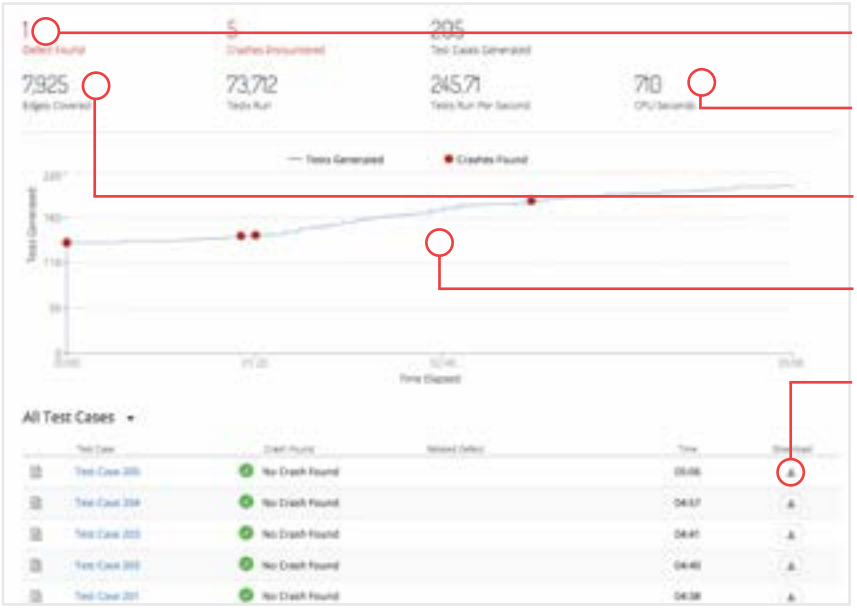
ForAllSecure

Mayhem

Continuous Security Built for Continuous Development

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

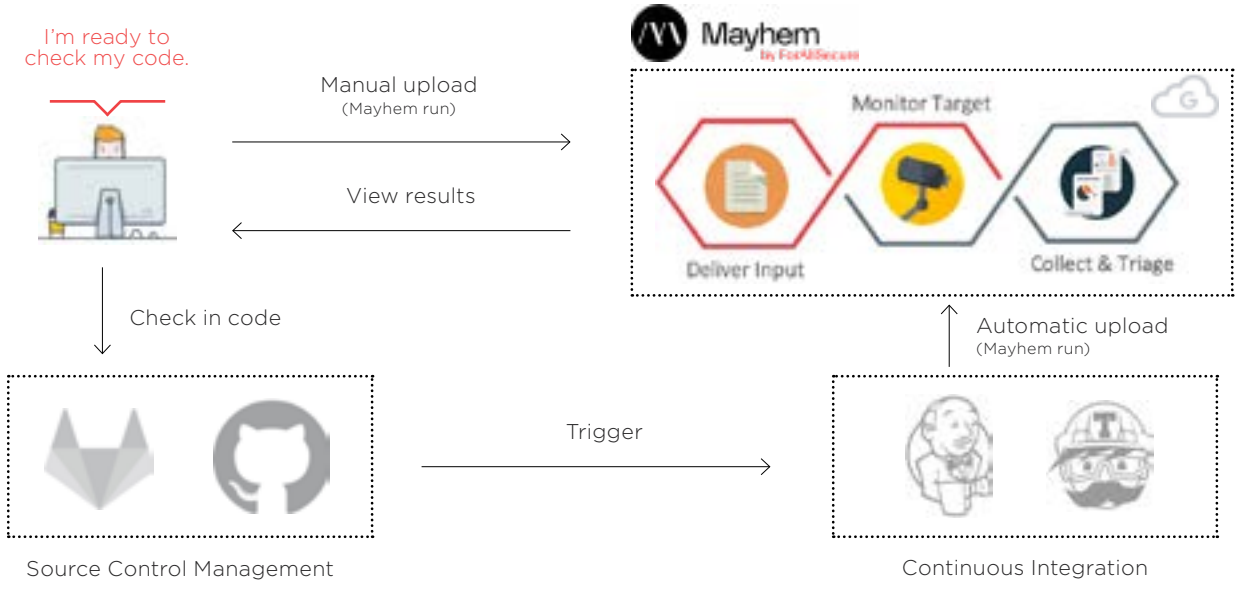
Test coverage

At-a-glance view of session progress

Built-in, auotmatic regression testing

How Does Mayhem Work?

Use Mayhem stand alone or within CI/CD environments



What Makes Mayhem Unique?

