

Automated vulnerability hunting

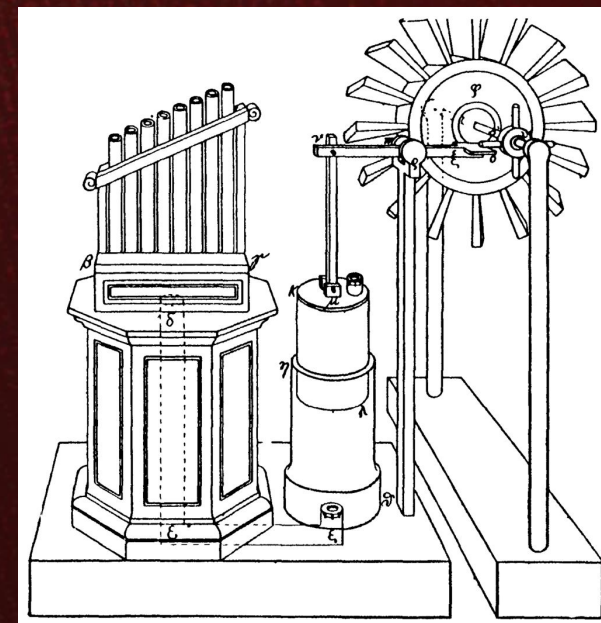
Where are we now ?



whoami

- Salim LARGO | @2ourc3
- Security Engineer @ Nexova - RF Pentest team
- Focusing on vulnerability research and DAST/SAST techniques
- Github <https://github.com/20urc3> | <https://bushido-sec.com/>





Cleverness + Laziness

(and a bit of nerdiness)

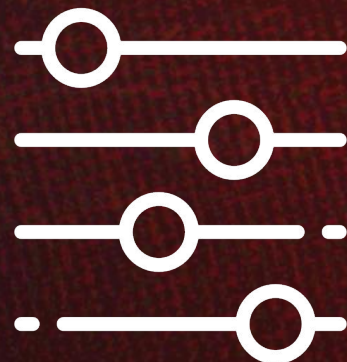




Manual work



Analysis



Tweak



Refine



Profit!





