Communicating with Databases

String based queries are prevalent:

- **JPA, Hibernate, TopLink**

Example: Using JPA to query DB

Query in JPA Query Language:

```
"SELECT w FROM Weblog w
 WHERE w.id = ?1 AND w.link.id = ?2"
```

Java syntax in query String

Mappi

- **Expressed in Object Relational Mapping (ORM)**

Example: Using JPA to query DB

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Example: Using JPA to query DB

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. **Build query string**

Example: Using JPA to query DB

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

▶ q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Build query string
2. **Create query**

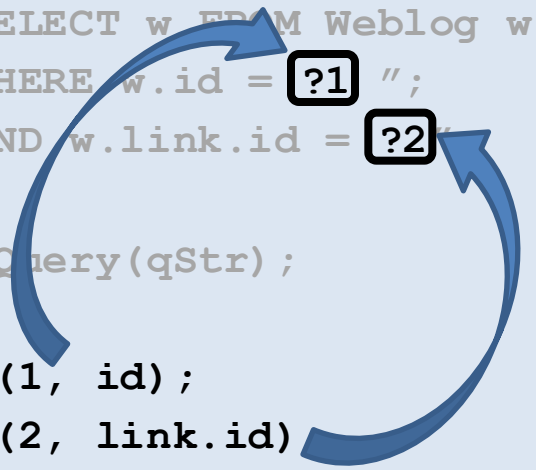
Example: Using JPA to query DB

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

▶ q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Build query string
2. Create query
3. **Set parameters**

Example: Using JPA to query DB

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id)

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```



1. Build query string
2. Create query
3. **Set parameters**

Example: Using JPA to query DB

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

▶ Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Build query string
2. Create query
3. Set parameters
4. **Execute query**

Example: Using JPA to query DB

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Build query string
2. Create query
3. Set parameters
4. Execute query

- Efficient
- Flexible

Unsafe

Uncaught Errors

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Uncaught Errors

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  // q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Uncaught Errors

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  // q.setParam(2, link.id);

▶ Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. **Unset parameter**

Uncaught Errors

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

▶ q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Unset parameter

Uncaught Errors

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

▶ q.setParam(1, new Weblog());
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Unset parameter
2. **Unsafe param type**

Uncaught Errors

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

▶ Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Unset parameter
2. Unsafe param type

Uncaught Errors

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Warranty w = (Warranty) q.execQuery();

