaches:

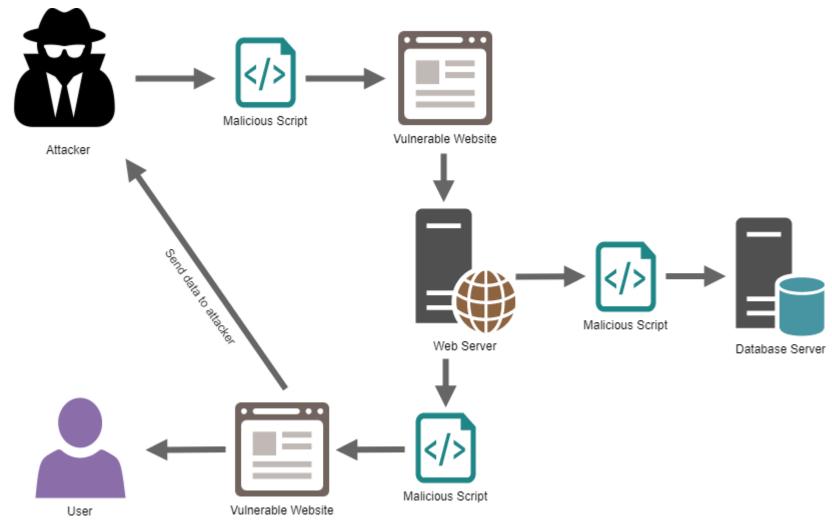
- Threat Detection Integrate leading edge intelligence and Managed detection and response (MDR) capabilities
- Identity and Access
 Management continue
 reducing risk to business
 critical identities and assets
- Information Protection— Discover, protect, and monitor your critical data
- Cloud Adoption Chart a secure path into a cloudenabled enterprise
- Device & Datacenter Security – Hardware protections for Devices, Credentials, Servers, and Applications
- App/Dev Security Secure your development practices and digital transformation components

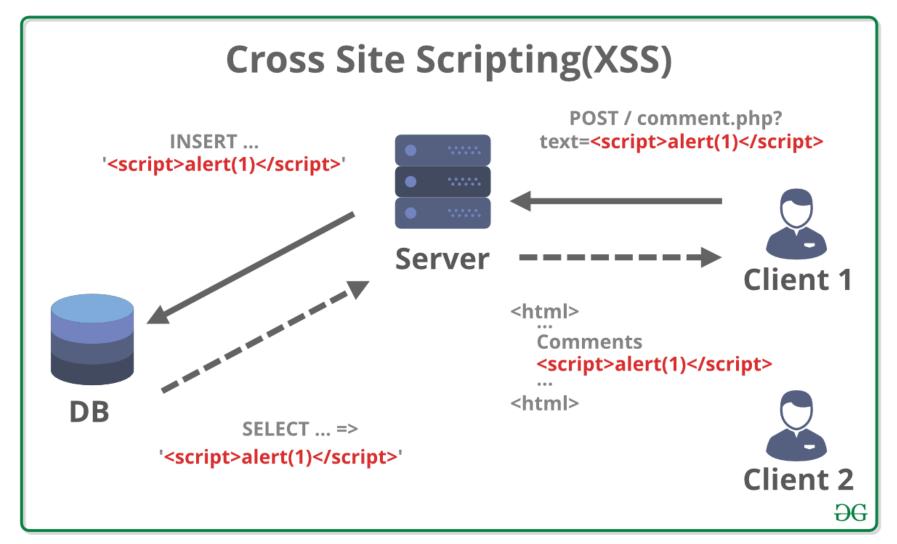
OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection		A1:2017-Injection
A2 – Broken Authentication and Session Management		A2:2017-Broken Authentication
A3 - Cross-Site Scripting (XSS)		A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]		A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration		A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	7	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]		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.]



