

Laboratorio de Seguridad para Servicios, Microservicios y SOA

Código: ARC-320

Propuesta de Valor: ARCITURA

Duración: 10 Horas



Como continuación de los Módulos 18 y 19, este taller práctico permite a los participantes aplicar los conceptos, técnicas, patrones y tecnologías de seguridad cubiertos previamente con el objetivo de completar un conjunto de ejercicios. Se pide a los participantes que analicen historiales de estudios de caso y realicen una serie de ejercicios para resolver problemas interrelacionados con el fin último de producir una serie de soluciones de seguridad.

AUDIENCIA

- Perfiles técnicos que tienen conocimientos de programación y desarrollo de software.
- Recién graduados.

PRE REQUISITOS

- Se recomienda realizar los cursos: ARC-318 y ARC-319.

OBJETIVOS

- Analizar historiales de estudios de caso.
- Realizar una serie de ejercicios para resolver problemas interrelacionados con el fin último de producir una serie de soluciones de seguridad.

CERTIFICACIÓN DISPONIBLE

- La ruta de Especialista en Seguridad de Servicios se compone de los Módulos 1, 2, 18, 19 y 20 de SOACP.



CONTENIDO

1. CONCEPTOS DE SEGURIDAD

- 1.1. CONFIANZA
- 1.2. RECLAMACIÓN
- 1.3. TOKENS
- 1.4. IDENTIFICACIÓN
- 1.5. AUTENTICACIÓN
- 1.6. AUTORIZACIÓN
- 1.7. CONFIDENCIALIDAD
- 1.8. INTEGRIDAD
- 1.9. NO REPUDIO
- 1.10. TRANSPORT LAYER SECURITY
- 1.11. SEGURIDAD DE LA CAPA DE MENSAJES

2. SEGURIDAD DEL CONTENEDOR

- 2.1. PRINCIPIO DE PRIVILEGIO MÍNIMO
- 2.2. DEFENSA EN PROFUNDIDAD

3. MECANISMOS DE SEGURIDAD

- 3.1. CIFRADO
- 3.2. HASH
- 3.3. FIRMAS DIGITALES
- 3.4. GESTIÓN DE IDENTIFICACIONES Y ACCESOS (IAM)
- 3.5. INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)
- 3.6. CERTIFICADOS DIGITALES
- 3.7. AUTORIDAD CERTIFICADORA (CA)
- 3.8. INICIO DE SESIÓN ÚNICO (SSO)
- 3.9. ACCIONES DE TOKEN DE SEGURIDAD
- 3.10. INTERMEDIACIÓN DE CONFIANZA
- 3.11. SESIONES DE SEGURIDAD
- 3.12. POLITICAS DE SEGURIDAD

4. ESTÁNDARES AVANZADOS DE LA INDUSTRIA

- 4.1. SERVICIOS WEB
- 4.2. SERVICIOS REST

5. MIDDLEWARE SOA

- 5.1. TAREAS DE SEGURIDAD
- 5.2. TEMAS DE SEGURIDAD

5.3. PATRONES

6. PATRONES DE SEGURIDAD DE INTERACCIÓN DE SERVICIOS

- 6.1. CONFIDENCIALIDAD DE LOS DATOS
- 6.2. AUTENTICACIÓN DE ORIGEN DE DATOS
- 6.3. AUTENTICACIÓN DIRECTA
- 6.4. AUTENTICACIÓN INTERMEDIADA

7. ESTÁNDARES DE LA INDUSTRIA PARA SERVICIOS REST

- 7.1. JWE
- 7.2. JWS
- 7.3. JWT
- 7.4. OAUTH 2.0
- 7.5. CONEXIÓN OPENID
- 7.6. TLS
- 7.7. HTTPS

8. TIPOS DE REGLAS DE CONTROL DE ACCESO

- 8.1. ACCIÓN
- 8.2. IDENTIDAD
- 8.3. RECURSO
- 8.4. AMBIENTE

9. AMENAZAS DE SEGURIDAD

- 9.1. AMENAZAS ORIENTADAS A DATOS
- 9.2. AMENAZAS ORIENTADAS AL ACCESO

10. ESTÁNDARES DE LA INDUSTRIA PARA SERVICIOS WEB

- 10.1. CIFRADO XML
- 10.2. FIRMA XML
- 10.3. CANONICALIZACIÓN
- 10.4. TRANSFORMACIÓN DE DESCIFRADO PARA FIRMA XML
- 10.5. WS-SECURITY
- 10.6. LENGUAJE DE MARCADO DE ASERCIÓN DE SEGURIDAD (SAML)

11. PATRONES DE SEGURIDAD DEL SERVICIO

- 11.1. BLINDAJE DE EXCEPCIONES
- 11.2. PANTALLA DE MENSAJES
- 11.3. SUBSISTEMA DE CONFIANZA
- 11.4. GUARDIA PERIMETRAL DE SERVICIO

12. AMENAZAS ESPECÍFICAS DE LA NUBE

12.1. AGENTES DE AMENAZA

12.2. ORIENTADO A DATOS

★ BENEFICIOS

- Al finalizar el curso, tendrás conocimientos en técnicas, patrones y tecnologías de seguridad cubiertos previamente con el objetivo de completar un conjunto de ejercicios.