MOBB

And the Next Evolution of Application Security is... Automatic Remediation

Eitan Worcel
March 2, 2023

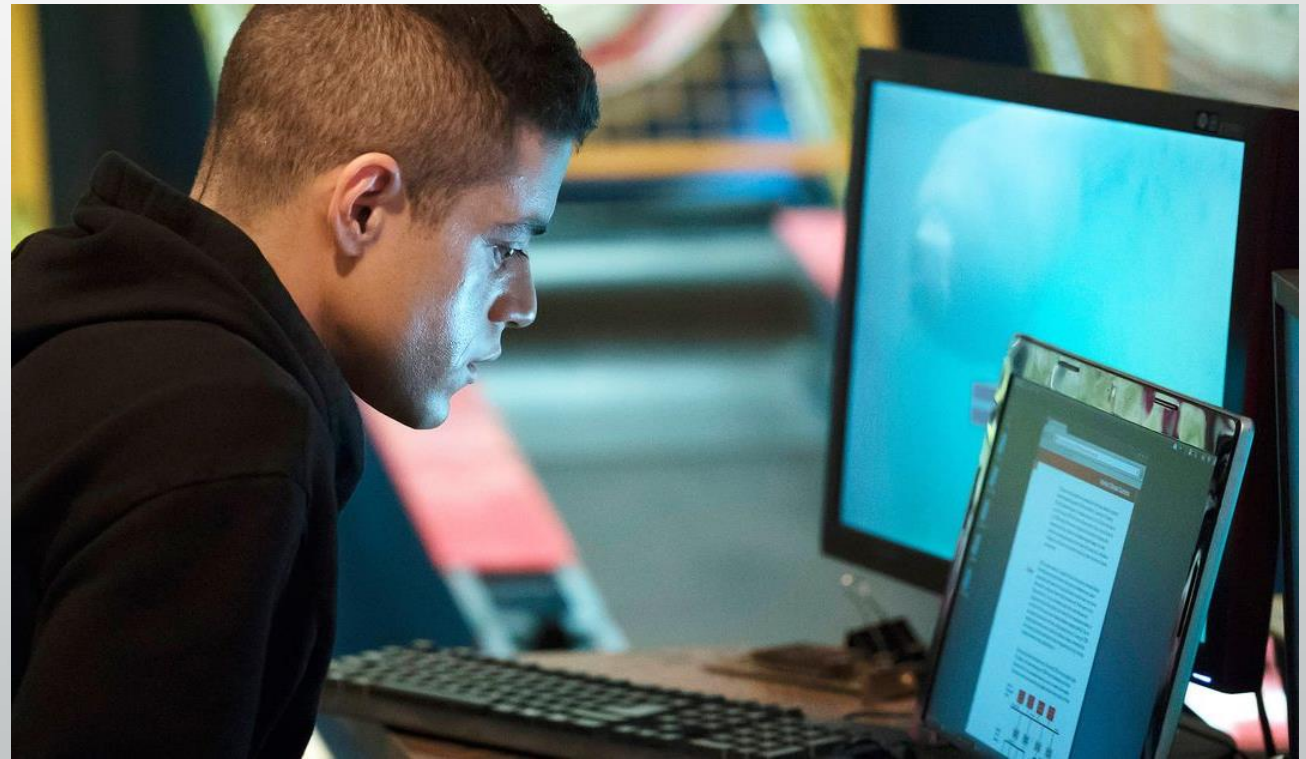
About Me

- Born and raised in Israel
- Lives in Massachusetts with my wife, three kids, and three dogs
- Retired long-distance runner
- Over 20 years of experience in the software world
- In the appsec space since 2007
- Co-founder & CEO of Mobb

https://www.linkedin.com/in/worcel/

MOBB

AppSec History 101



MOBB

Before Common Era

SNOWFROC

Dev

Waterfall

Security

Small and rare number of penetration testers using manual techniques and custom-made tools

Outcome

Small number of vulnerabilities that developers needed to address and long development cycles to do that

The Industrial Revolution

Dev

Growing number of developers

Agile Manifesto

Security

AppSec teams used complex, commercial and open-source tools to automatically scan applications

Outcome

# of vulnerabilities grew, but development cycles were still long;

introduced some levels of risk management

MOBB

Information Age

SNOWFROC

Dev

Rapid growth in number of developers

DevOps

Open source → 3rd parties

APIs

Cloud Native

Security

Security Champions

DevSecOps

SCA

API Security Testing

CSPM

Outcome

Teams find even more security vulnerabilities with much-shortened development cycles.
Smart prioritization - reachability and exploitability

