Testing Software Out-of-House: How to Make it Reliable while Ensuring Code Privacy ?

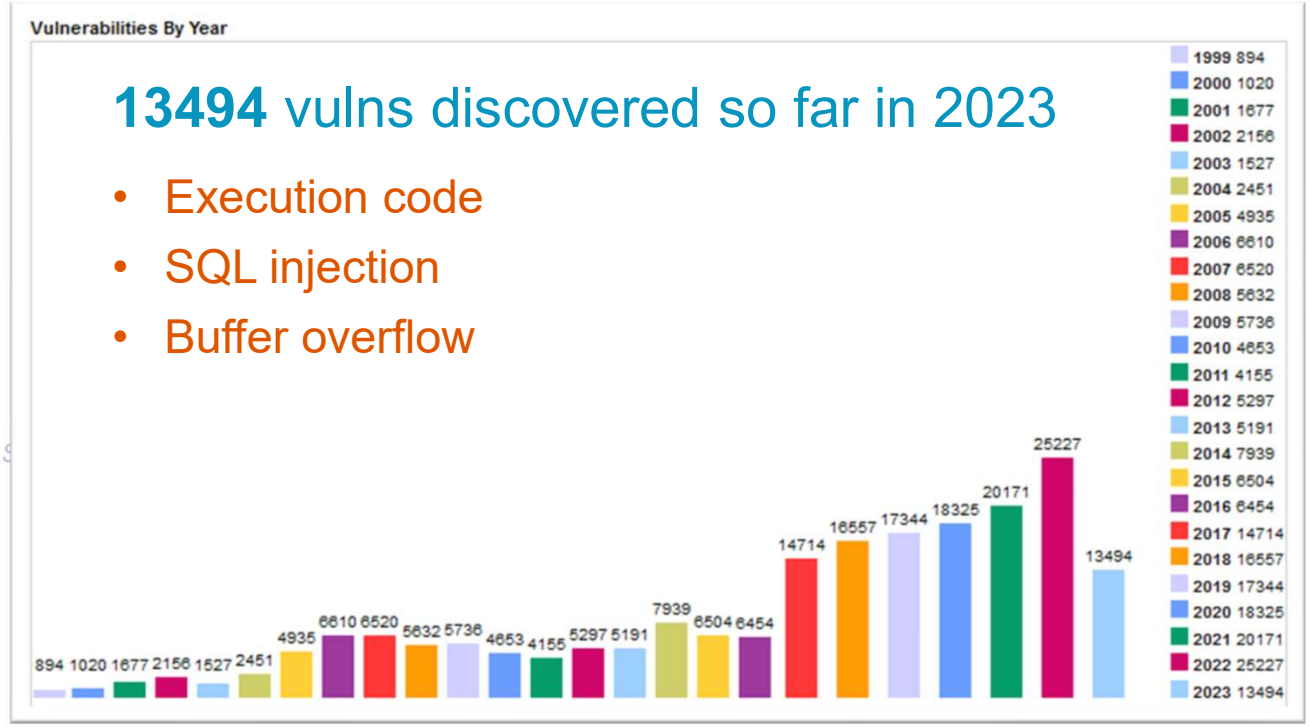
Ibéria Medeiros
LASIGE, Faculty of Sciences, University of Lisboa, Portugal

25.June.2023

- Society relies on IT supported by a myriad of software to concretize/access a diversity of tasks and services
- Software might have vulnerabilities that once exploited can compromise functionality, private data, ….

90% of security breaches happen because of vulnerabilities in the code.

Source: *Department of Homeland S*



90% of security breaches happen because of vulnerabilities in the code.

Source: *Department of Homeland Security*

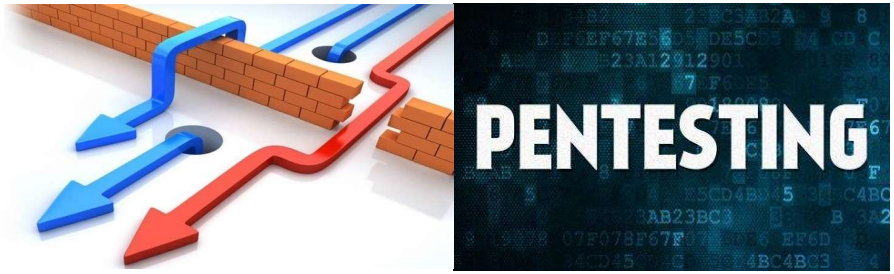
In a 2020 survey, just **55%** agreed that **security teams were responsible** for software security, whereas **85%** agreed that **developers were responsible.**

Source: *Snyk 2020 State of Open Source Security Report*

Developers are responsible for software security. **Why ?**

- Competitive market: deliver software faster and be the first
- Lack of time to test the software
- They may do not know how to make secure software, i.e., write secure code

It is necessary to test the software correctly. Who does this? Out-of-House



- Finds vulnerabilities by attacking the SUT
- Injects random inputs in SUT, while it is running
- Does not e code of SUT
- Does not SUT's code

90% of security breaches happen because of vulnerabilities in the code.

Developers must find them in the code.
They do not have time to that

Vulnerabilities might remain unfixed !

Static Analysis

How to ensure Code Privacy and allow static analysis out-of-house?

Is the NDA sufficient?
Has it been working for code privacy?

Third-Parties must access to the source code!

