

# Distributing Fuzz Test Cases

---



**Dr. Jared DeMott**

CTO AND FOUNDER

@jareddemott [www.vdalabs.com](http://www.vdalabs.com)



# Overview



## Distributed fuzzing

- Private
- Research/Open Source
- Commercial
- Closed, but now commercial

# Demo



## Peach community

- Parallel mode. You write the glue.



Closed

## Adobe

- <http://blogs.adobe.com/security/2012/05/a-basic-distributed-fuzzing-framework-for-foe.html>

## Google

- <https://security.googleblog.com/2011/08/fuzzing-at-scale.html>



## Cisco

- [http://blogs.cisco.com/cin/protocol\\_fuzzing\\_with\\_jimmy\\_ray](http://blogs.cisco.com/cin/protocol_fuzzing_with_jimmy_ray)

## More



FOE

 |  **Software Engineering Institute** | Carnegie Mellon University

[Work Areas ▾](#) | [Engage with Us](#) | [Training ▾](#) | [About Us ▾](#) | [News](#) | [Careers](#)

[Home](#) > [Vulnerability Analysis](#) > [Tools](#) > Failure Observation Engine (FOE)

[Overview](#)  
[Research](#)

## Failure Observation Engine (FOE)

The CERT Failure Observation Engine (FOE) is a software testing tool that finds applications that run on the Windows platform. FOE performs mutational fuzzing





## FOE Python wrapper

- Helped to coordinate FOE across multiple machines
- Pull seed files from a central location
- View status of fuzzing runs and results from the same location

# Research

## Fuzzpark

- <https://www.coseinc.com/en/index.php?rt=download&act=publication&file=A%20New%20Fuzzing%20Framework.pptx>

## Cyberfuzz

- [http://www.vdalabs.com/tools/DeMott\\_Dissertation.pdf](http://www.vdalabs.com/tools/DeMott_Dissertation.pdf)