MOBB

Today's Dev Experience

The five stages of grief dealing with security results

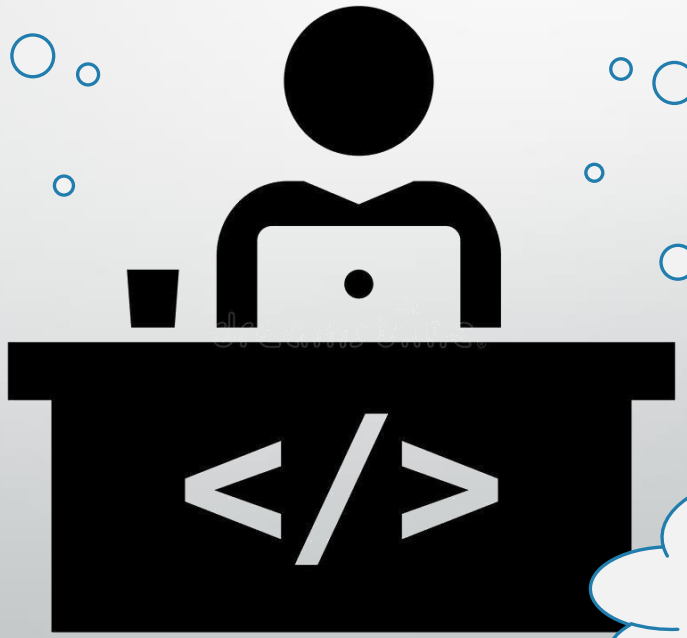
#1 **Denial**: My code is great, the tool is wrong

#2 **Anger**: This @$# security team is just hurting the business with its requirements and tools to justify its existence

#3 **Bargaining**: If you want me to look at the reported issues, don't expect to get XYZ feature delivered next week

#4 **Depression**: Sh!t, instead of doing something interesting and productive, I'm going to spend the day on this

#5 **Acceptance**: I will go and spend the time fixing this non-interesting, alleged security vulnerability for no good reason outside of CYA, but I'm not happy about it.



SNOWFROC

“A minute spent on fixing a security vulnerability is a minute not spent on driving the business forward”

