TestREx: a Testbed for Repeatable Exploits

Stanislav Dashevskyi, Daniel Ricardo Dos Santos,
Fabio Massacci, Antonino Sabetta

https://github.com/standash/TestREx

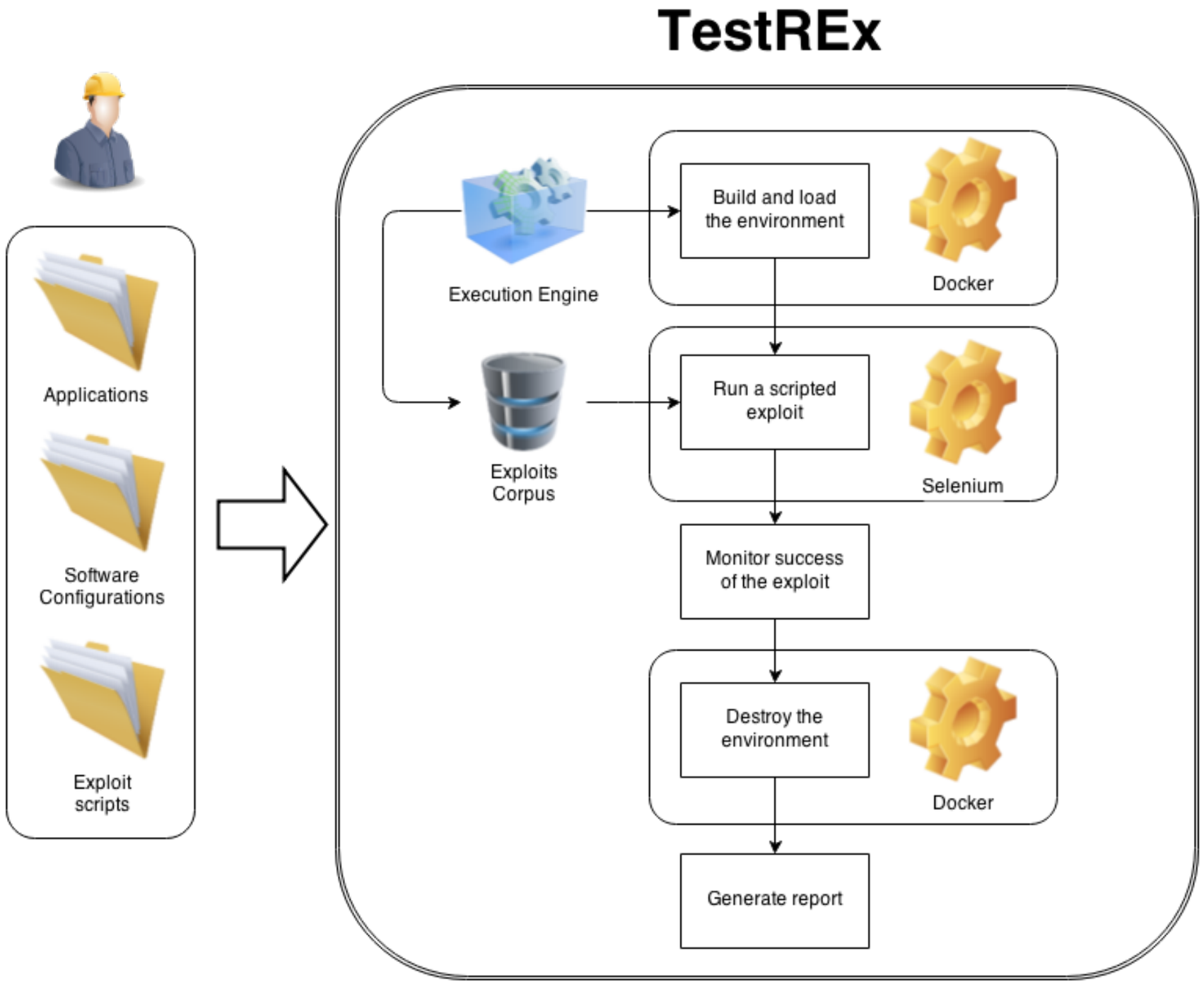
What's TestREx?

