

# Security and AOP

Patrick White

This is a story about Bob. Bob builds software.

**SOFTWARE THAT'S NOT  
SECURE**

But that can change

# **BOB HAS ENEMIES**

Users

Managers

Hackers

# **BOB HAS WEAPONS**

Design Analysis

Source Code Analysis

Dynamic Analysis

Hackers

# **HIS WEAPONS HAVE PROBLEMS**

Source Code Analysis

# **HIS WEAPONS HAVE PROBLEMS**

Application Scanning



# **HIS ENEMIES HAVE INCENTIVES**

Time

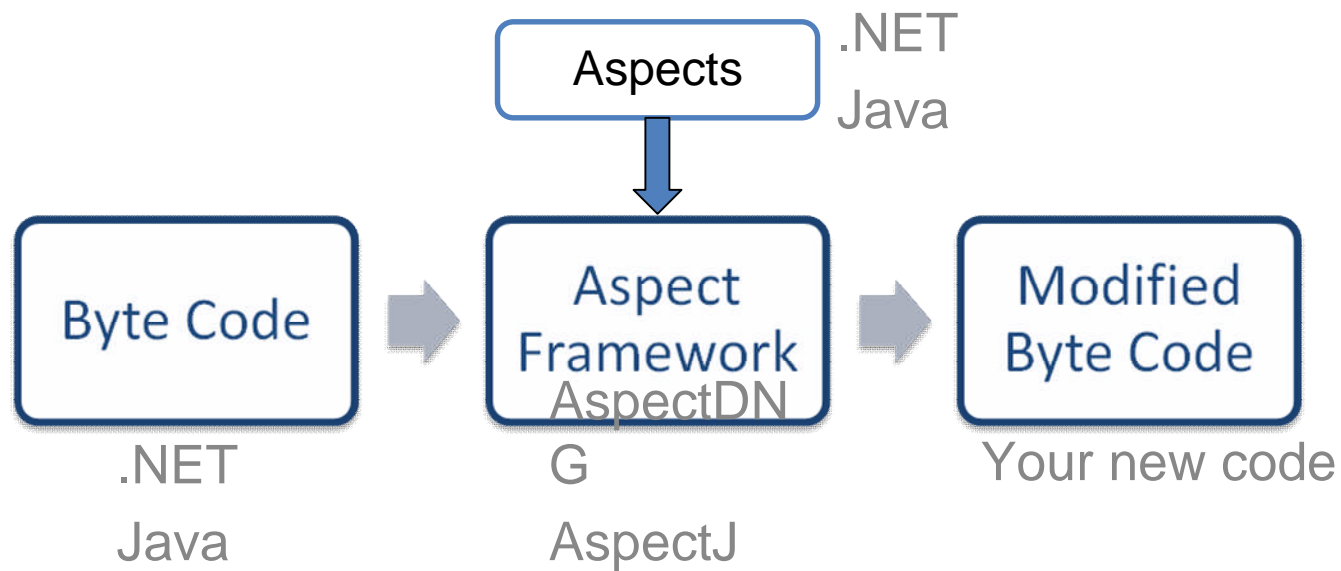
Money

Prestige

**BOB HAS A NEW WEAPON**

Aspect Oriented Programming

# AOP MEANS INJECTING CODE



# CODE INJECTION

```
String sql = "select * from tab where id=" + id +  
"";  
executeQuery(sql);
```

```
String sql = "select * from tab where id=" + id +  
"";  
executeQuery(sql);
```

```
String sql = "select stuff from mytable where id=" + id + "";  
MyLibrary.doCheck(sql);  
executeQuery(sql);
```

# AOP IS ABOUT...

Reusability

Out of cycle development

Functionality

# **2 THINGS FOR BOB**

Find Issues

Fix Issues

# **AOP TO FIND ISSUES**

Demo

# **AOP TO FIX ISSUES**

Demo



# **AOP TO FIX PROCESSES**

Out of Cycle Security  
Development

**QUESTIONS?**

Thanks a lot!