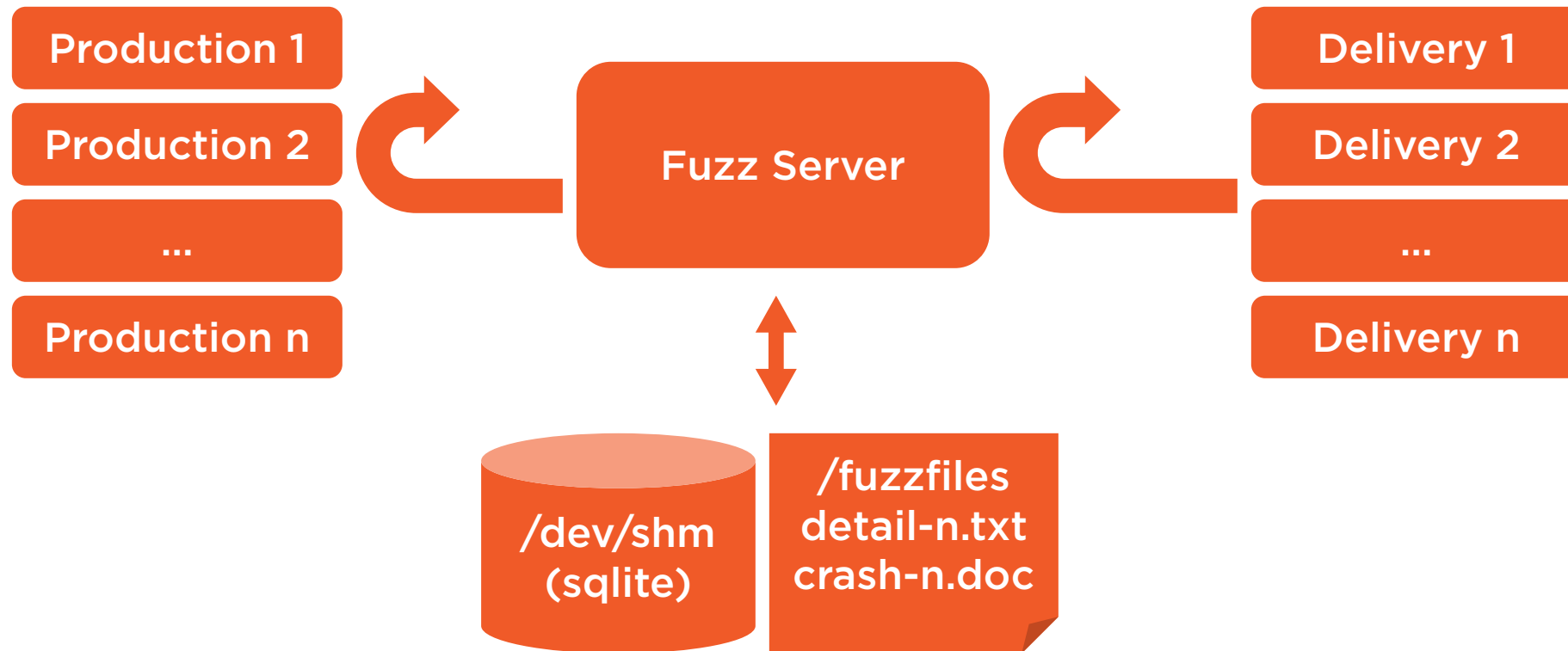
## KernelFuzzer

- <https://github.com/mwrlabs/KernelFuzzer>

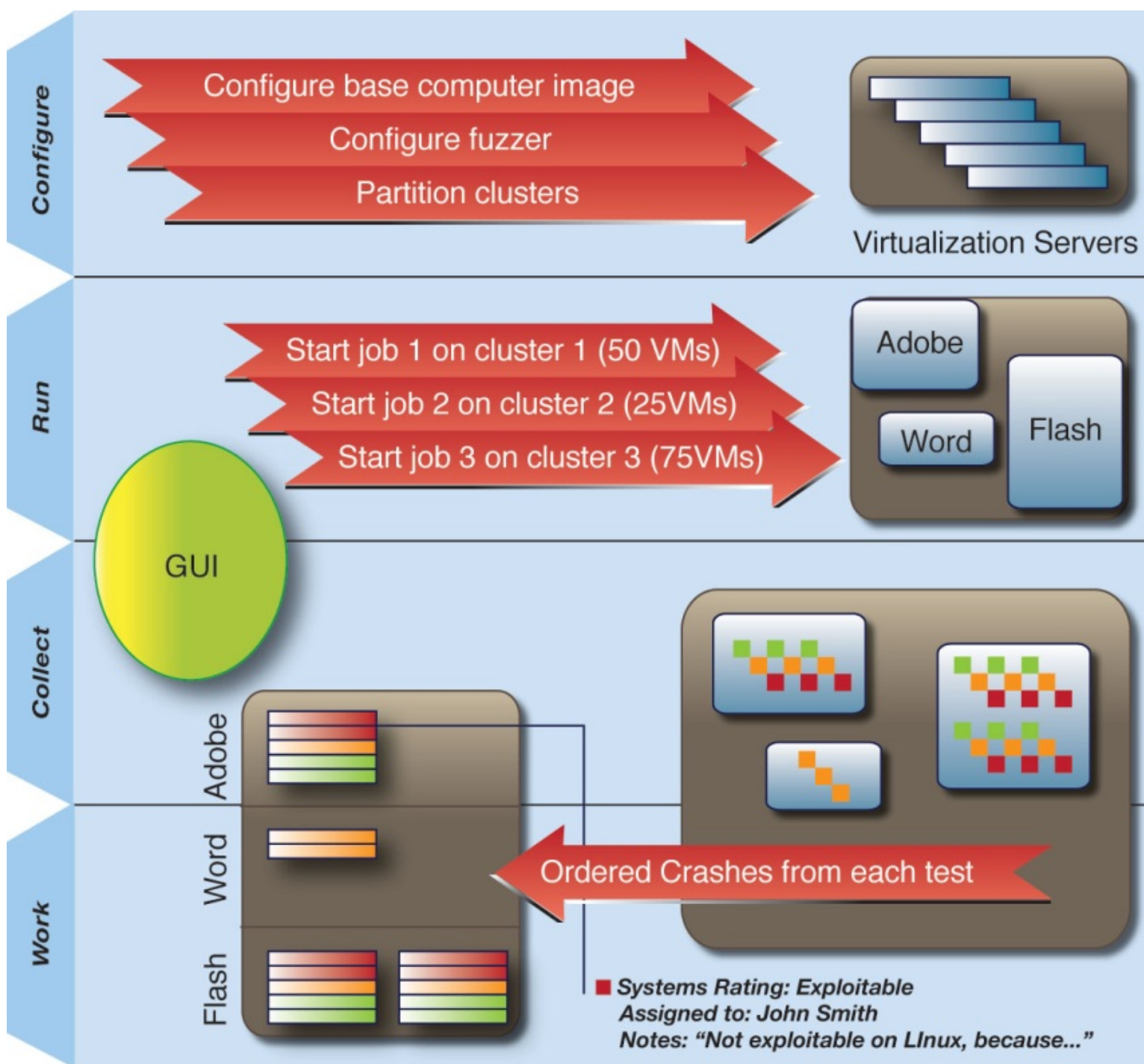
