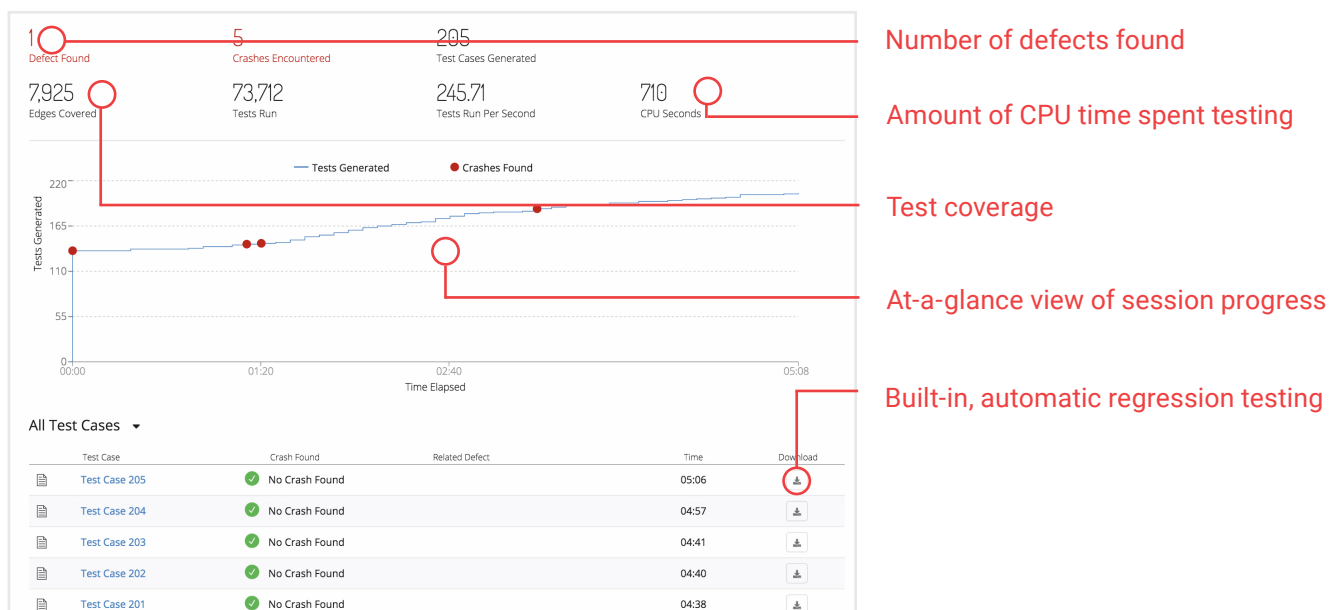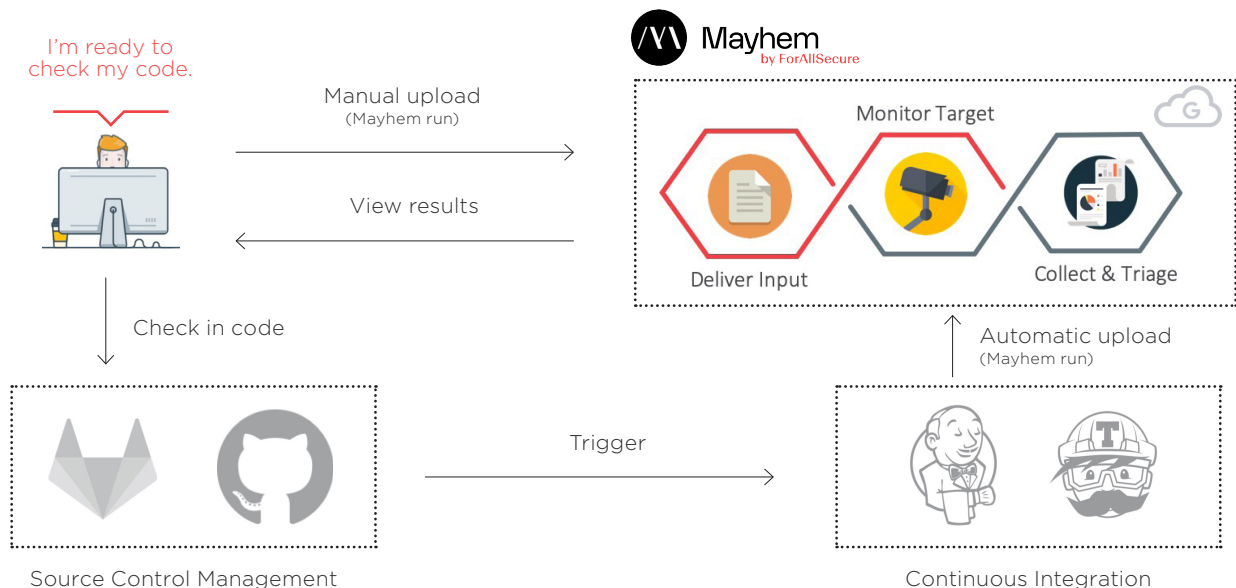# ForAllSecure

