? CODE QUIZ: SMALL BUG – BIG IMPACT

BTPEX SRM DEVELOPER FORUM

“All bugs in this presentation are based on actual events.” 🐞🎬

You litteraly could say:

> *“The following code has actually taken down rockets, banks, and billions.”* 💥

DISCLAIMER

Yes, this is exaggerated. No, it’s not that unrealistic.

Some examples were intentionally created or adapted for this presentation to illustrate real-world issues. In some cases, the original incidents are not publicly documented or are under NDA.

QUIZ

```
if ((err = SSLVerify(...)) != 0)
    goto fail;
    goto fail;
```

? What's the issue on this c Code?

✅ FIX

```
if ((err = SSLVerify(...)) != 0)
    goto fail;
```

delete second goto

QUIZ: APPLE "GOTO FAIL" (2014)

⚠️ IMPACT

- SSL certificate verification skipped
- Affected iOS and macOS
- Allowed MitM attacks over HTTPS
- Shook public trust in Apple security

Source

QUIZ

```
ecs-cli down --cluster "s3-*"
```

? What went wrong with bash command?

✅ FIX

```
# Intended:
ecs-cli down --cluster "s3-a"
# Actual:
ecs-cli down --cluster "s3-*"
```

eliminate wildcard on input agrument

✅ ADDITIONAL FIX

```
read -p "Confirm cluster: $CLUSTER_NAME? (yes/no): " ans
[[ "$ans" != "yes" ]] && exit 1
```

☁️ QUIZ: AWS S3 OUTAGE (2017)

⚠️ IMPACT

- Disabled entire region’s S3 infrastructure
- Took down major platforms: GitHub, Slack, Trello
- Estimated economic loss in the hundreds of millions

Source

💥 QUIZ

```
double time = t * 0.1;  // using fixed-point approximation
```

❓ Why is this dangerous in long-running systems?

✅ FIX

```
uint64_t ticks = t;
double time = ticks * 0.1;  // use precise conversion
```

💥 QUIZ: PATRIOT MISSILE DRIFT (1991)

⚠️ IMPACT

- System time drifted ~0.34s after 100h
- Caused missile defense failure
- 28 soldiers killed in attack

Source

💼 QUIZ

```
balance = Math.round(balance * 100) / 100.0;
```

? What's the risk with this rounding logic?

✅ FIX

```
int balanceCents = depositCents - withdrawalCents;
```

💼 QUIZ: HORIZON ACCOUNTING SCANDAL

⚠️ IMPACT

- 700+ postmasters falsely accused and convicted
- Based on flawed accounting system
- Legal battle, reputational damage, ruined lives

> *to be fair: this was just one small issue – there were over 28 financial relevant bugs in the software!*

Source

QUIZ

(FICTIONAL JAVA EXAMPLE)

```java
public class Config {
    private String databaseUrl;
    public String getDatabaseUrl() {
        return databaseUrl;
    }
}

public class App {
    public static void main(String[] args) {
        Config config = new Config();
        System.out.println("DB: " + config.getDatabaseUrl().toLowerCase());
    }
}
```

? What might happen during the execution?

✅ FIX

```
public class App {
    public static void main(String[] args) {
        Config config = new Config();

        if (config.getDatabaseUrl() == null || config.getDatabaseUrl().isEmpty()) {
            throw new IllegalArgumentException("Missing database URL");
        }

        System.out.println("DB: " + config.getDatabaseUrl().toLowerCase());
    }
}
```

☁️ QUIZ: GOOGLE CLOUD OUTAGE (2025)

⚠️ IMPACT

- Global services went offline
- Due to unvalidated critical config fields (null / empty check)
- Highlighted fragility of cloud infrastructure

Source

> *Google Incident Report: "The issue with this change was that it did not have appropriate error handling nor was it feature flag protected. Without the appropriate error handling, the null pointer caused the binary to crash."*

 QUIZ

```
CATIA V4 (german team)
CATIA V5 (french team)
```

? What’s the risk of using different CAD tools?

⚠️ PROBLEM

```
CATIA V4: cable = 1000 mm
CATIA V5: required = 1001 mm
```

✅ FIX

- Standardize to CATIA V5
- Validate full digital mockups (DMU)
- Sync ECAD–MCAD data across teams

✈️ QUIZ: AIRBUS A380 – CAD VERSION MISMATCH

⚠️ IMPACT

- 530 km of cabling incorrect
- Massive rework, 2-year delay
- Billions of euros in cost

Source

QUIZ

```java
try {
    Connection conn = dataSource.getConnection();
    // processing code that throws an exception...
    conn.close();
} catch (Exception e) {
    logger.error("Failure", e);
}
```

? What's the critical mistake in this try block?

✅ FIX

```
Connection conn = null;
try {
    conn = dataSource.getConnection();
    // work with conn
} catch (Exception e) {
    logger.error("Failure", e);
} finally {
    if (conn != null) {
      try {
        conn.close();
      } catch (SQLException ignore) {
        // handle / log closing-issue
      }
    }
}
```

✅ EVEN BETTER FIX

```
try (Connection conn = dataSource.getConnection()) {
    // safe processing
} catch (Exception e) {
    logger.error("Failure", e);
}
```

☕ QUIZ: SAP HANA JAVA CONNECTION LEAK (~2017)

⚠️ IMPACT

- Happened in **SAP IoT context** under load
- Unclosed HANA connections accumulated silently
- After ~500 connections → **DB crashed**
- Crash occurred after ~15 min of runtime
- Required debug analysis across services and logs
- several ours of service outage for customers

[Source – Matthias memories]

🧠 KEY TAKEAWAYS

✅ Automated testing catches edge cases early
✅ Four-eyes principle for pull requests prevents human oversight
✅ Consistent tooling & formats reduce integration errors
✅ Config validation is as critical as code
✅ Legacy code reuse must be validated in new contexts
✅ Edge-case awareness (overflows, precision, units) is vital
✅ Communication across teams and systems prevents disasters
✅ Float ≠ money or time – use precise datatypes (Java)

🙌 THANKS FOR PLAYING!

BTPEX SRM DEVELOPER FORUM

🎯 Which failure surprised you the most? What could you bring into your daily development practice?