## Others

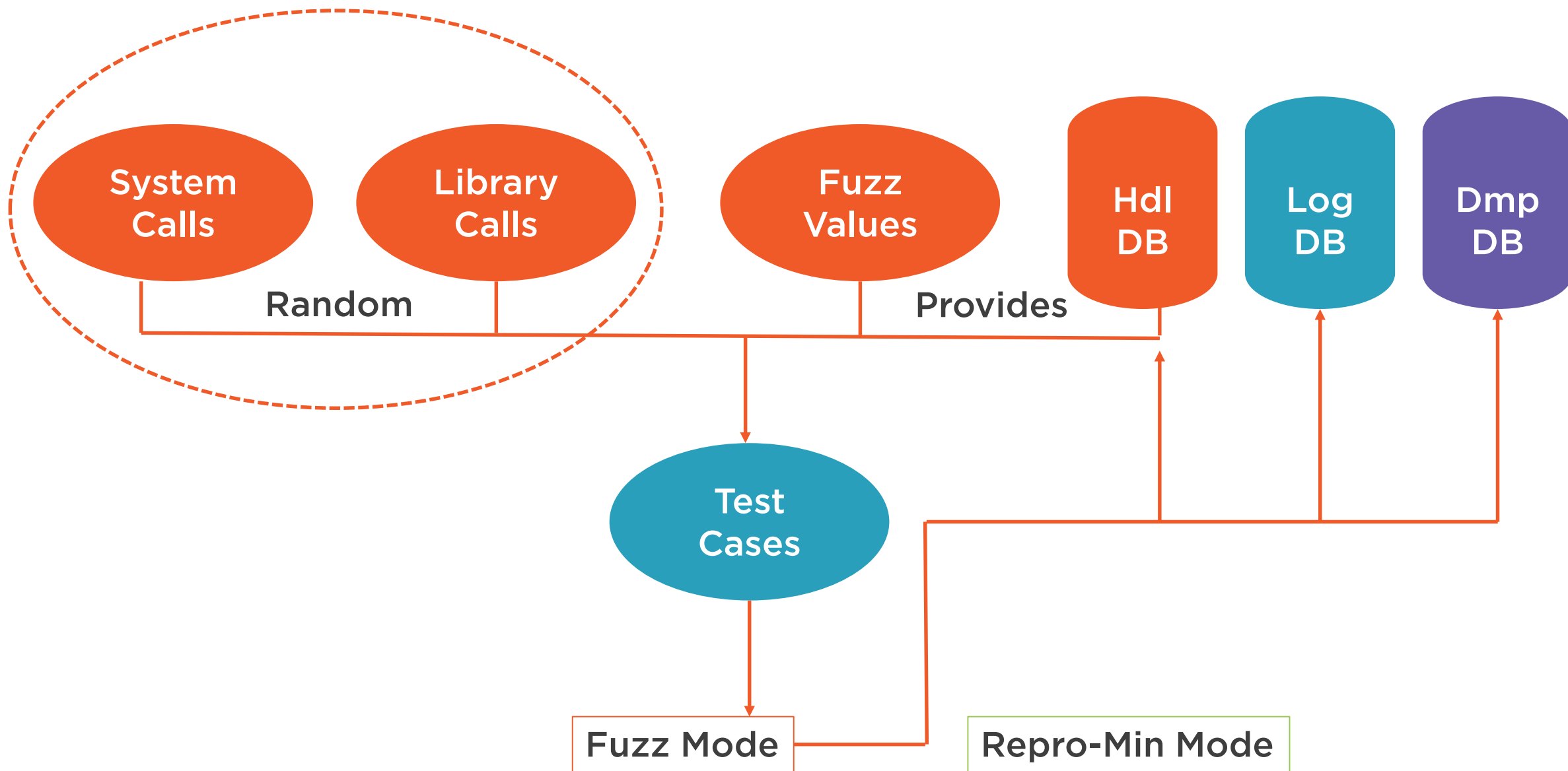
- <https://github.com/joxeankoret/nightmare>











Common

## Configure base OS

- gflags, verifier, bcdedit, etc.