Mayhem

Making the World's Software Safe

Mayhem is an advanced fuzzer that combines the tried-and-true methods of guided fuzzing with the ingenuity of symbolic execution. At unprecedented speed, scale, and accuracy, Mayhem continuously uncovers defects. Deliver safe, secure, reliable software with less time, cost, and effort.

Number of defects found

Amount of CPU time spent testing

Test coverage

At-a-glance view of session progress

Built-in, automatic regression testing

	Test Case	Crash Found	Related Defect	Time	Download
	Test Case 205	✓ No Crash Found		05:06	⬇
	Test Case 204	✓ No Crash Found		04:57	⬇
	Test Case 203	✓ No Crash Found		04:41	⬇
	Test Case 202	✓ No Crash Found		04:40	⬇
	Test Case 201	✓ No Crash Found		04:38	⬇

How Does Mayhem Work?

Use Mayhem stand alone or within CI/CD environments

I'm ready to check my code.

Manual upload
(Mayhem run)

View results

Check in code

Mayhem
by ForAllSecure

Monitor Target

Deliver Input

Collect & Triage

Automatic upload
(Mayhem run)

Source Control Management

Trigger

Continuous Integration

What Makes Mayhem Unique?

Continuous, deep analysis.
Mayhem acquires intelligence of its targets over time. As Mayhem's knowledge grows, it deepens analysis, maximizes code coverage, and continues to uncover defects indefinitely.

