Best Practices:

Problem: Field level vulnerability:

*This rule makes sure that the code checks for access permissions before running a SOQL, SOSL, or DML operation.  
This prevents access to protected resources by users without the correct privileges.*

Solution:

Multiple ways.

public class Foo {

public void justGiveMeFoo() {

AggregateResult[] test = [SELECT Id FROM Opportunity]; **//Bad**: The resource is accessed without checking permissions.

}

public void giveMeFooSafely() {

if (**Opportunity.sObjectType.getDescribe().isAccessible()**) { **//Good:** Permissions are checked before any resources are accessed.

return;

}

AggregateResult[] test = [SELECT Id FROM Opportunity];

}

public void giveMeFooSafelyWithEnforcedSecurity() {

AggregateResult[] test = [SELECT Id FROM Opportunity WITH SECURITY\_ENFORCED]; **//Good**: Permissions are checked using the **WITH SECURITY\_ENFORCED** clause

}

}

2.