

Seguridad de aplicaciones web

Ejemplos por sector de la industria



Ejemplos por sector de la industria

Industria	Perfil del Atacante	Deben estar en		
		Oportunista	Estándar	Avanzado
Financiera y Seguros.	<p>Ataques oportunistas, por motivos financieros.</p> <p>Búsqueda de datos o credenciales de cuentas a fin de realizar fraudes o beneficiarse directamente por el flujo de dinero (Transacciones B2B) que presentan estas aplicaciones.</p> <p>Chantajos basados en secuestro de datos (ransomware).</p> <p>Técnicas más comunes:</p> <p>Robo de credenciales y claves.</p> <p>Ataques a nivel de aplicación.</p> <p>Ingeniería social.</p>	Aplicaciones que son accesibles desde internet.	<p>Aplicaciones donde se transfiere dinero entre cuentas de la misma organización.</p> <p>Aplicaciones donde se realicen movimientos de dinero con Cámara de Compensación Automatizada (Automated Clearing House network, ACH) y con límites de transacción.</p> <p>Aplicaciones donde se realizan transferencias en línea con un rango de tiempo determinado.</p>	<p>Software que poseen sustanciales volúmenes de información delicada de cuentas bancarias.</p> <p>Aplicaciones donde las transferencias se realicen velozmente con sustanciales cantidades de dinero.</p> <p>Aplicaciones donde se permita realizar transacciones por lotes o individuales de grandes sumas de dinero.</p>
Manufacturera.	Ataques más organizados y con un	Aplicaciones que son	Aplicaciones donde la	Aplicaciones con

Profesional. Transporte. Tecnología. Utilidades. Infraestructura. Defensa.	<p>objetivo concreto, teniendo tiempo de preparación, grandes habilidades y sobre todo recursos; debido a que, llegar a la fuente de la información preciada es complejo y difícil de localizar.</p> <p>Haciendo uso de técnicas de ingeniería social avanzada se realizan ataques donde se requiere utilizar o manipular a los empleados de la organización o externos de la empresa pero con relación con alguno de los trabajadores.</p> <p>Búsqueda de datos de propiedad intelectual para obtener ventajas estratégicas sobre la competencia y venderlas al mejor postor.</p> <p>Ataques dirigidos a abusar de las funcionalidades para influenciar el comportamiento de forma directa o alterna, a fin de lograr beneficios personales, realizar chantajes, suplantar la identidad de otro, pagos de manera ilegal, o alterar partes sensibles del sistema.</p> <p>Técnicas más comunes:</p> <p>Robo de credenciales y claves.</p> <p>Ataques a nivel de aplicación.</p> <p>Ingeniería social avanzada.</p>	<p>accesibles desde internet.</p>	<p>información de los empleados se puede usar para modificar el núcleo del sistema.</p> <p>Sistemas que poseen en su información material de secretos empresariales y derechos de autor o propiedad intelectual.</p>	<p>contenido de secretos empresariales, gubernamentales, que poseen derechos de autor o propiedad intelectual que representan el éxito y la supervivencia de una organización.</p> <p>Aplicaciones que dentro de sus funciones existen controladores para operaciones muy delicadas donde un fallo expone la vida o amenaza la seguridad en general.</p>
Salud.	<p>Ataques más organizados y con un objetivo concreto, teniendo tiempo de preparación, grandes habilidades y sobre todo recursos; debido a que,</p>	<p>Aplicaciones que son accesibles desde internet.</p>	<p>Aplicaciones con información médica confidencial o sensible.</p>	<p>Aplicaciones que permiten controlar equipos sensibles en hospitales y salas de</p>

	<p>Llegar a la fuente de la información preciada es complejo y difícil de localizar.</p> <p>Haciendo uso de técnicas de ingeniería social avanzada se realizan ataques donde se requiere utilizar o manipular a los empleados de la organización o externos de la empresa pero con relación con alguno de los trabajadores.</p> <p>Búsqueda de datos de propiedad intelectual para obtener ventajas estratégicas sobre la competencia y venderlas al mejor postor.</p> <p>Ataques dirigidos a abusar de las funcionalidades para influenciar el comportamiento de forma directa o alterna, a fin de lograr beneficios personales, realizar chantajes, suplantar la identidad de otro, pagos de manera ilegal, o alterar partes sensibles del sistema.</p> <p>Técnicas más comunes:</p> <p>Robo de credenciales y claves.</p> <p>Ataques a nivel de aplicación.</p> <p>Ingeniería social avanzada.</p>			<p>cirugía, o dispositivos que monitorean la salud de un paciente y se ponga en riesgo su vida.</p>
Venta por menor, alimento, hospitalidad.	<p>Ataques utilizando tácticas oportunistas de "aplaste y agarre".</p> <p>Ataques Oportunistas, por motivos financieros o por motivos personales identificables.</p>	Aplicaciones que son accesibles desde internet.	Aplicaciones que presenten sus catálogos empresariales con información sensible de sus productos o servicios, o datos corporativos de sus empleados o junta directiva	Aplicaciones POS que tienen multitud de información de transacciones que si se detectan se pueden usar para realizar robos o fraudes.

	<p>Ataques más orquestados y totalmente enfocados a sustraer información específica de propiedad intelectual, derechos de autor, entre otros, con el fin de tener una ventaja competitiva contra sus pares empresariales.</p> <p>Técnicas más comunes:</p> <p>Robo de credenciales y claves.</p> <p>Ataques a nivel de aplicación.</p> <p>Tácticas oportunistas de "aplaste y agarre".</p> <p>Ingeniería social avanzada.</p>		<p>y algunas aplicaciones que ocultan información a los usuarios.</p> <p>Aplicaciones con ínfimas cantidades de funciones de datos o de confirmaciones de pagos.</p>	<p>Sistemas que gestionan un volumen sustancial de datos sensibles, que poseen información de tarjetas de crédito, nombres completos y documentos de identidad.</p>
--	---	--	--	---

Tomado de (OWASP. 2021).