It is necessary to test the software correctly. Who does this?

Out-of-House

Cloud Storage Security

- Allows the storage of data with protection
- Data/code is encrypted and then stored
- Code is protected and its privacy preserved
- Code must be decrypted to analyze it

Does the cloud enable code analysis, ensuring its privacy ? **NO!**

Code Obfuscation

- Obfuscates the code turning it intelligible to humans:
  - Change variable and function names
  - Change the program structure, but not its logic
  - Resort base 64 to obfuscate the code (e.g., vars)
- Code is protected and its privacy preserved
- STA are not capable of analyzing obfuscated code
- There are no existing tools for obfuscated code analysis

Does obfuscation enable code analysis, ensuring its privacy ? **NO!**

Out-of-House

How to ensure Code Privacy and allow Static Analysis?

Idea:

- Encrypt the code and, without decrypting it, do searches over it to find vulnerabilities
- The code can be stored in a public storage
- Code privacy is preserved

Challenges:

- How to get code privacy with support to code analysis?
- Which data structure is able to maintain code privacy while performing code analysis?
- How to find vulnerabilities over encrypted code when static analysis cannot understand the data?

The first steps:

A system for vulnerability detection while maintains code privacy

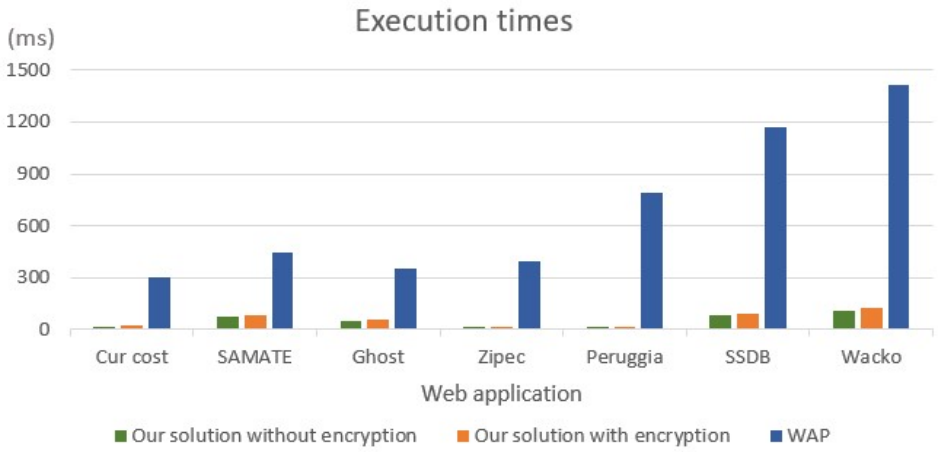
- ❖Code privacy through encryption
- ❖Vulnerability detection combining taint analysis and searchable symmetric encryption (SSE)

Out-of-House

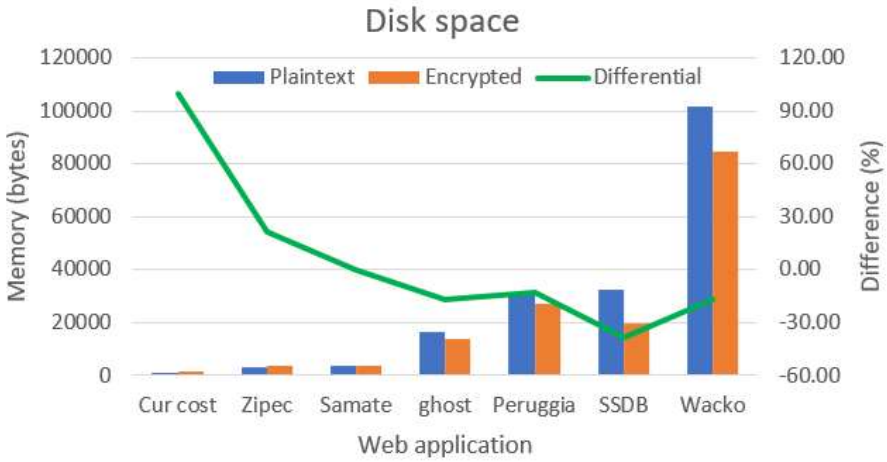
How to ensure Code Privacy and allow Static Analysis?

Web Application	Our Solution			WAP			Pixy		
	XSS	SQLi	-	XSS	SQLi	-	XSS	SQLi	-
	TP	TP	FP	TP	TP	FP	TP	TP	FP
Zipec	2	2	0	0	3	1	7	2	8
Ghost	10	3	2	5	2	0	-	-	-
Peruggia	4	6	3	3	15	0	-	-	-
SAMATE	14	3	2	11	3	0	11	4	1
Current Cost	0	3	0	4	3	2	5	3	3
DVWA	11	7	1	2	4	2	0	4	2
WackoPicko	3	1	0	5	3	0	-	-	-
Total	**44**	**25**	**8**	**30**	**33**	**5**	**23**	**13**	**14**

Precision of 89%



Our Solution < Other tools



Our solution < Source Code

Testing Software Out-of-House: How to Make it Reliable while Ensuring Code Privacy ?

Ibéria Medeiros
LASIGE, Faculty of Sciences, University of Lisboa
http://www.di.fc.ul.pt/~imedeiros/
imedeiros@di.fc.ul.pt

Thank you!