Ori Bendet

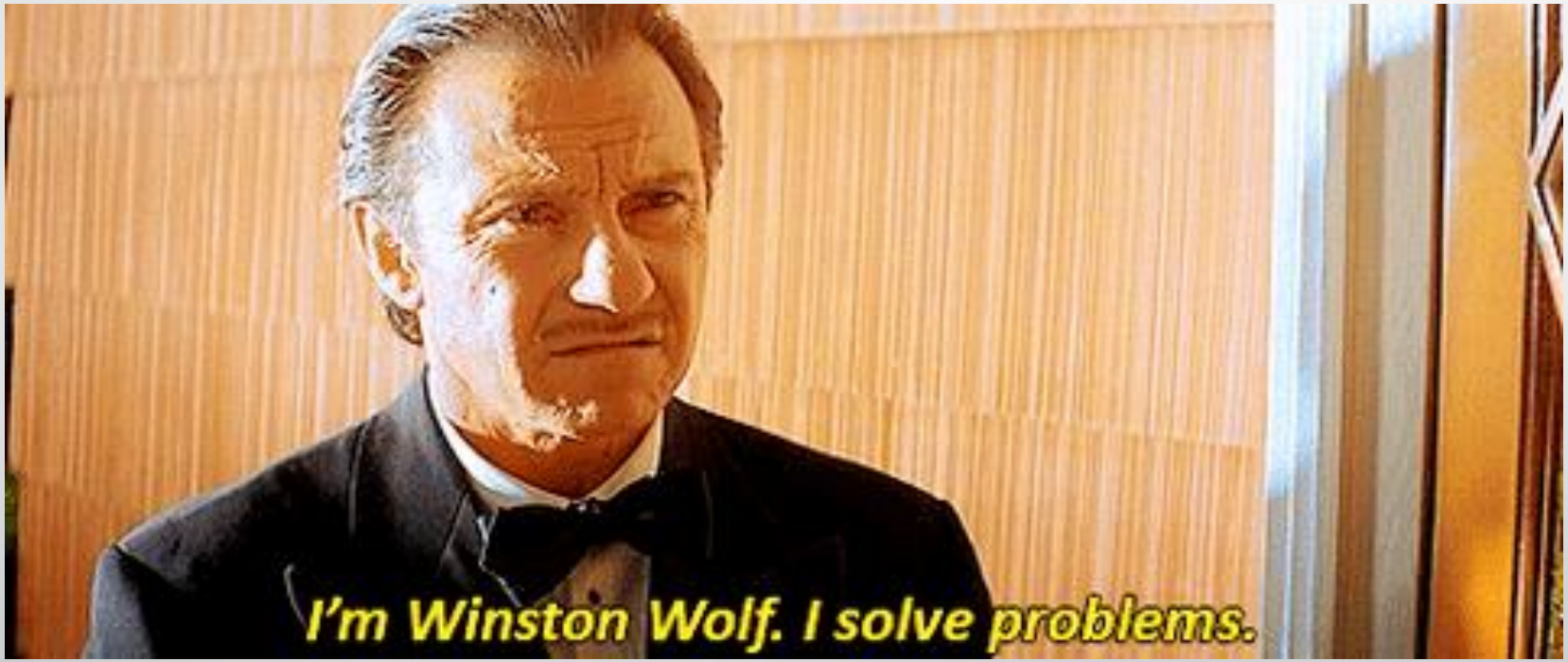
MOBB

With DevOps -

- x Remediating security vulnerabilities is not a resource problem.
- x Remediating security vulnerabilities is not a process problem.
- ✓ Remediating security vulnerabilities is a technological problem requiring security teams to make tough decisions until solved.

MOBB

SNOWFROC



MOBB

SNOWFROC

HERE I COME TO SAVE THE DAY!