Zero false-positives.
Mayhem dramatically reduces manual vulnerability management efforts. All findings reported by Mayhem are verified with a proof of defect.
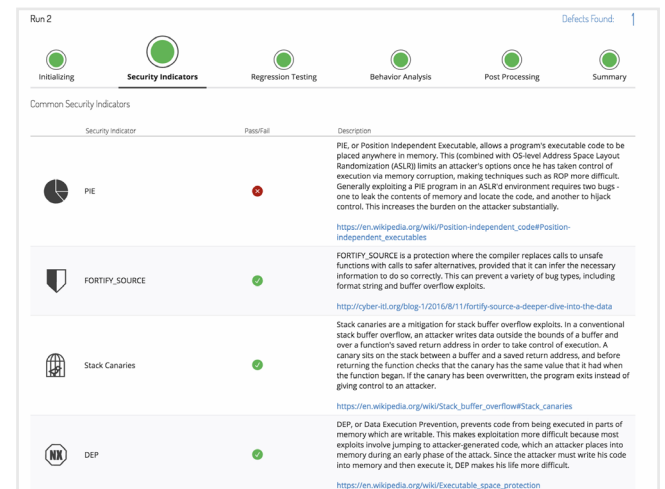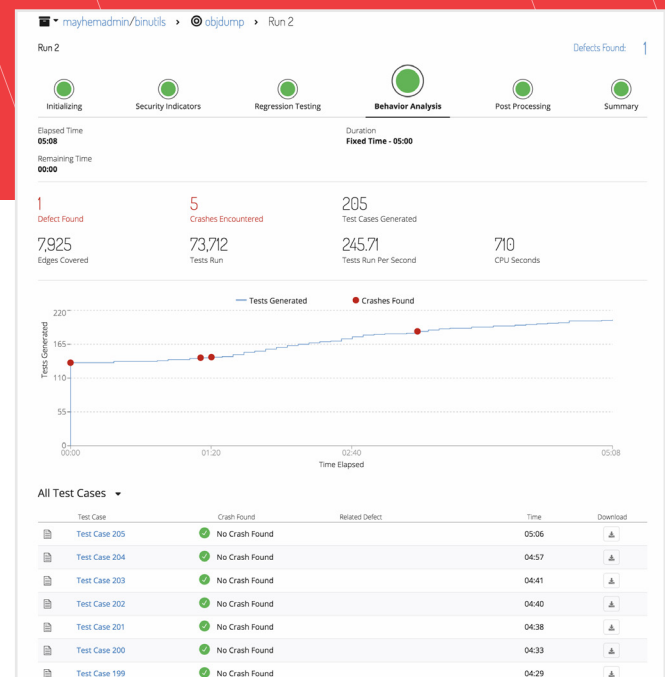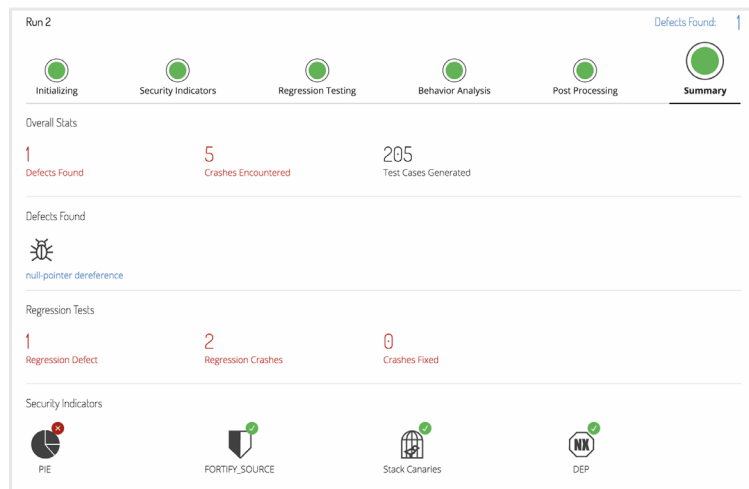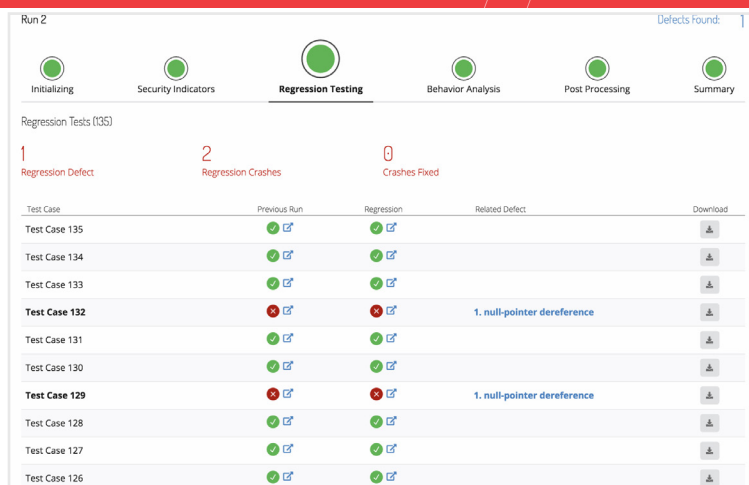
Autonomous test case generation.
Utilizing patented technology from a decade of research at CMU, Mayhem effectively and efficiently uncovers defects. Mayhem utilizes target feedback to custom generate test cases on-the-fly.
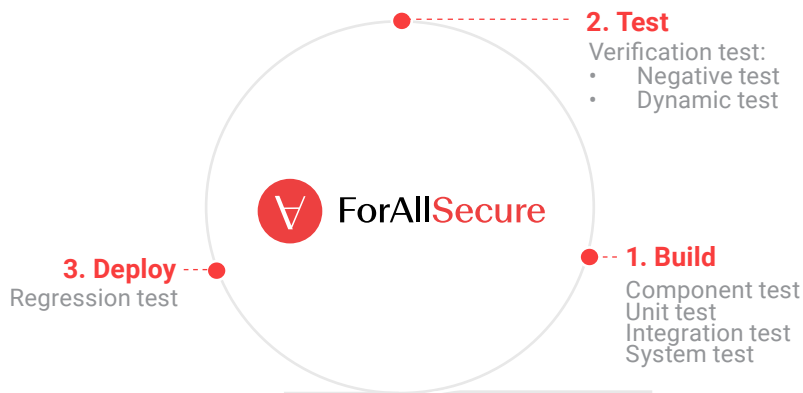
Shift-left in the SDL.
Mayhem shifts-left verification testing practices, such as dynamic analysis and fuzz testing, to help organizations control remediation costs. Mayhem plugs directly into CI pipelines to continuously test as part of DevOps workflows.