  return w.text;
}
```

1. Unset parameter
2. Unsafe param type
3. **Unsafe downcast**

Uncaught Errors

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Unset parameter
2. Unsafe param type
3. Unsafe downcast

Java compiler does not reason about the query strings; cannot typecheck.

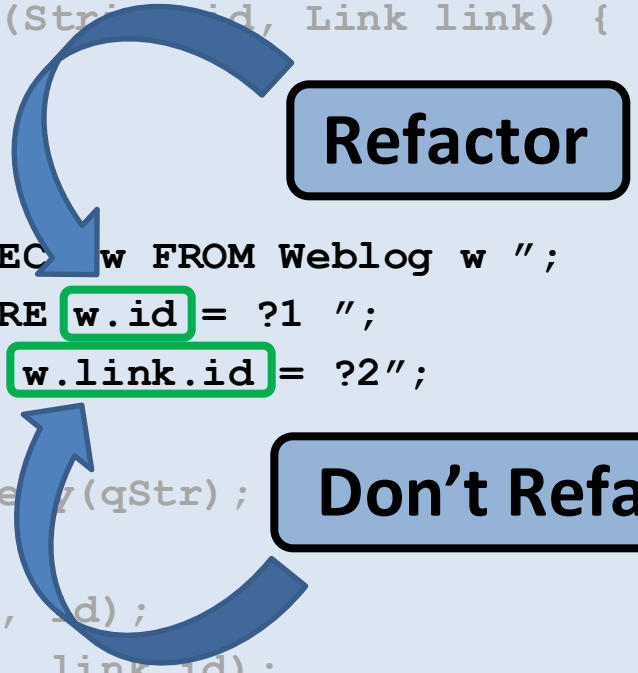
Refactor: Weblog.id → Weblog.name

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Unset parameter
2. Unsafe param type
3. Unsafe downcast

Refactor: Weblog.id → Weblog.name

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```



1. Unset parameter
2. Unsafe param type
3. Unsafe downcast

Need to know type of w and w.link to refactor safely.

Refactor: Weblog.id → Weblog.name

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Unset parameter
2. Unsafe param type
3. Unsafe downcast
4. **Refactoring difficult**

String Based Query Challenges

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

1. Unset parameter
2. Unsafe param type
3. Unsafe downcast
4. Refactoring difficult

Deep Typechecking Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

▶ Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Query safety:

- **All params set**
- **Params safely set**
- **Result safely downcast**

Is this query exec safe?

Need to know:

1. **query string**
2. **param types**

Deep Typechecking Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

▶ Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