Tooling



LLM



Distribution



LLMS AT THE FOREFRONT: PIONEERING THE FUTURE OF FUZZ TESTING IN A RAPIDLY CHANGING WORLD

ChatGPT, write me fuzz tests for this
source code

DEFCON



0:01 / 43:37



HD



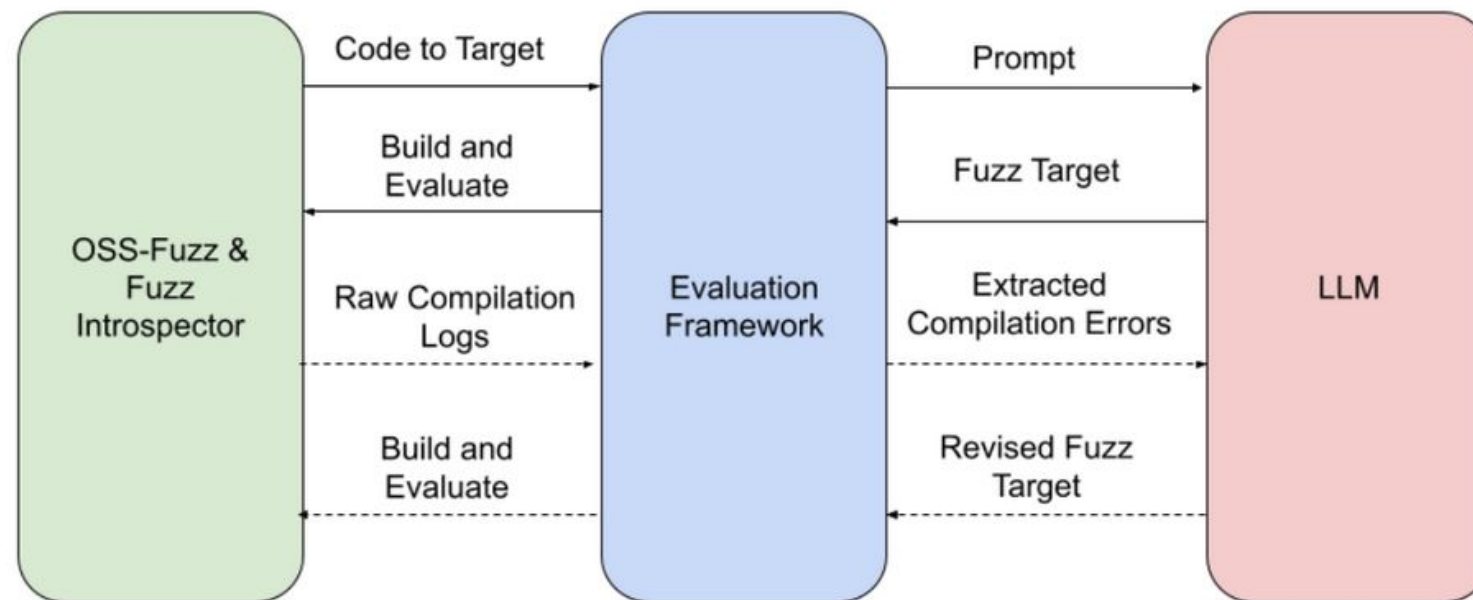
DEF CON 31 - LLMs at the Forefront Pioneering the Future of Fuzz Testing - X

<https://www.youtube.com/watch?v=k9gt7MNXPdY>



Experiment framework

To discover whether an LLM could successfully write new fuzz targets, we built an evaluation framework that connects OSS-Fuzz to Google's LLMs, conducts the experiment, and evaluates the results. The steps look like this:



https://google.github.io/oss-fuzz/research/llms/target_generation/

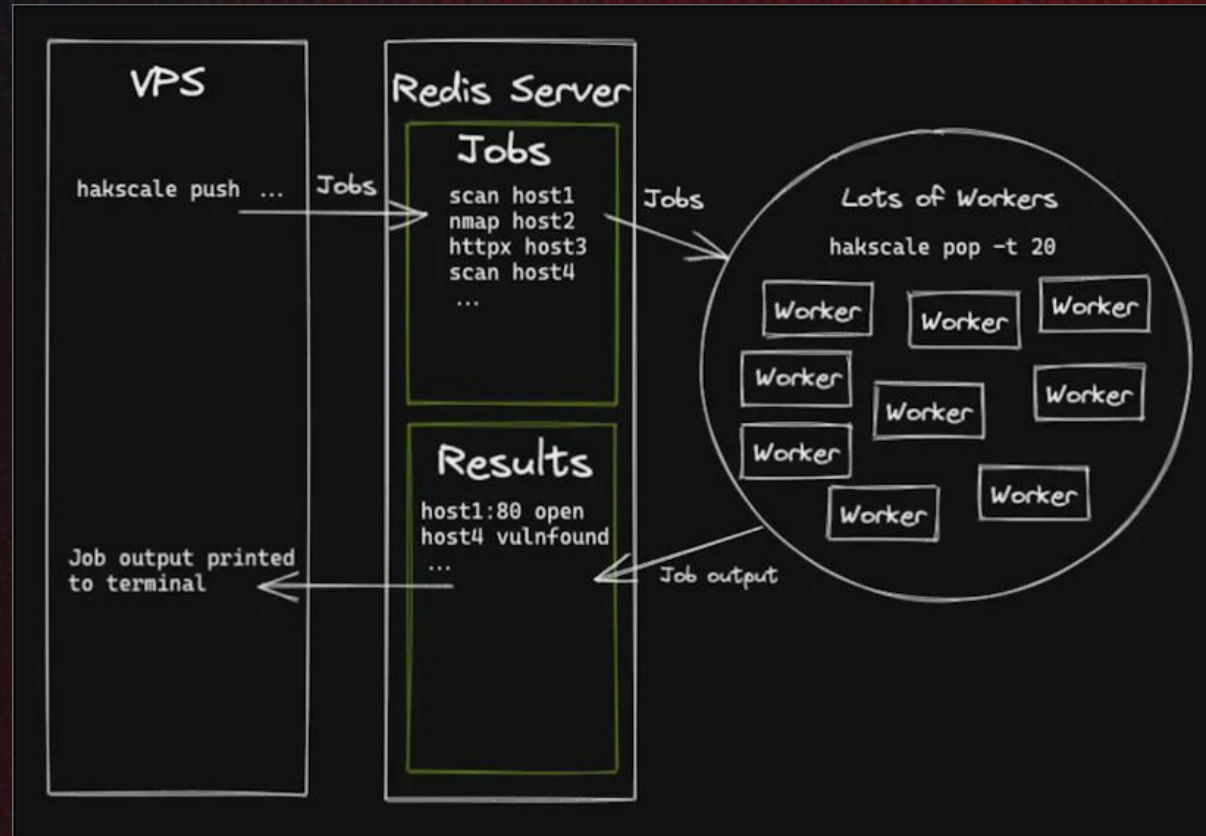




How we made \$120k in bug bounty with automation

<https://blog.vidocsecurity.com/blog/2022-summary-how-we-made-120k-bug-bounty-in-a-year/>





<https://labs.detectify.com/ethical-hacking/hakluke-creating-the-perfect-bug-bounty-automation/>





Monitoring bug
bounty websites



Automated reverse
engineering



SAST/DAST



Profit

ZDI-CAN-24307 7-Zip CVSS: 6.5 2024-06-26 2ourc3



Lesson learned



References:

- https://en.wikipedia.org/wiki/Antikythera_mechanism
- https://en.wikipedia.org/wiki/Hero_of_Alexandria
- https://en.wikipedia.org/wiki/Hero_of_Alexandria
- <https://github.com/Vsimpro/f3d>
- <https://blog.vidocsecurity.com/blog/2022-summary-how-we-made-120k-bug-bounty-in-a-year/>
- https://google.github.io/oss-fuzz/research/llms/target_generation/
- <https://www.youtube.com/watch?v=k9gt7MNXPdY>
- <https://github.com/20urc3/Sekiryu>



- <https://github.com/sullo/nikto>
- <https://portswigger.net/burp>
- <https://www.tenable.com/products/nessus>
- <https://github.com/projectdiscovery/nuclei>
- <https://www.kali.org/tools/dirb/>
- <https://www.kali.org/tools/dirbuster/>
- <https://github.com/OJ/gobuster>
- <https://github.com/tomnomnom/ffuf>
- <https://github.com/lanmaster53/recon-ng>
- <https://sqlmap.org/>
- <https://github.com/laramies/theHarvester>
- <https://github.com/ffuf/ffuf>
- <https://nmap.org/>
- <https://www.cloudamqp.com/blog/part1-rabbitmq-for-beginners-what-is-rabbitmq.html>
- <https://codeql.github.com/>
- <https://clang-analyzer.lvm.org/>
- <https://cppcheck.sourceforge.io/>
- <https://semgrep.dev/>
- <https://github.com/google/fuzzbench>
- <https://github.com/AFLplusplus/AFLplusplus>
- <https://github.com/AFLplusplus/LibAFL>
- <https://github.com/googleprojectzero/winaf1>
- <https://github.com/googleprojectzero/Jackalope>
- <https://github.com/google/honggfuzz>
- <https://github.com/google/syzkaller>
- <https://github.com/googleprojectzero/fuzzilli>
- <https://lvm.org/docs/LibFuzzer.html>

