Java
Exceptional Behavior (ERR)

Mario Alviano

University of Calabria, Italy

A.Y. 2016/2017

Do not suppress or ignore checked exceptions

- ✗ Printing the stack trace is good for debugging, not for the release bytecode
- ✓ Properly handle exceptions
- ✓ Propagate exceptions when you cannot handle them

```
https://www.securecoding.cert.org/confluence/
display/java/ERR00-J.+Do+not+suppress+or+ignore+
checked+exceptions
```

Do not allow exceptions to expose sensitive information

- ✗ Don’t print that stack trace!
- ✓ Give back to the user only unsensitive information
- ✓ Provide details to a secure logger

```
https://www.securecoding.cert.org/confluence/
display/java/ERR01-J.+Do+not+allow+exceptions+to+
expose+sensitive+information
```

Prevent exceptions while logging data

- ✗ Are you still thinking to print that stack trace to STDERR?
- ✓ Use a proper logger library
- ✓ For example, `java.util.logging.Logger` or `log4j`

```
https://www.securecoding.cert.org/confluence/
display/java/ERR02-J.+Prevent+exceptions+while+
logging+data
```

Restore prior object state on method failure

- ✗ Do not leave inconsistent states
- ✓ Validate before modification of state
- ✓ Rollback on failures
- ✓ Modify temporary copies, then replace the original object

```
https://www.securecoding.cert.org/confluence/
display/java/ERR03-J.+Restore+prior+object+state+
on+method+failure
```

Do not complete abruptly from a finally block

- `finally` is executed in any case
- ✗ A `return`, `break` or `continue` will terminate `finally`, discarding any exception in the `try` block
- ✓ Handle exceptions in a `catch` block
- ✓ Move any `return` after the `finally` block

```
https://www.securecoding.cert.org/confluence/
display/java/ERR04-J.+Do+not+complete+abruptly+
from+a+finally+block
```

Do not let checked exceptions escape from a finally block

- ✓ Handle any possible exception inside `finally` blocks
- ✓ Use try-with-resources blocks (Java 7)

```
https://www.securecoding.cert.org/confluence/
display/java/ERR05-J.+Do+not+let+checked+
exceptions+escape+from+a+finally+block
```

Do not throw RuntimeException, Exception, or Throwable

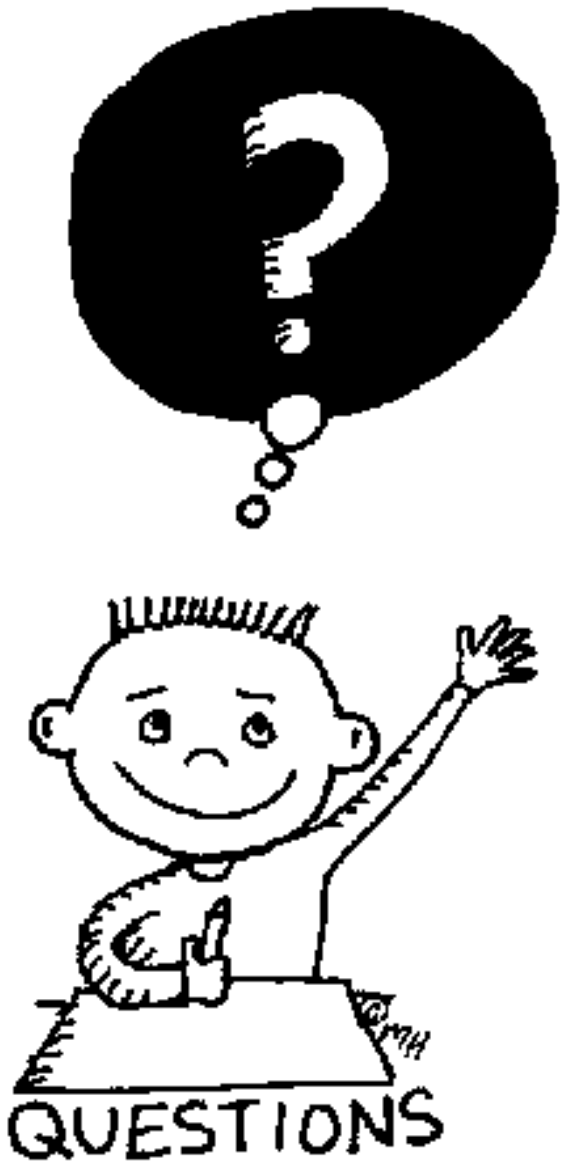
- ✗ These are really generic exceptions
- ✓ Try to be specific
- ✓ Subclass `Exception` or `RuntimeException`

```
https://www.securecoding.cert.org/confluence/
display/java/ERR07-J.+Do+not+throw+
RuntimeException%2C+Exception%2C+or+Throwable
```

Do not catch NullPointerException or any of its ancestors

- ✗ Do you really know how to handle all kinds of exceptions?
- ✗ A `NullPointerException` may be raised in several points of a block
- ✓ Handle specific exceptions

```
https://www.securecoding.cert.org/confluence/
display/java/ERR08-J.+Do+not+catch+
NullPointerException+or+any+of+its+ancestors
```



END OF THE LECTURE