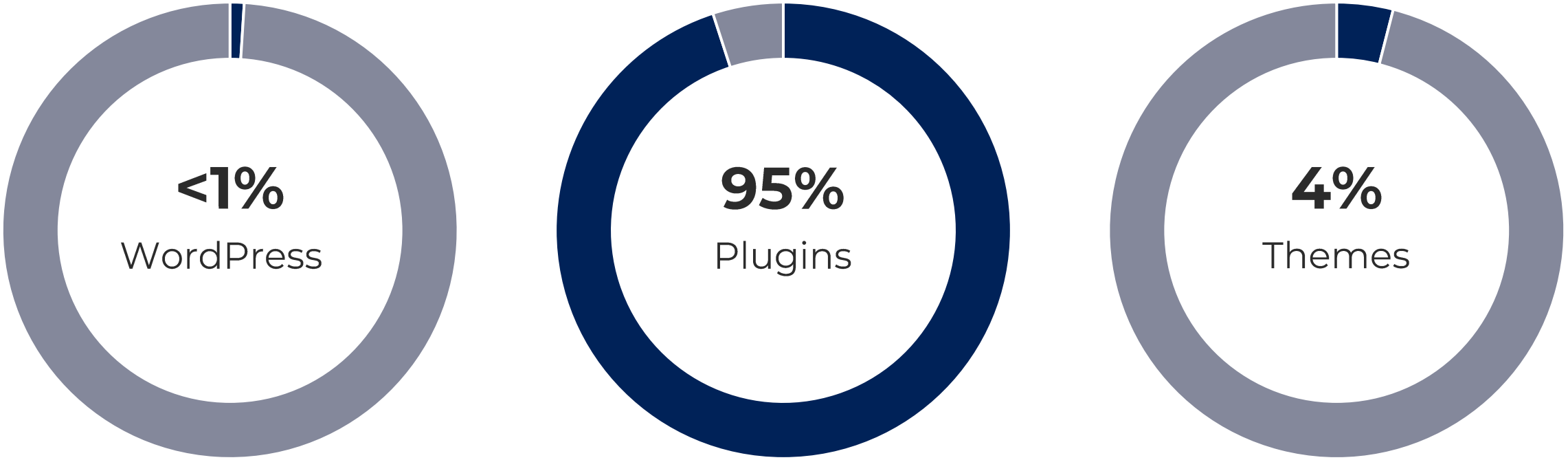
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

THEMIS: Context-Aware Grey-box Fuzzing for WordPress Plugins

Matteo Leonelli, David Jannis Dewes, Thorsten Holz

Motivation



Vulnerabilities by Source

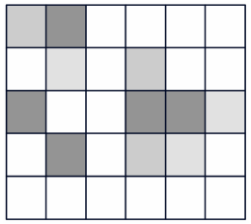
Source: WPScan, Wordfence

Key Challenges

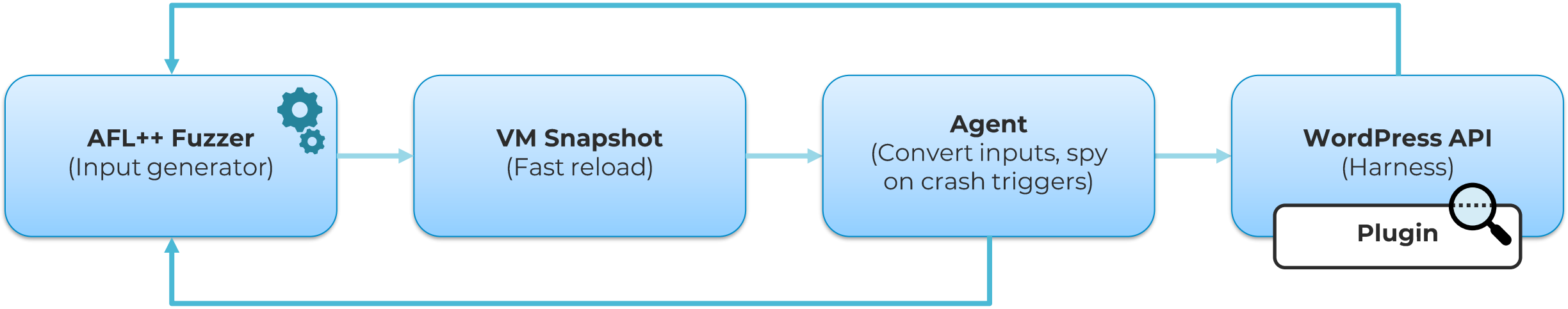
- Fuzzing as effective dynamic testing technique
- Applying fuzzing to web applications is hard
  - **Performance** overhead
  - Complex & **stateful communication**
  - Difficult **crash detection**
- Testing WordPress (or CMSs in general) is even harder
  - **Symptoms** limited to WordPress itself
  - WordPress is extremely **large** (**slow** and **noisy**)

Main Takeaway: Focus on plugin logic, ignore everything else!