- Management system for software environments
  - Provides an isolated playground for every application and its corresponding software environment
- Testbed for performing web application vulnerability experiments
  - Run scripted exploits automatically
  - Give testers the access to a sandboxed application and let them play
- Test suite for managing and running scripted exploits against the corresponding applications

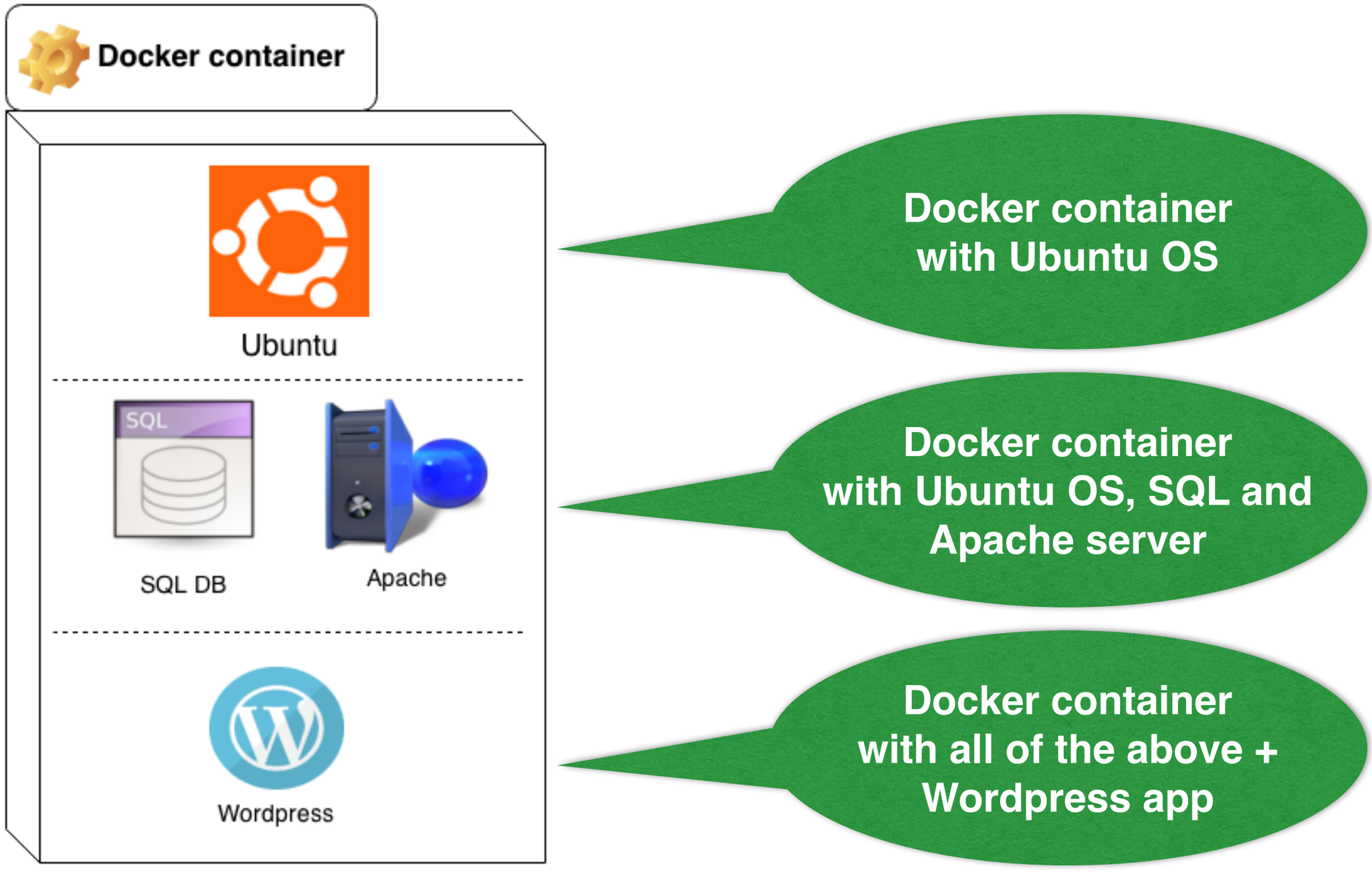
TestREx baseline

- Focus on web-facing code (Java/JavaScript)
- Built on top of existing approaches
  - BugBox by Nilson et al.
  - MalwareLab by Allodi et al.
- Objectives
  - Simple and modular architecture to deploy web apps
  - “Actionable” information on applications, software, and execution environments
  - Report successful and unsuccessful exploits

TestREx: workflow



How sandboxes are implemented?



Exploits (TestREx view)

- A sequence of [automated] actions required to subvert a vulnerability in and application and verify that subversion was successful
  - Self-contained unit test + metadata
  - Python scripts that use Selenium to automate browser and simulate attacker's actions
  - Scripts are controlled by Execution Engine of TestREx

Example application: *Nodegoat*

- An environment for learning how OWASP Top 10 security risks applied to Node.js web applications

- The goal is to demonstrate Node.js vulnerabilities that might be present in a real web application

- Demo site: http://nodegoat.herokuapp.com/

- Information: https://github.com/OWASP/NodeGoat#nodegoat

- Source code: https://github.com/OWASP/NodeGoat

Demo