Challenge

MOBB

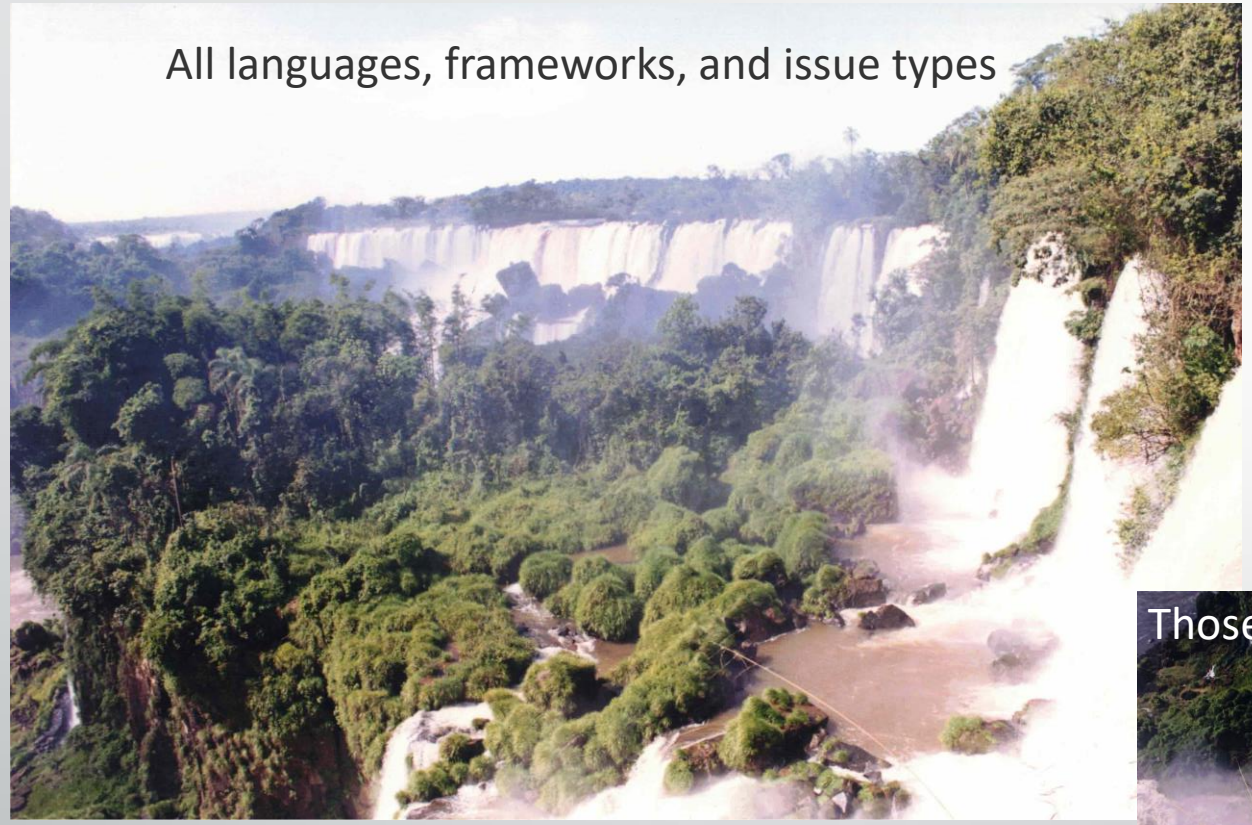
The Challenges

- **Technology**
  - Size of the problem (number of languages, frameworks, and different issue types)
  - False positives
  - Fixes need to meet different coding conventions and org limitations
  - Reported findings and the code will often miss information essential to a fix's correctness
  - Architecture and business logic vulnerabilities

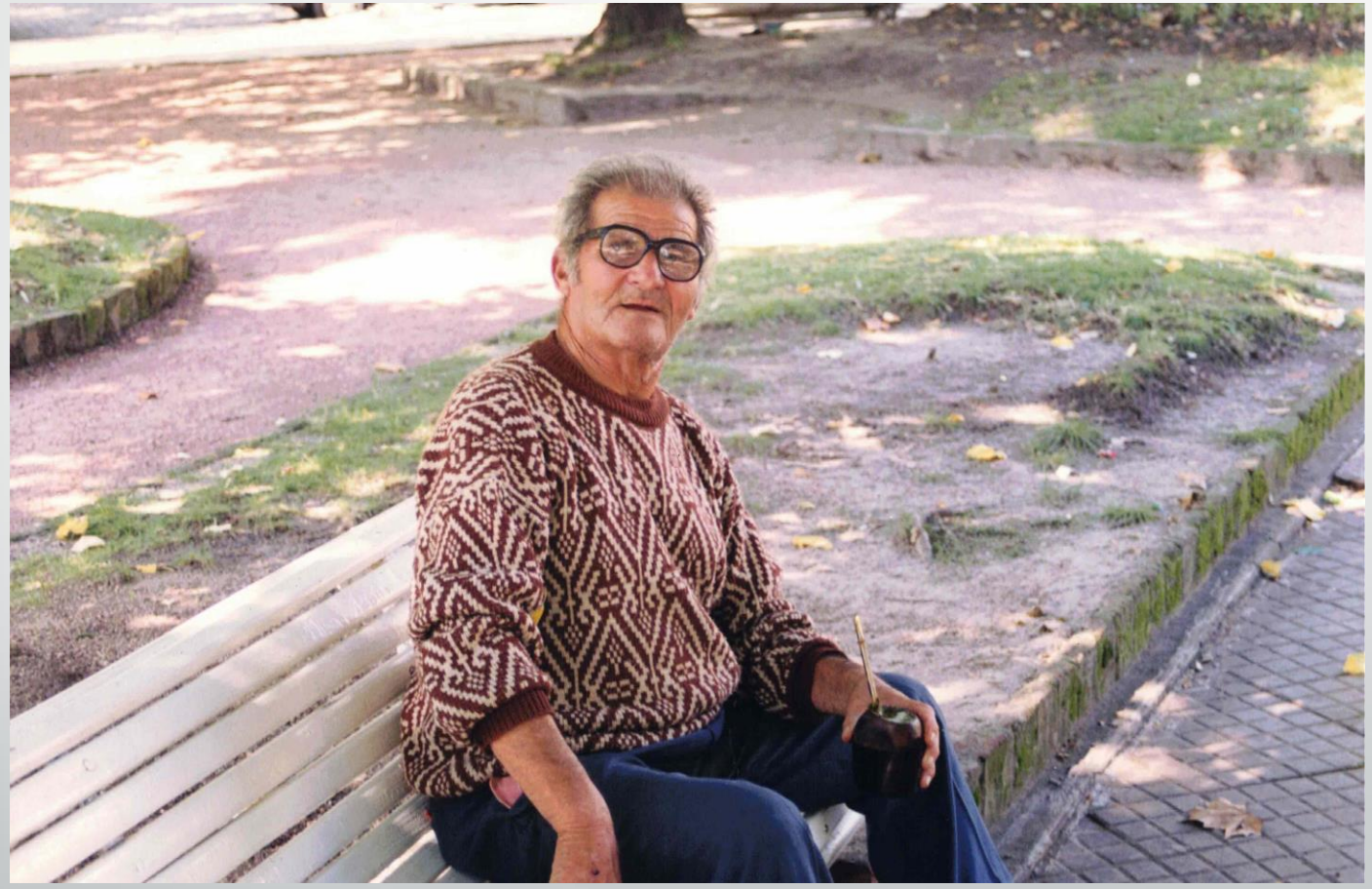
- **Developer bias**
  - Lack of trust in security tools and their findings from the start
  - Won't accept automatic code changes due to ego
  - Will wait in the corner to prove that the tool's suggestion broke their code