## Cloud or on-prem VMs

## Implement via scripts

- Push jobs
- View job
- Verify results



# Commercial

## Synopsys

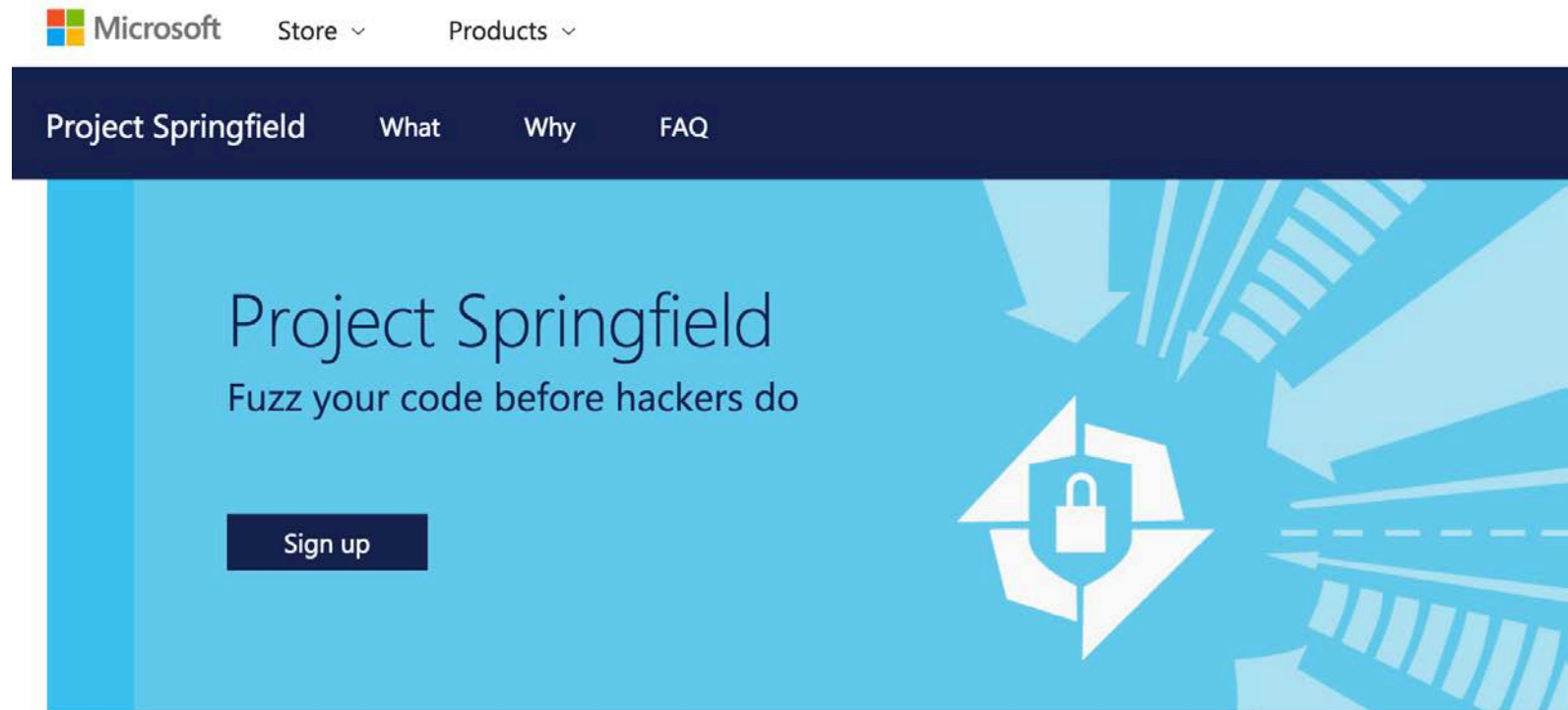
- <https://www.synopsys.com/software-integrity/products/intelligent-fuzz-testing.html>

## Peachfuzzer

- <http://www.peachfuzzer.com/>



Closed but  
Open to  
Commercial



<https://www.microsoft.com/en-us/springfield/>



# Summary



**Lots of machines equals less time**

**Other fuzzing topics**

- API