LAB 1

1. **In which pase of the software development Lifecycle will it be possible to eliminate most of security flaws?**
   a. Requirement
   b. Design
   c. Development
   d. Deployment

2. **In which phase of the Security Development Lifecycle would you perform security and privacy risk assessments?**
   a. Training phase
   b. Requirements phase
   c. Design phase
   d. Implementation phase

3. **Ted is an application security engineer who ensures application security activities are being followed during the entire lifecycle of the project. One day, he was analyzing various interactions of users depicted in the use cases of the project under inception. Based on the use case in hand, he started depicting the scenarios where attacker could misuse the application. Can you identify the activity on which Ted is working?**
   a. Ted was depicting lower-level use cases
   b. Ted was depicting abuse cases
   c. Ted was depicting security use cases
   d. Ted was depicting abstract use cases

4. **Which of the following relationship is used to describe abuse case scenarios?**

   a. Threatens Relationship
   b. Mitigates Relationship
   c. Include Relationship
   d. Extend Relationship

5. **Which of the following relationship is used to describe security use case scenario?**

a. Threatens Relationship
b. Mitigates Relationship
c. Include Relationship
d. Extend Relationship

6. **Which of the following can be derived from abuse cases to elicit security requirements for software system?**

a. Use cases
b. Misuse cases
c. Security use cases
d. Data flow diagram

POSSIBLE CASES OF ABUSE

Registro

Abuse case ID:	001
Name:	Cross side scripting
Priority:	Alta
Scope:	Total
Development environment:	Desarrollo
Mis-actors:	Usuario, sistema
Access right levels:	No autenticado
Point of entry:	Formulario
Security attributes affected:	Confidencialidad, integridad
Description:	Se podría cambiar el código de registro para que envié las credenciales de todas las personas que se registren y así robar credenciales y dinero.
Sophistication:	Fácil

Abuse case ID:	002
Name:	Phishing
Priority:	Media
Scope:	Parcial
Development environment:	Desarrollo
Mis-actors:	Sistema
Access right levels:	No autenticado
Point of entry:	Formulario
Security attributes affected:	Integridad, no repudio
Description:	Al registrarse se envía un correo para confirmar la cuenta y así robar credenciales.
Sophistication:	Medio

Autenticación

Abuse case ID:	003
Name:	Robo de credenciales
Priority:	Medio
Scope:	Parcial´
Development environment:	Desarrollo
Mis-actors:	Usuario, Admin,
Access right levels:	Autenticado
Point of entry:	Formulario
Security attributes affected:	Confidencialidad
Description:	Siguiendo la lógica del caso de abuso 001, se puede hacer un robo de credenciales.
Sophistication:	Fácil

Abuse case ID:	004
Name:	Secuestro de sesión
Priority:	Baja
Scope:	Parcial
Development environment:	Desarrollo
Mis-actors:	Usuario, Admin
Access right levels:	Autenticado
Point of entry:	Cookies

Security attributes affected:	Integridad, Confidencialidad
Description:	Robar cookie de sesión y secuestrar sesión.
Sophistication:	Fácil

Ver productos

Abuse case ID:	005
Name:	Cambiar precios productos
Priority:	Alta
Scope:	Total
Development environment:	Desarrollo
Mis-actors:	Usuario, sistema
Access right levels:	Autenticado
Point of entry:	Admin, sistema
Security attributes affected:	Integridad, no repudio
Description:	Modificar los precios de los productos así afectar la compra de los clientes. Una manera de hacer eso es entrando con permisos de administrador.
Sophistication:	Difícil

Abuse case ID:	006
Name:	Mostrar productos diferentes
Priority:	Alta
Scope:	Total
Development environment:	Desarrollo
Mis-actors:	Sistema, Admin
Access right levels:	Autenticado
Point of entry:	Sistema, Admin
Security attributes affected:	Integridad, no repudio
Description:	Mostrar productos diferentes que no pertenecen a la tienda para así estafar a las personas.
Sophistication:	Difícil

Comprar

Abuse case ID:	007
Name:	Modificar precio pagado
Priority:	Baja
Scope:	Parcial
Development environment:	Desarrollo
Mis-actors:	Usuario, sistema
Access right levels:	Autenticado
Point of entry:	Banco, sistema, Usuario
Security attributes affected:	Integridad, no repudio
Description:	Comprar el producto por un precio y que se descuente un monto diferente a la tarjeta.
Sophistication:	Difícil

Abuse case ID:	008
Name:	Robo de tarjeta crédito
Priority:	Alta
Scope:	Parcial
Development environment:	Desarrollo
Mis-actors:	Banco, sistema, Usuario
Access right levels:	Autenticado
Point of entry:	Banco, sistema, Usuario
Security attributes affected:	Integridad, No repudio, Confidencialidad
Description:	A la hora de poner la info de la tarjeta para pagar, robar su información.
Sophistication:	Medio

Acceder a un descuento

Abuse case ID:	009
Name:	Descuento incrementado
Priority:	Alta
Scope:	Parcial
Development environment:	Desarrollo
Mis-actors:	Sistema, Admin
Access right levels:	Autenticado
Point of entry:	Sistema, Admin

Security attributes affected:	Integridad, no repudio
Description:	Hay un descuento y la hora de pagar se incrementa para el usuario.
Sophistication:	Media

Abuse case ID:	010
Name:	Acceso denegado al descuento
Priority:	Baja
Scope:	Parcial
Development environment:	Desarrollo
Mis-actors:	Sistema, Admin
Access right levels:	Autenticado
Point of entry:	Sistema, Admin
Security attributes affected:	Integridad, no repudio
Description:	Hay un descuento y la hora de pagar no se puede aplicar para el usuario
Sophistication:	Baja

Cambiar foto de perfil

Abuse case ID:	011
Name:	Phishing
Priority:	Baja
Scope:	Parcial
Development environment:	Desarrollo
Mis-actors:	Usuario
Access right levels:	Autenticado
Point of entry:	Sistema
Security attributes affected:	Integridad, no repudio, Confidencialidad
Description:	Para cambiar la foto de perfil, se te envía un correo para confirmar el cambio en donde hay que autenticarse.
Sophistication:	Medio

Abuse case ID:	012
Name:	Robo de datos
Priority:	Alta

Scope:	Parcial
Development environment:	Desarrollo
Mis-actors:	Usuario, sistema
Access right levels:	Autenticado
Point of entry:	Usuario, sistema
Security attributes affected:	Integridad, Confidencialidad
Description:	A la hora de cambiar la foto de perfil y acceder a las fotos para elegir una, poder robar todas las fotos guardadas.
Sophistication:	Medio