***Bound Query*:**

- **query string**
- **param types**

Example :

query : "SELECT … ?1 … ?2 … ?3 …"
?1 : String
?2 : Weblog
?3 : unknown

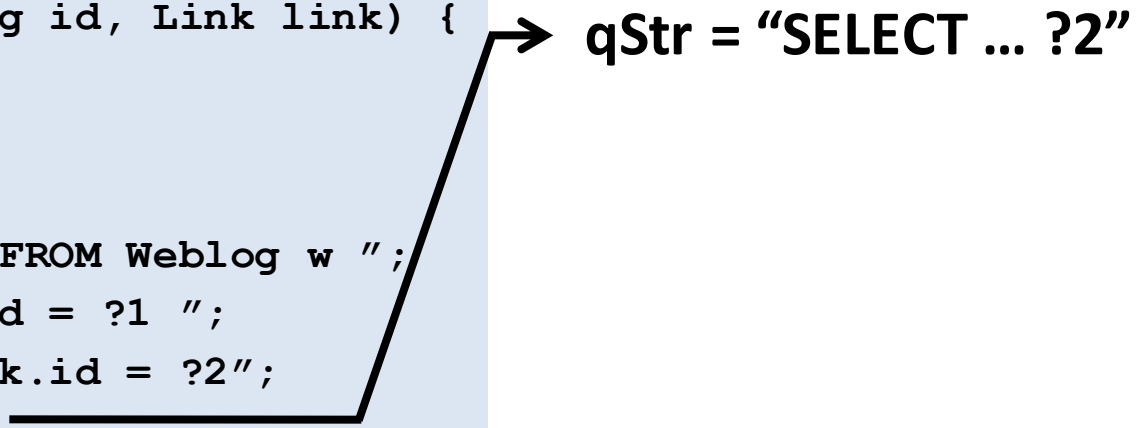
At each program point map each var to a set of BQs.

Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

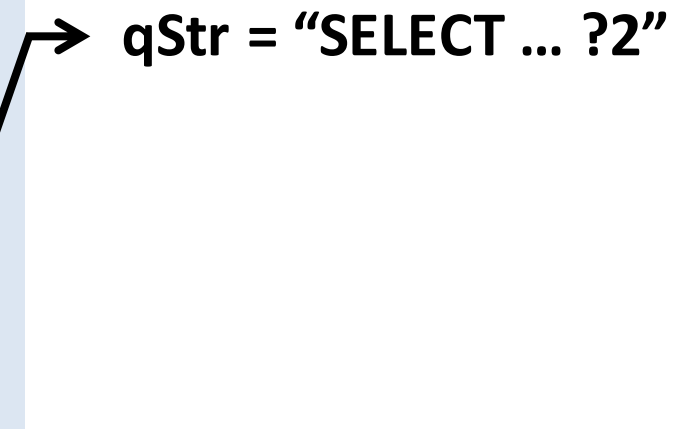
Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```



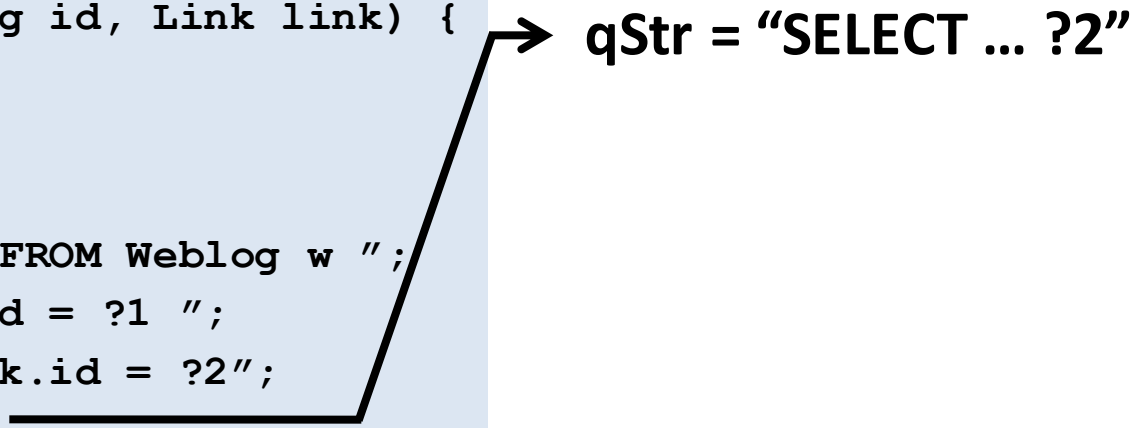
Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```



Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```



Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

qStr = "SELECT … ?2"

query : "SELECT …"
?1 : unknown
?2 : unknown

Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

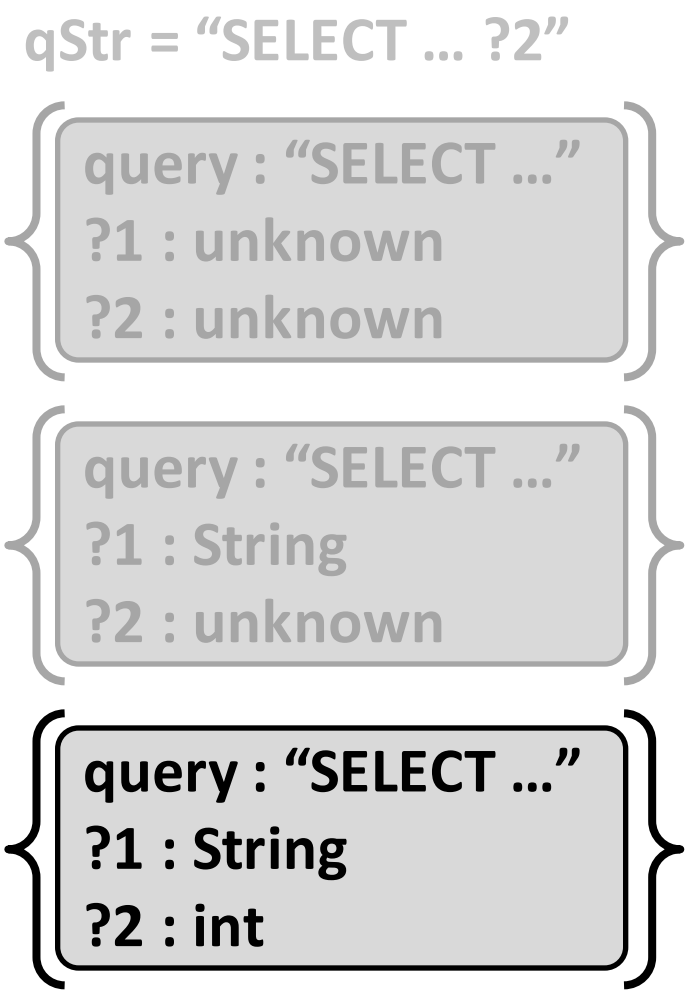
qStr = "SELECT … ?2"

query : "SELECT …"
?1 : unknown
?2 : unknown

query : "SELECT …"
?1 : String
?2 : unknown

Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```



Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Checking param types:

1. **Parse query string**
2. **Check all params set**
3. **Check param types**

Bound Queries:

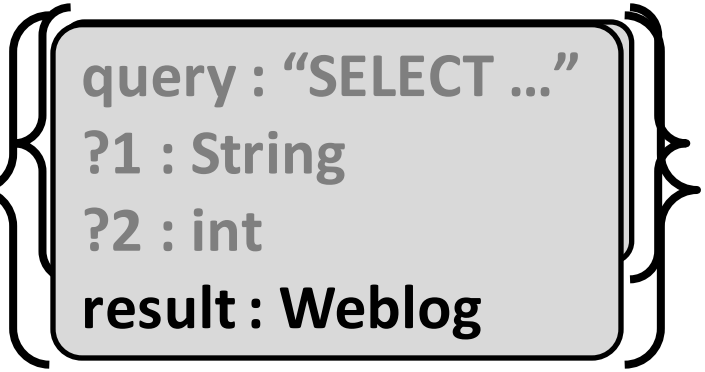
Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Checking result type:

1. **Infer result type**
2. **Propagate result type**
3. **Check downcasts**

Bound Queries:



Bound Query Analysis

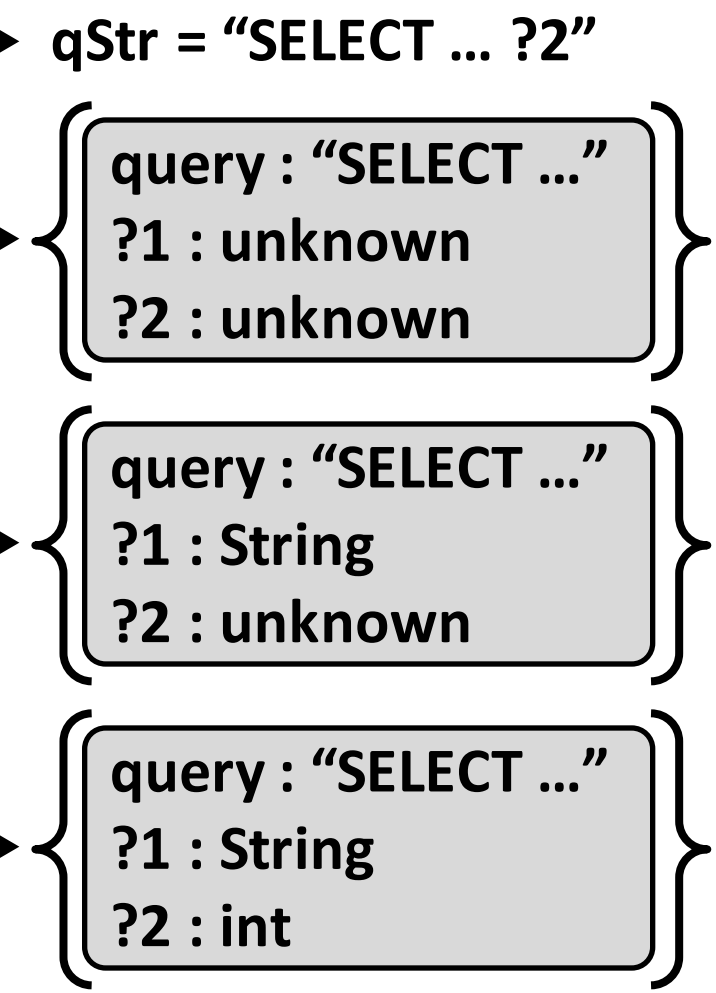
```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

