27_ejemplos_de_codigo_inseguro

May 8, 2020

1 Código inseguro.

A continuación se mostrarán algunos ejemplos representativos de código inseguro tomados del Top 25 del proyecto "Common Weakness Enumeration".

https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

1.1 Validación impropia de un ingreso de datos.

https://cwe.mitre.org/data/definitions/20.html

1.1.1 Ejemplo 1.

El siguiente código no impide que se usen números negativos, por lo que un usuario podría ingresar un saldo a favor.

```
...
public static final double price = 20.00;
int quantity = currentUser.getAttribute("quantity");
double total = price * quantity;
chargeUser(total);
...
```

1.1.2 Ejemplo 2.

El siguiente código crea una lista a partir de un valor ingresado por el usuario. Valida que no se ingresen números negativos, pero permite crear arreglos de valor igual a `0`, lo que desnecadenará una excepción.

```
private void buildList ( int untrustedListSize ){
if ( 0 > untrustedListSize ){
die("Negative value supplied for list size, die evil hacker!");
}
Widget[] list = new Widget [ untrustedListSize ];
list[0] = new Widget();
}
```

1.1.3 Ejemplo 3.

El siguiente código asume que siempre se ingresará una URL.

En caso de no ingresar una URL, el método `intent.getStringExtra()` regresará `null`, causando una excepción al ejecutar `URL.length()`.

```
...
IntentFilter filter = new IntentFilter("com.example.URLHandler.openURL");
MyReceiver receiver = new MyReceiver();
registerReceiver(receiver, filter);
...

public class UrlHandlerReceiver extends BroadcastReceiver {
@Override
public void onReceive(Context context, Intent intent) {
if("com.example.URLHandler.openURL".equals(intent.getAction())) {
String URL = intent.getStringExtra("URLToOpen");
int length = URL.length();

...
}
}
}
```

1.2 Exposición de datos sensibles a un usuario sin autorización.

https://cwe.mitre.org/data/definitions/200.html

1.2.1 Ejemplo 1.

El siguiente código intentará abrir una conexión a una base de datos y desplegará la información de una excepción en caso de que ocurra.

```
try {
openDbConnection();
}
//print exception message that includes exception message and configuration file location
catch (Exception $e) {
echo 'Caught exception: ', $e->getMessage(), '\n';
echo 'Check credentials in config file at: ', $Mysql_config_location, '\n';
}
```

1.2.2 Ejemplo 2.

En le siguiente código, el método `getUserBankAccount()` accede a la información de una base de datos por medio de `username` y `accountNumber`.

La ocurrir una excepción `SQLException`, el mensaje es enviado a una bitácora.

El mensaje de error incluye información sobre la consulta a la base de datos, lo quen podría facilitar un ataque posterior de SQL Injection.

```
public BankAccount getUserBankAccount(String username, String accountNumber) {
BankAccount userAccount = null;
```

```
String query = null;
try {
if (isAuthorizedUser(username)) {
query = "SELECT * FROM accounts WHERE owner = "
+ username + " AND accountID = " + accountNumber;
DatabaseManager dbManager = new DatabaseManager();
Connection conn = dbManager.getConnection();
Statement stmt = conn.createStatement();
ResultSet queryResult = stmt.executeQuery(query);
userAccount = (BankAccount)queryResult.getObject(accountNumber);
}
} catch (SQLException ex) {
String logMessage = "Unable to retrieve account information from database,\nquery: " + query;
Logger.getLogger(BankManager.class.getName()).log(Level.SEVERE, logMessage, ex);
}
return userAccount;
}
```

1.2.3 Ejemplo 3.

- El siguiente código almacena información sobre la localización de un usuario, la cual será enviada a una bitácora.

```
locationClient = new LocationClient(this, this, this);
locationClient.connect();
currentUser.setLocation(locationClient.getLastLocation());
...

catch (Exception e) {
AlertDialog.Builder builder = new AlertDialog.Builder(this);
builder.setMessage("Sorry, this application has experienced an error.");
AlertDialog alert = builder.create();
alert.show();
Log.e("ExampleActivity", "Caught exception: " + e + " While on User:" + User.toString());
}
```

1.2.4 Ejemplo 4.

En el siguiente caso, una aplicación requiere de la localización de un usuario. Sin embargo, no es necesario que la lozalización sea de lata precisión.

- El archivo `manifest.xml` indica que la aplicación debe de usar una localización de alta precisión.

```
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
```

- La aplicación solo requiere datos generales de localización.

```
locationClient = new LocationClient(this, this, this);
locationClient.connect();
Location userCurrLocation;
```

```
userCurrLocation = locationClient.getLastLocation();
deriveStateFromCoords(userCurrLocation);
```

1.3 Otros ejemplos de código distinto a Java.

1.3.1 Cross site scripting.

https://cwe.mitre.org/data/definitions/79.html

1.3.2 SQL Injection.

https://cwe.mitre.org/data/definitions/89.html

1.3.3 Cross-Site Request Forgery (CSRF)

https://cwe.mitre.org/data/definitions/352.html

1.3.4 Autenticación impropia.

https://cwe.mitre.org/data/definitions/287.html

1.3.5 Restricción impropia de una referencia a una entidad externa de XML.

https://cwe.mitre.org/data/definitions/611.html

1.3.6 Inyección de código.

https://cwe.mitre.org/data/definitions/94.html