Architecture

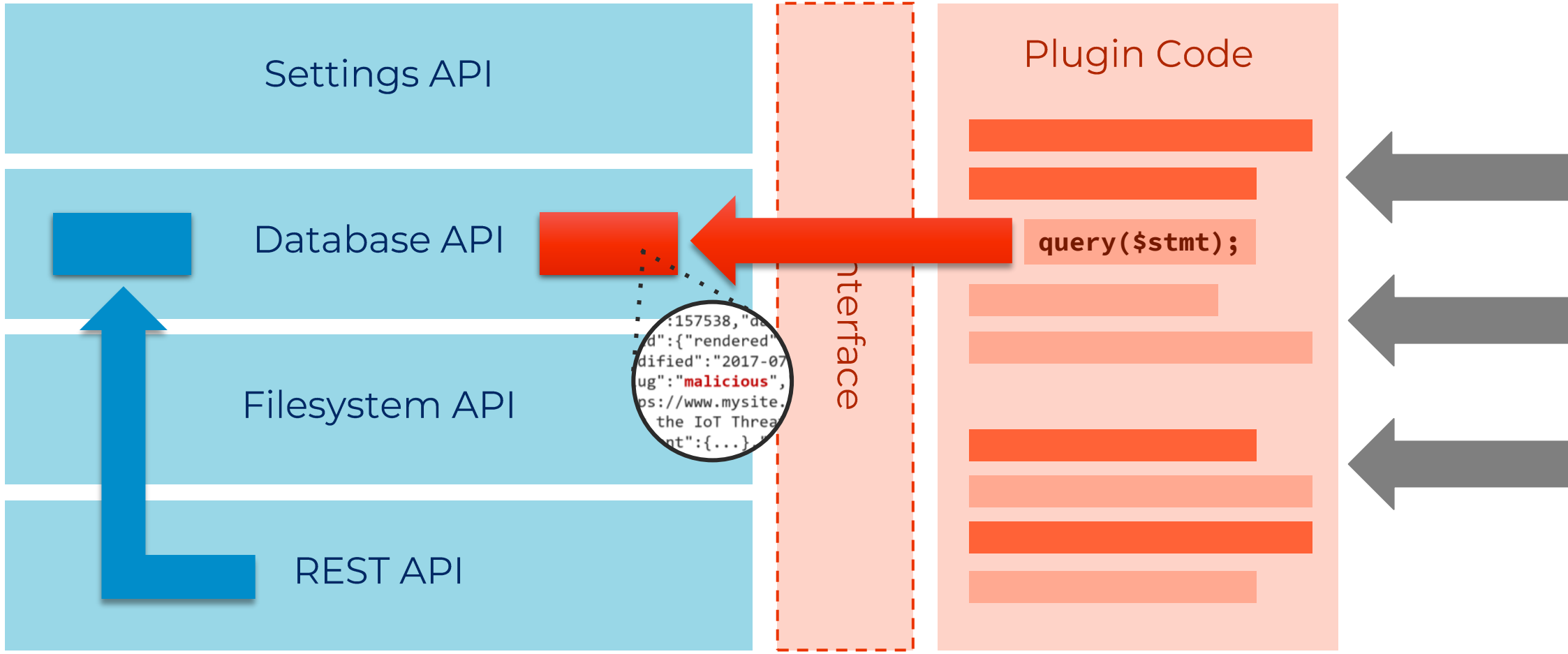


Coverage Feedback



Crash Oracle

Approach


Settings API
Database API
Filesystem API
REST API
nterface
Plugin Code
query($stmt);

Conclusion

+ Successes

- Up to **76.9%** more code coverage in plugins
- Vulnerability discovery is up to **10-20x** faster
- Contributed **10** new findings (3 CVEs)
- Reproduced **27** known vulnerabilities

− Limitations

- Increased false-positive rate (FPR)
- **Throughput** remains a bottleneck
- Missing support for **XSS & client-side bugs**
- Lack of **scalability**
- Only **partial vulnerability information** reported