If a query passes Deep Typechecking, then it will not cause an error at runtime.

Therefore, Bound Query Analysis has no silent failures.

Bound Query Analysis

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```



Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Refactor Weblog field:

id → name

Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Refactor Weblog field:

id → name

Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Refactor Weblog field:

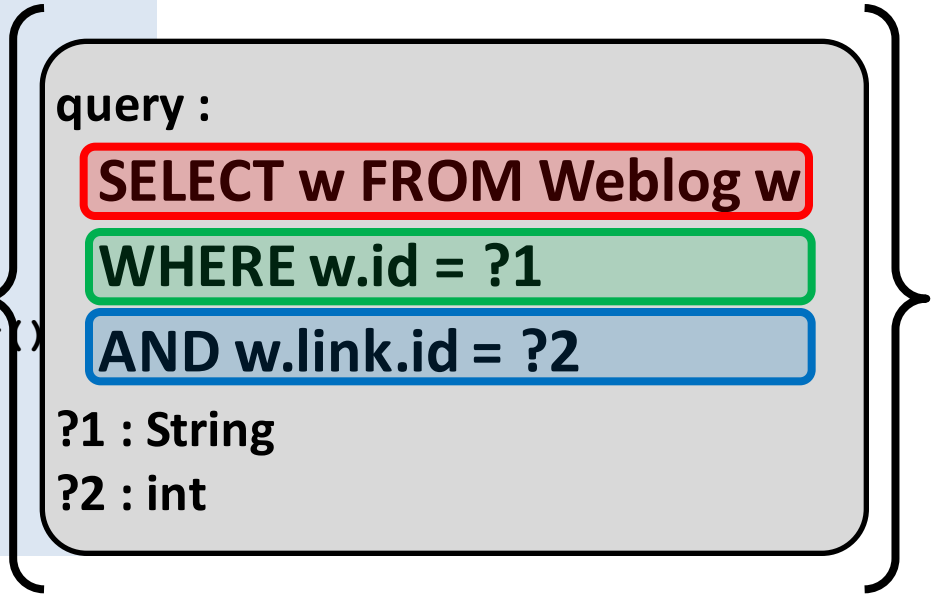
id → name

Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Refactor Weblog field:

id → name



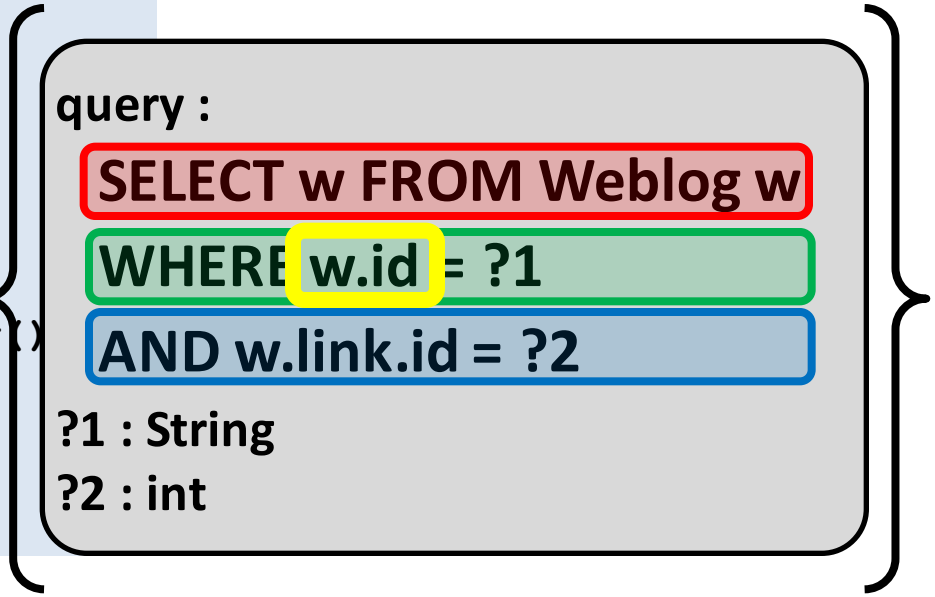
Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Refactor Weblog field:

id → name

1. **Refactor full query**



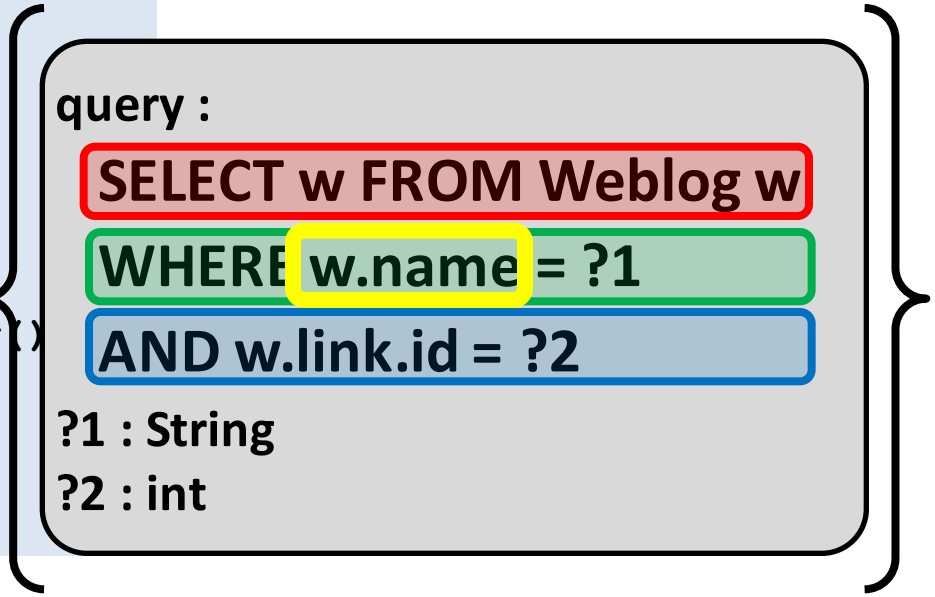
Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Refactor Weblog field:

id → name

1. **Refactor full query**



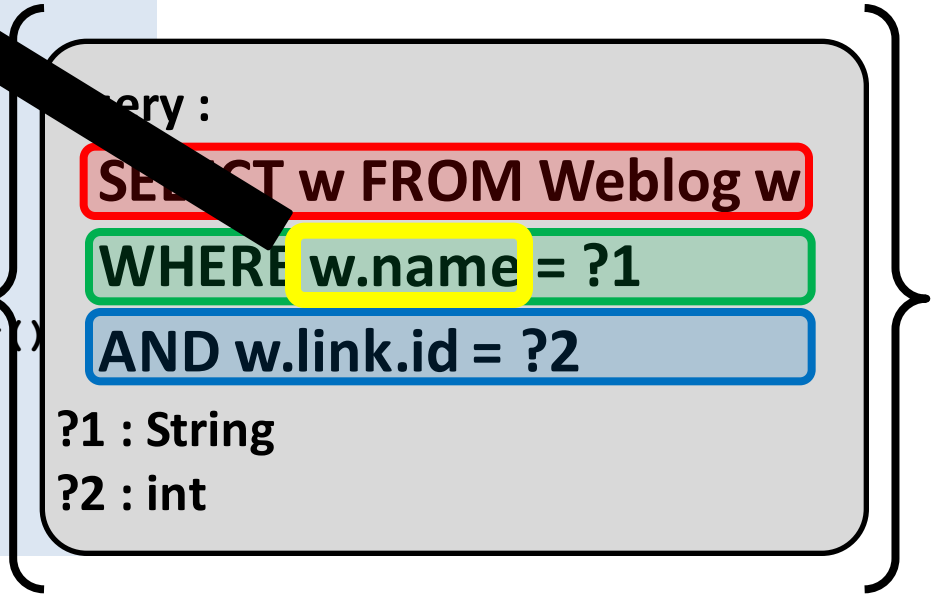
Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Refactor Weblog field:

id → name

1. **Refactor full query**
2. **Propagate changes**



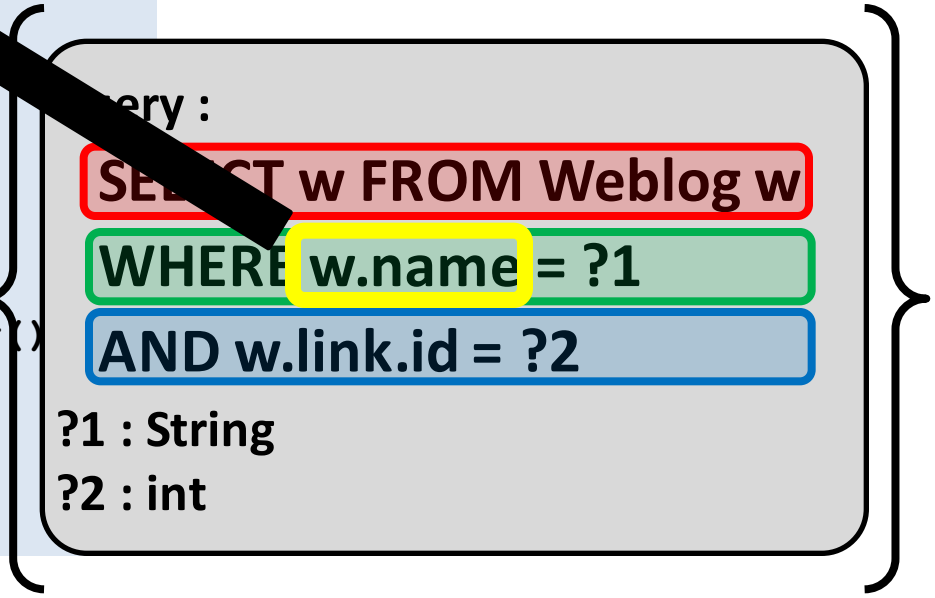
Deep Refactoring Example

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.name = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Refactor Weblog field:

id → name

1. **Refactor full query**
2. **Propagate changes**



Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "AND w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  qStr += "AND w.link.id = ?2";
  q = createQuery(qStr);
  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  qStr += "AND w.link.id = ?2";
  q = createQuery(qStr);
  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {



  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

Flow Sensitivity

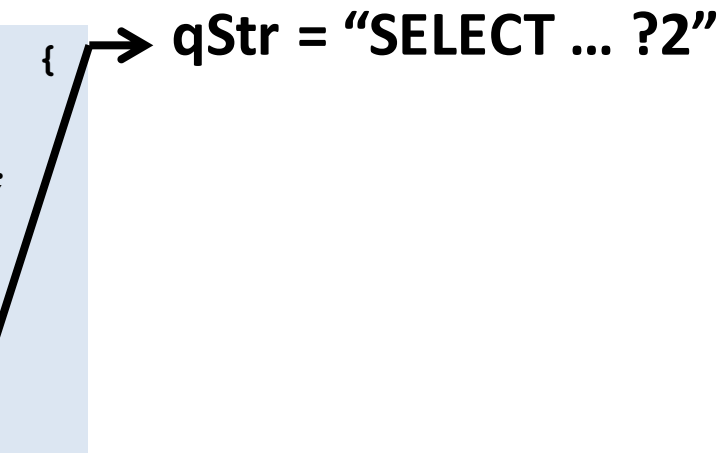
```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```



Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

qStr = "SELECT … ?2"

query : "SEL … ?2"
?1 : String
?2 : int

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

qStr = "SELECT … ?2"

query : "SEL … ?2"
?1 : String
?2 : int

qStr = "SELECT … ?1"

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

qStr = "SELECT … ?2"

query : "SEL … ?2"
?1 : String
?2 : int

qStr = "SELECT … ?1"

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

qStr = "SELECT … ?2"

query : "SEL … ?2"
?1 : String
?2 : int

qStr = "SELECT … ?1"

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

qStr = "SELECT … ?2"

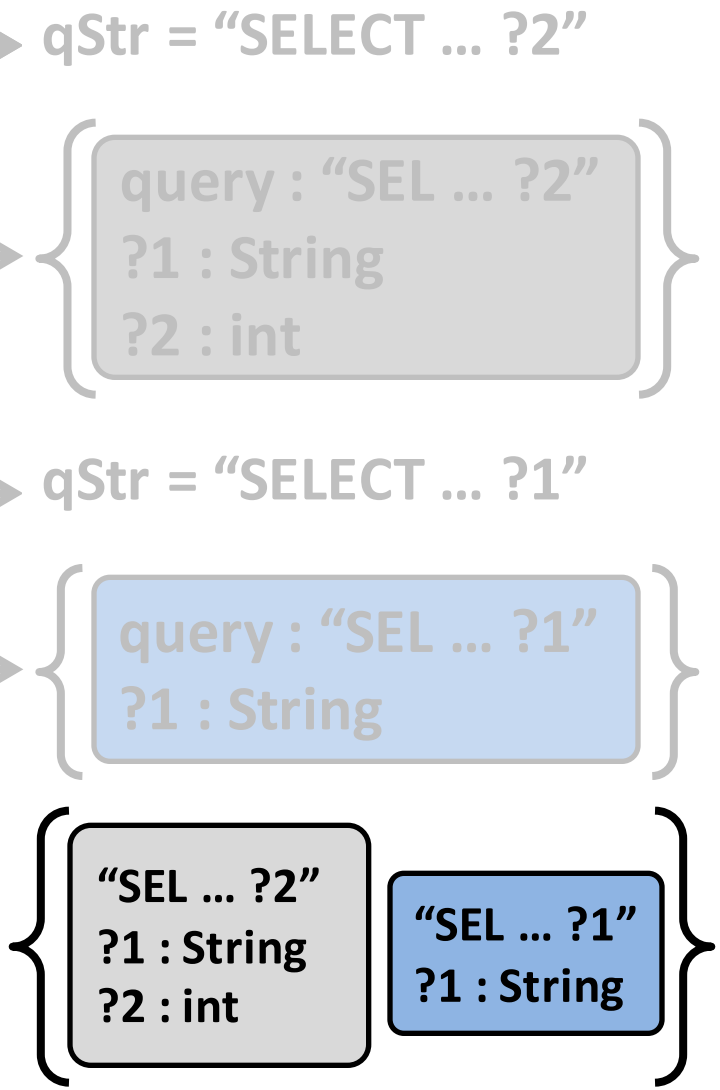
query : "SEL … ?2"
?1 : String
?2 : int

qStr = "SELECT … ?1"

query : "SEL … ?1"
?1 : String

Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```



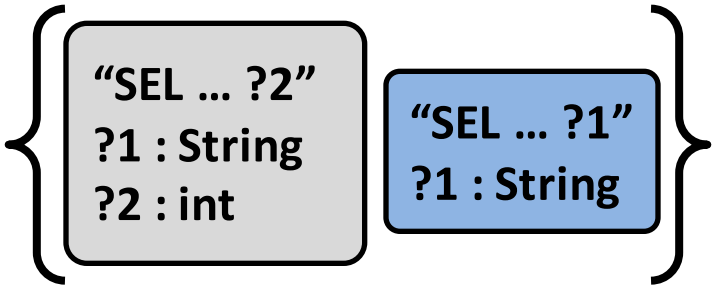
Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```

As before, for each bound query:

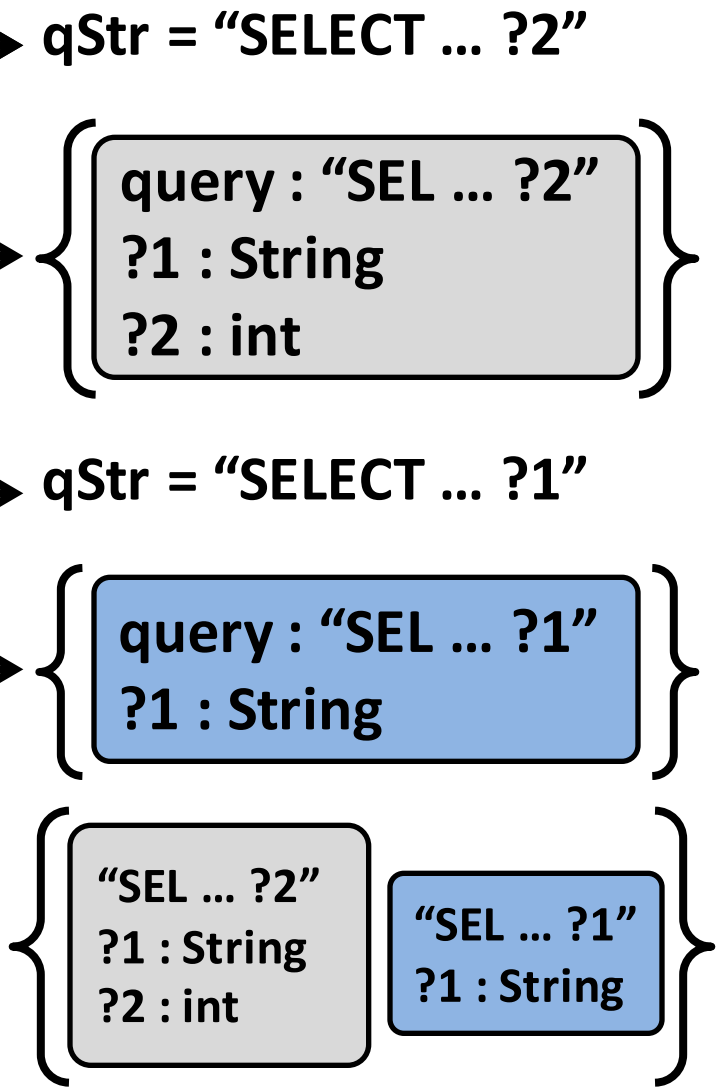
1. **Check param types**
2. **Check result type**

In general, we express Bound Query Analysis as a dataflow analysis.



Flow Sensitivity

```
String getText(String id, Link link) {
  String qStr; Query q;
  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  if(link != null) {
    qStr += "AND w.link.id = ?2";
    q = createQuery(qStr);
    q.setParam(1, id);
    q.setParam(2, link.id);
  } else {
    q = createQuery(qStr);
    q.setParam(1, id);
  }

  Weblog w = (Weblog) q.execQuery();
  return w.text;
}
```



Loops

```
String getText(String id, Link link) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "OR w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Loops

```
String getText(String id, List<Link> links) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "OR w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Loops

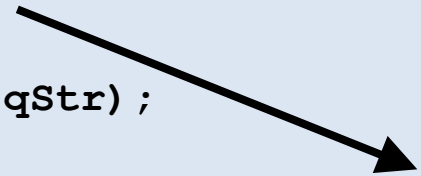
```
String getText(String id, List<Link> links) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";
  qStr += "OR w.link.id = ?2";

  q = createQuery(qStr);

  q.setParam(1, id);
  q.setParam(2, link.id);