Why not simply use ChatGPT?

Size of the Problem

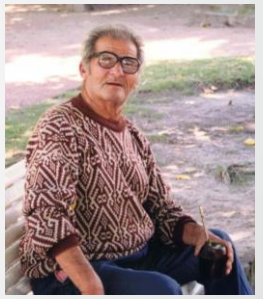


What is a False Positive?



Organization Policies

```java
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;

public class PingAction extends BaseController {

    private void doExecCommand() throws IOException {
        Runtime runtime = Runtime.getRuntime();
        String[] command = { "/bin/bash", "-c", "ping -t 5 -c 5 " + getAddress() };
        Process process = runtime.exec(command);
```



How can the tool know if org.apache.commons/commons-text maven dependency is or can be installed?

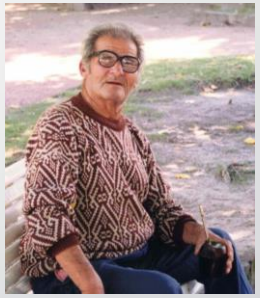
```java
import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import org.apache.commons.text.StringEscapeUtils;

public class PingAction extends BaseController {

    private void doExecCommand() throws IOException {
        Runtime runtime = Runtime.getRuntime();
        String[] command = { "/bin/bash", "-c", "ping -t 5 -c 5 " + StringEscapeUtils.escapeXSI(getAddress()) };
        Process process = runtime.exec(command);
```


18

Missing Context

```java
public void foo(String obj) {
    String query = "SELECT * FROM obj_table WHERE object = '" + obj + "'";
    try (Connection connection = dataSource.getConnection()) {
        try {
            Statement statement = connection.createStatement();
            ResultSet results = statement.executeQuery(query);
```

```java
public void foo(String obj) {
    String query = "SELECT * FROM obj_table WHERE object = ?";
    try (Connection connection = dataSource.getConnection()) {
        try {
            PreparedStatement statement = connection.prepareStatement(query);
            statement.setString(1, obj);
            ResultSet results = statement.executeQuery();
```



Do you want the tool to guess the parameter type?

Results | Messages

	TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	COLUMN_NAME	ORDINAL_POSITION	COLUMN_DEFAULT	IS_NULLABLE	DATA_TYPE
1	testDB	dbo	obj_table	objID	1	NULL	NO	int
2	testDB	dbo	obj_table	Description	2	NULL	YES	nchar
3	testDB	dbo	obj_table	Value	3	NULL	YES	nchar
4	testDB	dbo	obj_table	Catalog	4	NULL	YES	nchar
5	testDB	dbo	obj_table	Object	5	NULL	NO	date
6	testDB	dbo	obj_table	IsActive	6	((1))	NO	bit

MOBB

Architecture Changes

What About using ChatGPT?

Copy code

```
protected AttackResult injectableQueryAvailability(String action) {
    StringBuffer output = new StringBuffer();
    String sql = "SELECT * FROM access_log WHERE action LIKE ?";
    String parameter = "%" + action + "%";

    try (Connection connection = dataSource.getConnection()) {
        try {
            PreparedStatement statement = connection.prepareStatement(sql,
ResultSet.TYPE_SCROLL_INSENSITIVE, ResultSet.CONCUR_READ_ONLY);
            statement.setString(1, parameter);
            ResultSet results = statement.executeQuery();

            if (results.getStatement() != null) {
                results.first();
                output.append(SqlInjectionLesson8.generateTable(results));
                return failed(this).feedback("sql-
injection.10.entries").output(output.toString()).build();
            } else {
                if (tableExists(connection)) {
                    return failed(this).feedback("sql-
injection.10.entries").output(output.toString()).build();
                } else {
```