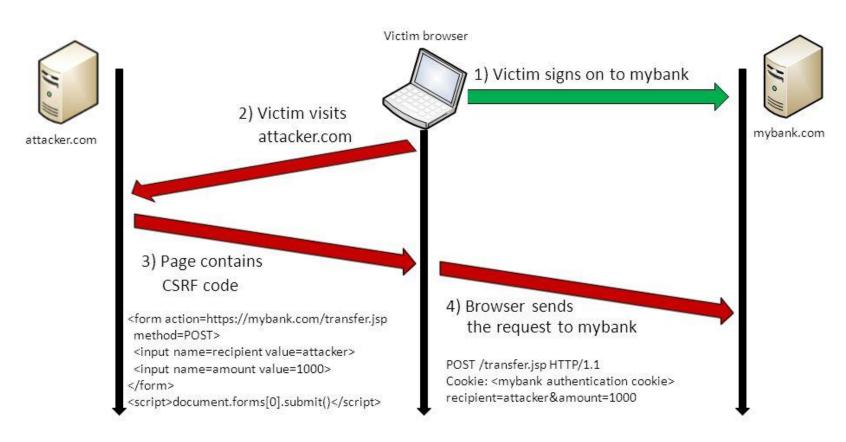
SQL Injection

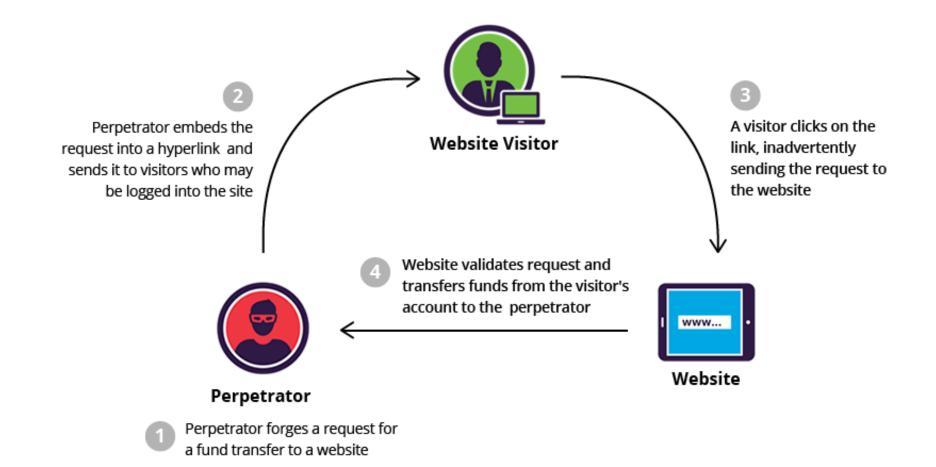


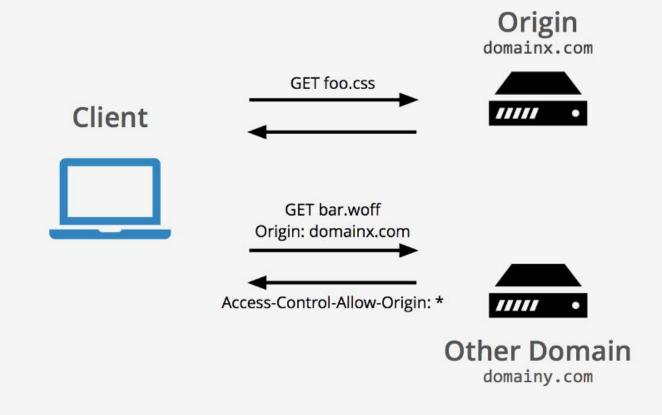




OWASP Top Ten Cross-Site Request Forgery (CSRF)



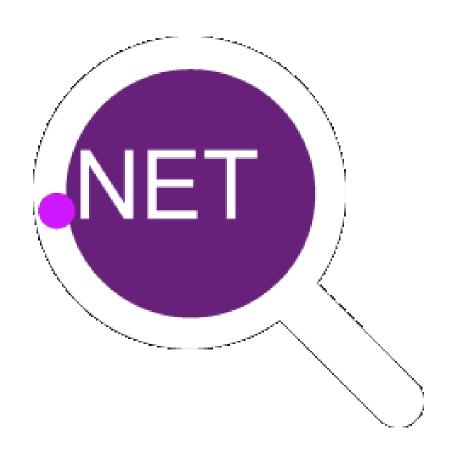




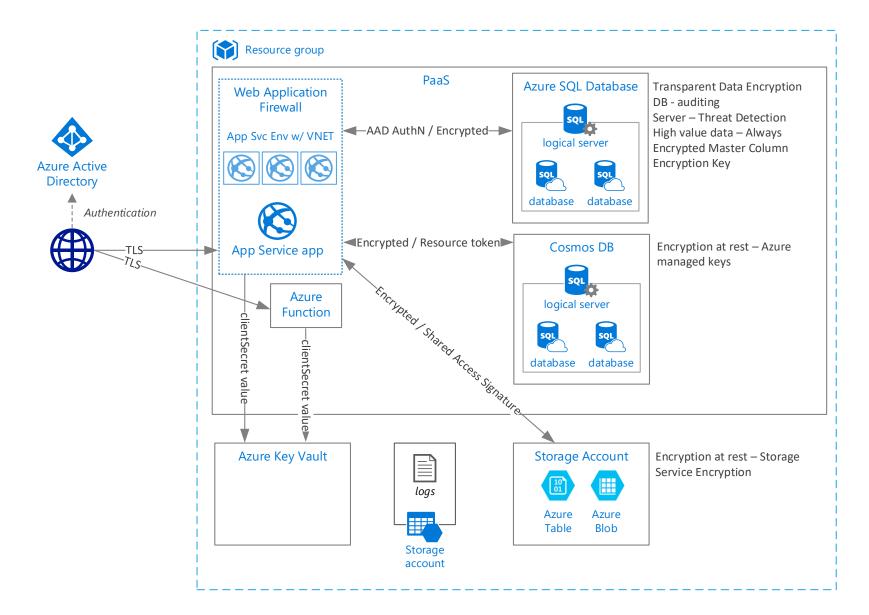
CORS

RISK	Threat Agents	Attack Vectors Exploitability		ecurity eakness Detectability	Impa	cts Business	Score
A1:2017- Injection	App Specific	EASY ③	соммон 2	EASY 3	SEVERE 3	App Specific	8.0
A2:2017- Authentication	App Specific	EASY 🕙	соммон 🕹	AVERAGE ②	SEVERE 3	App Specific	7.0
A3:2017- Sens. Data Exposure	App Specific	AVERAGE 2	WIDESPREAD 3	AVERAGE 2	SEVERE ①	App Specific	7.0
A4:2017-XML Exter- nal Entities (XXE)	App Specific	AVERAGE 2	соммон 🥹	EASY 🔾	SEVERE 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE ②	соммон 🥹	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 O	MODERATE @	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT 0	соммон 🚇	AVERAGE 2	SEVERE 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE	WIDESPREAD 3	AVERAGE 🔮	MODERATE	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE 3	WIDESPREAD 3	DIFFICULT 0	MODERATE @	App Specific	4.0

.NET Security Cheat Sheet



Recommended Architecture





OWASP with .NET 5 and Angular

Robert Rozas navarro
Senior Customer Engineer
rorozasn@microsoft.com

Thank you!