Differentiating the Pros and Cons of Automated Security Testing

Peter Mosmans
LEAD PENETRATION TESTER

@onwebsecurity https://www.onwebsecurity.com

Scenario

Maeve

“Is it something for us?”

Jennifer

“Let’s talk about the pros and cons first”

Module Overview

Advantages of automated security testing

Disadvantages of automated security testing

When it makes sense - and when not

Advantages of Automated Security Testing

Scalable

Repeatable

Automatically block builds when tests fail (gating)

Security becomes a habit, a standard in the development process

Test results can change over time even if the code doesn't change

Disadvantages of Automated Security Testing

Scans can take a long time

Tools are generic

False positives can get in the way

Configuring and maintaining relevant tests is a continuous cost

Security is not static, so test parameters should change over time

Not everything is a candidate for automated security testing

When Automated Security Testing Is Useful

Investment versus reward

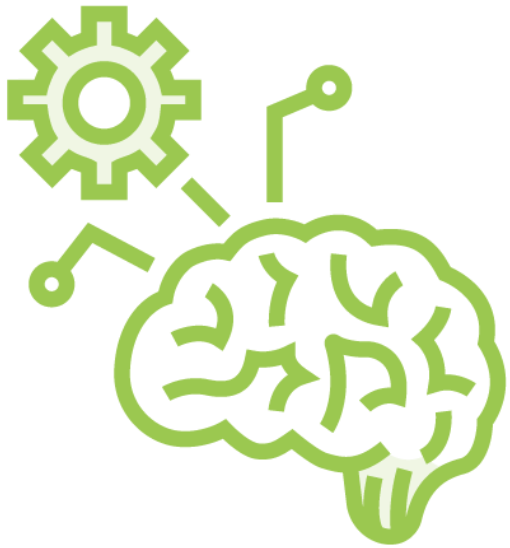
When delta scans are easy

To comply with standards

To get a security baseline

When Automated Security Testing Is Less Useful

Investment versus reward



Complex business rules

Fast-changing environments

Mix of frameworks and languages

Not All Tools Are Equal

- Use more than one tool for the same kind of test
- Let the team experiment with different tools
- Reporting format can make a difference
- Implement what works best for the team
- Facilitate, not mandate

Know what to do with non-compliancy results before implementing scans

Summary

No one-size fits all approach

Security is always a trade-off

- Costs vs. benefits

Always useful to comply with standards

Next Up

“I’m convinced”

Maeve

“I thought it might be a great fit.”

“Let’s look at what to test and where...”

“...and how to proceed further”

Jennifer