Microsoft warns employees not to share 'sensitive data' with ChatGPT

Eugene Kim Jan 31, 2023, 3:27 PM

https://www.businessinsider.com/chatgpt-microsoft-warns-employees-not-to-share-sensitive-data-openai-2023-1

21

MOBB

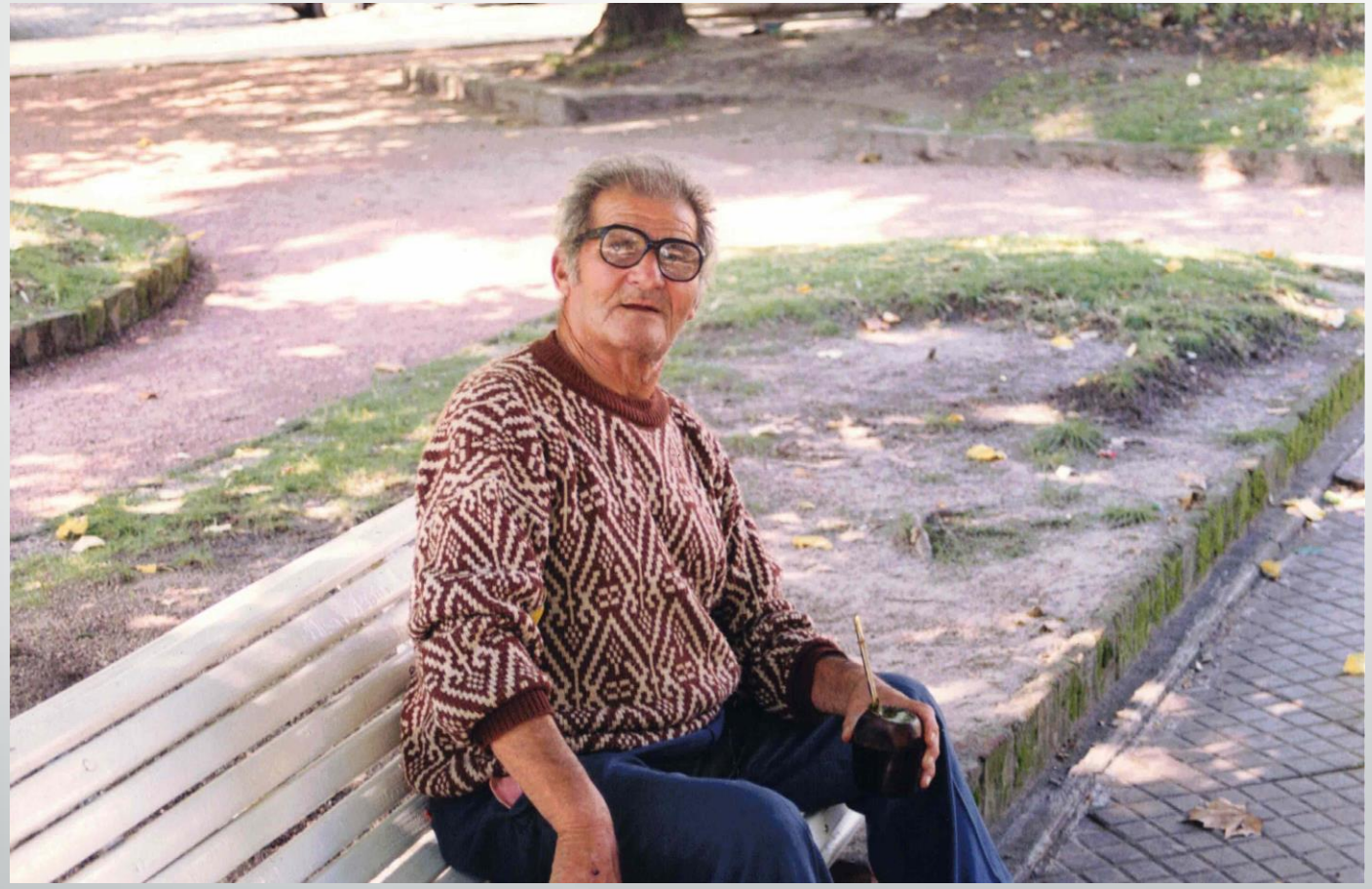
How to Get Ready?

SNOWFROC

- Improve automated testing coverage
- Set expectations
- Validate the fixes and give your stamp of approval
- Empower developers to automate fixes on their own
- Positioning, positioning, positioning

It is going to be an awesome ride

Questions?



Still Skeptical?