Manage the software supply chain.
Whether you rely on free open source or third-party code to build applications, Mayhem mitigates the risk inherited from unchecked software supply chains.

How is Mayhem Used?

2. Test
Verification test:
- Negative test
- Dynamic test

1. Build
Component test
Unit test
Integration test
System test

3. Deploy
Regression test

ForAllSecure

Mayhem is a continuous and scalable fuzzing solution that integrates into the development lifecycle.

Mayhem automates numerous secure development practices. Fuzz testing is an accepted component of defense-in-depth security testing programs.

Mayhem is proven. To date, Mayhem has uncovered over 20 critical vulnerabilities in MatrixSSL, MATIO, Das U-Boot, Netflix DIAL reference, OpenWRT, H20 server, and more!

Who Can Use Mayhem?

Mayhem is a versatile solution adopted within defense, aerospace, automotive, and high-tech industries.

Left-of-Ship

Left-of-ship customers use Mayhem to proactively secure the software they build.

- Autonomous test case generation dramatically reduces manual testing efforts.
- Accurate, actionable results elevate development, security, and QA productivity.
- Continuously mitigates inherited defects from vulnerable third-party and open source components.

Right-of-Ship

Right-of-ship customers use Mayhem to verify the software they use.

- Deliver safe, reliable services by verifying the security and resiliency of vendor code.
- Mayhem utilizes proven dynamic testing techniques that verify third-party and proprietary code.
- Reports contain test cases to enable enhanced collaboration across the supply chain.

The Department of Defense awarded ForAllSecure Mayhem a seven-figure, two-year contract to apply its cutting-edge technology to defense systems, including U.S. Navy ships and aircrafts.

What Does Mayhem Support?

Languages

C, C++, golang, Rust

Platforms

ARM, Linux, x86, x64

Open Source Fuzzer Interoperability

AFL
Honggfuzz
LibFuzzer

Target Interoperability

Binaries (full Linux executables)
Dockerized apps
Programs that read input from:
- Files
- TCP/UDP sockets
- stdin

DevOps

Travis CI, Jenkins, GitLab, GitHub

Mayhem Makes the World's Software Safe

ForAllSecure was founded on the mission to make the world's software safe. Utilizing patented technology from a decade of research at Carnegie e Mellon University, ForAllSecure delivers an advanced fuzz testing solution. Fortune 1000 companies in aerospace, automotive, and high-tech partner with ForAllSecure for scalable, autonomous security testing that keeps pace with increasing development speeds and deployment frequencies. DARPA deemed ForAllSecure the winner in the Cyber Grand Challenge, and MIT Technology Review named ForAllSecure in the 50 Smartest Companies list. Efficiently and effectively secure critical software with ForAllSecure.

For more information, visit www.forallsecure.com
To learn more, contact info@forallsecure.com

Winner of

DARPA

Named to

MIT Technology Review 50 SMARTEST COMPANIES

Exhibited at

Smithsonian