  Weblog w = (Weblog) q.execQuery();

  return w.text;
}
```

Loops

```
String getText(String id, List<Link> links) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  for(int i = 0; i < links.size(); i++) {
    qStr += " OR w.link.id = ?" + i;
  }

  q = createQuery(qStr);

  ...
}
```

Loops

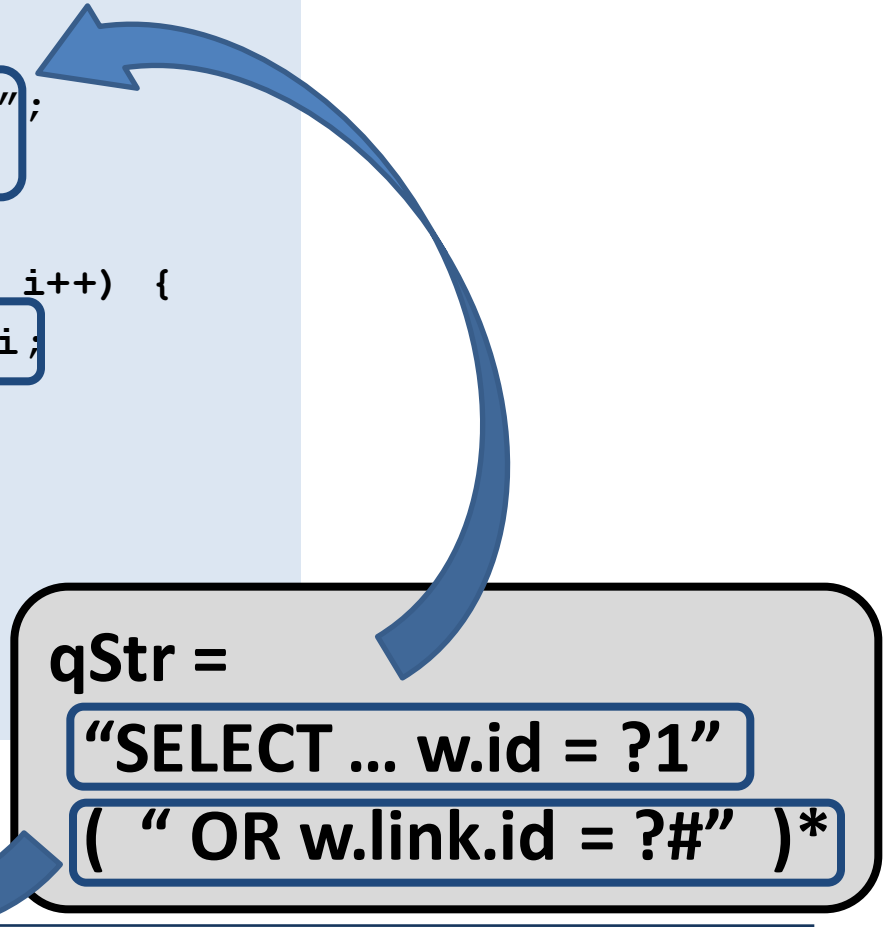
```
String getText(String id, List<Link> links) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  for(int i = 0; i < links.size(); i++) {
    qStr += " OR w.link.id = ?" + i;
  }

  q = createQuery(qStr);

  ...
}
```



qStr =
"SELECT … w.id = ?1"
(" OR w.link.id = ?#")*

Loops

```
String getText(String id, List<Link> links) {
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  for(int i = 0; i < links.size(); i++) {
    qStr += " OR w.link.id = ?" + i;
  }

  q = createQuery(qStr);

  ...
}
```



Loops

```
String getText(String id, List<Link> li
  String qStr;
  Query q;

  qStr  = "SELECT w FROM Weblog w ";
  qStr += "WHERE w.id = ?1 ";

  for(int i = 0; i < links.size(); i++)
    qStr += " OR w.link.id = ?" + i;
  }

  q = createQuery(qStr);

  ...
}
```

Deep Refactoring:

- know query structure
- know fragment locs
- refactor across loops

Deep Typechecking:

- unknown # of params
- do not check params
- can still check result

qStr =

"SELECT … w.id = ?1"

(" OR w.link.id = ?#")*

Multiple Methods

```
String mainQueryStr() {
  return "SELECT ... ?1";
}

Object getMain() {
  String qStr = mainQueryStr();

  Query q = createQuery(qStr);

  q.setParam(1, "main");

  return q.execQuery();
}

String mainId() {
  return ((Weblog) getMain()).id;
}
```

String Analysis :

- interprocedural
- compute regexps

Bound Query Analysis :

- intraprocedural
- no complex aliasing

Result Analysis :

- interprocedural
- propagate result type