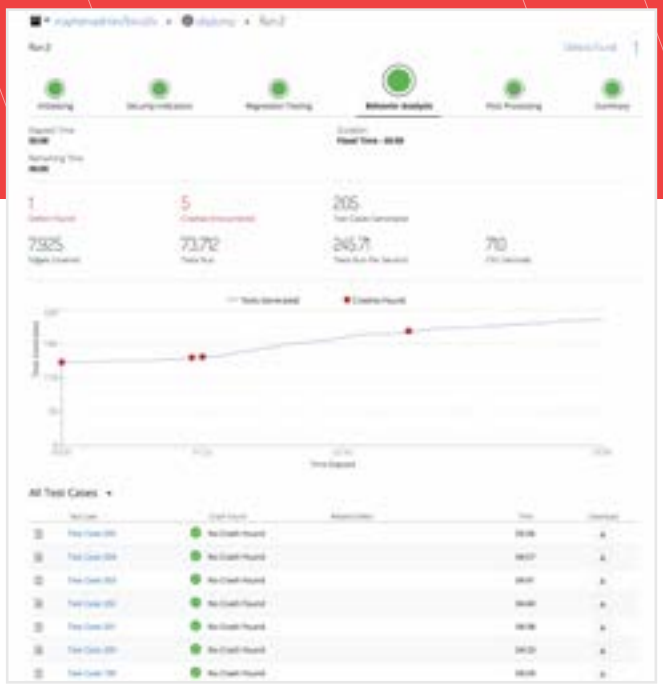
Continuous, deep analysis.
Mayhem acquires intelligence of its targets over time. As Mayhem's knowledge grows, it deepens analysis, maximizes code coverage, and continues to uncover defects indefinitely.

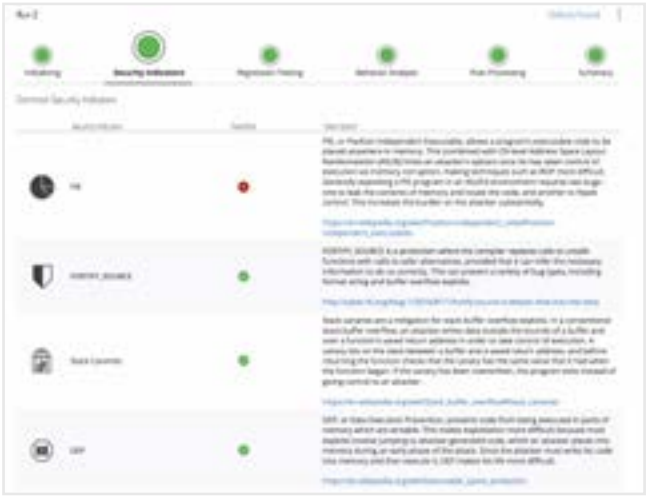
Zero false-positives.
Mayhem dramatically reduces manual vulnerability management efforts. All findings reported by Mayhem are verified with a proof of defect.

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.

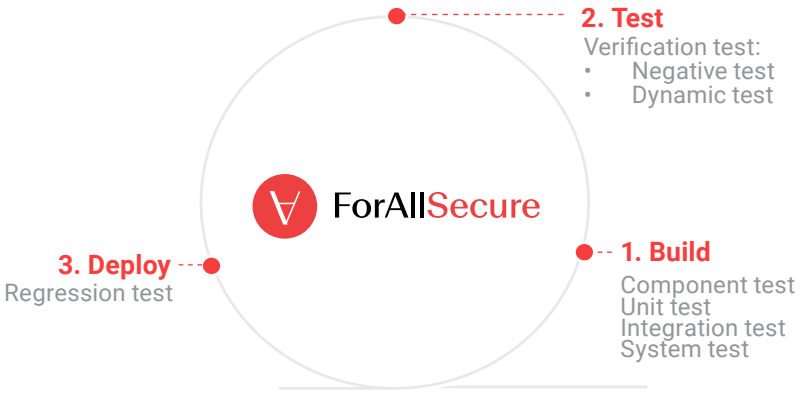
Shift-left in the SDL.
Mayhem shifts-left verification testing practices, such as dynamic analysis and fuzz testing, to help organizations control remediation costs. Mayhem plugs directly into CI pipelines to continuously test as part of DevOps workflows.

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?



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 popular open source components.

Why Mayhem?

Continuous fuzz testing is a recommended practice for organizations seeking to develop secure software. Fuzzing is well-documented for its effectiveness at verifying the quality, stability, and security of software. Since its inception, Mayhem has detected numerous critical vulnerabilities in popular open source components. See below for just a few of our most notable finds:

Netflix DIAL Reference
The DIAL server is commonly found in televisions to support online streaming services.

- CVE-2019-10028

Das U-Boot
Das U-Boot is a bootloader common in embedded devices, including Amazon Kindles, ARM Chromebooks, networking hardware, and more.

- CVE-2019-13103
- CVE-2019-13104
- CVE-2019-13105
- CVE-2019-13106

stb
stb is a suite of single-file C libraries containing utility functions useful to for computer graphics applications or games.

- CVE-2019-13217
- CVE-2019-13218
- CVE-2019-13219
- CVE-2019-13220
- CVE-2019-13221
- CVE-2019-13222
- CVE-2019-13223

MatrixSSL & WolfSSL
MatrixSSL and WolfSSL are open source cryptographic library aimed at IoT and other lightweight use cases.

- CVE-2019-13470

FreeImage
FreeImage is an open source library for supporting popular graphic image formats, including PNG, BMG, JPEG, TIFF, and more.

- CVE-2019-13499
- CVE-2019-13500
- CVE-2019-13501

H2O Web Server
H2O is an open source HTTP server written in C. H2O is known for its ability to deliver quicker responses to users with less CPU utilization than older generations of web servers.

- CVE-2018-0608

What Does Mayhem Support?

Languages



Platforms


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


Mayhem Secures the World's Critical Software

ForAllSecure was founded on the mission to make software secure. Utilizing patented technology from a decade of research at Carnegie Mellon ForAllSecure was founded on the mission to make the world's software secure. Utilizing patented technology from a decade of research at Carnegie 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

Named to

Exhibited at