SMART INDIA HACKATHON 2024

- **Problem Statement ID -** SIH1750
- **Problem Statement Title -**
  Creating a Comprehensive Web Application Fuzzer
- **Theme -** Miscellaneous
- **PS Category -** Software
- **Team ID -** S178
- **Team Name -** Tekstatik

TEKSTATIK

FizzBuzz:

web fuzzing and resolution tools for developers

SMART INDIA HACKATHON 2024

Proposed Solution:

- Identifying, testing, and solving web application vulnerabilities has always been a problem leading to **security risks** and **delayed deployment**.
- Introducing **FizzBuzz**, a one stop integrated platform with all tools required to ease this process efficiently thus **evolving developer experience**.
- The solution offers the following-
  - ○ **Chrome extension** for detecting client-side requests to backend and fuzzing it to detect vulnerabilities and sending it to dashboard. Also highlights potential threats of malware injection.
  - ○ **CLI Tool** for deep server-side scans, logging vulnerabilities also having custom options for fuzzing.
  - ○ **IDE Fixer** for real-time code issue fixing for issues to be immediately addressed, reducing the risk of exploitation and pushing only quality code.
  - ○ **Web/App Dashboard** is the central hub for vulnerability data, analytics of issues and all the relevant solutions. Also contains risk assessment on basis of impact and status of applied fixes.

TEKSTATIK

TECHNICAL APPROACH

SMART INDIA HACKATHON 2024

Technology Stack:

Chrome Extension:

- React

CLI Tool:

- NodeJS

Web Dashboard:

- MERN

Scripts:

- Python
- JavaScript

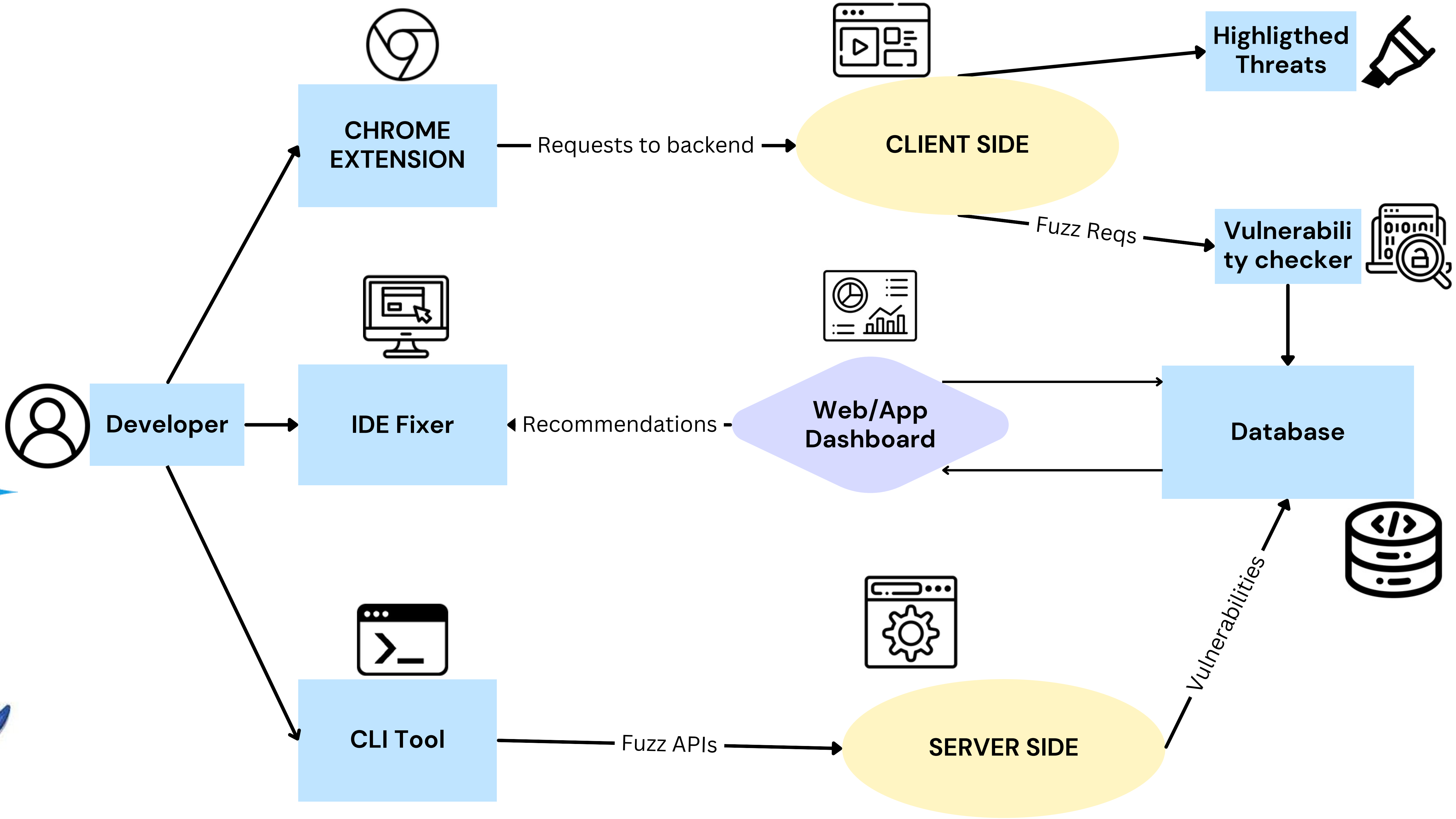
Database:

- MongoDB

Tools:

- Wfuzz
- Chrome DevTools
- Gemini API

Application Architecture:



TEKSTATIK

FEASIBILITY AND VIABILITY

SMART INDIA HACKATHON 2024

Feasibility Analysis

- Efficient integration
- Fuzz result processing
- Non competitive market landscape
- Increasing market demand
- Usage of established tools under the hood
- Reduced development costs and time
- Robust architecture

Potential Challenges

- Performance issues while complex system analysis
- Usage adoption
- Maintenance and upgradation according to market needs
- Different code writing process by different developers

Viable Strategies

- Modular Approach
- Demand for security
- One stop functionality
- Developer friendly
- Optimized fuzzing algorithms
- Fully customizable testcases and payload

IMPACT AND BENEFITS

Impact:

- Application uptime increased
- Low server load
- Improved developer efficiency
- Low production code break
- Foolproof code with good quality
- Secure code practicies

Benefits:

Social:

- Enhanced digital safety
- Production level knowledge

Economic:

- Cost savings
- Increased productivity

Environmental:

- Reduced resource consumption
- Efficient use of computing power

TEKSTATIK

RESEARCH AND REFERENCES

SMART INDIA HACKATHON 2024

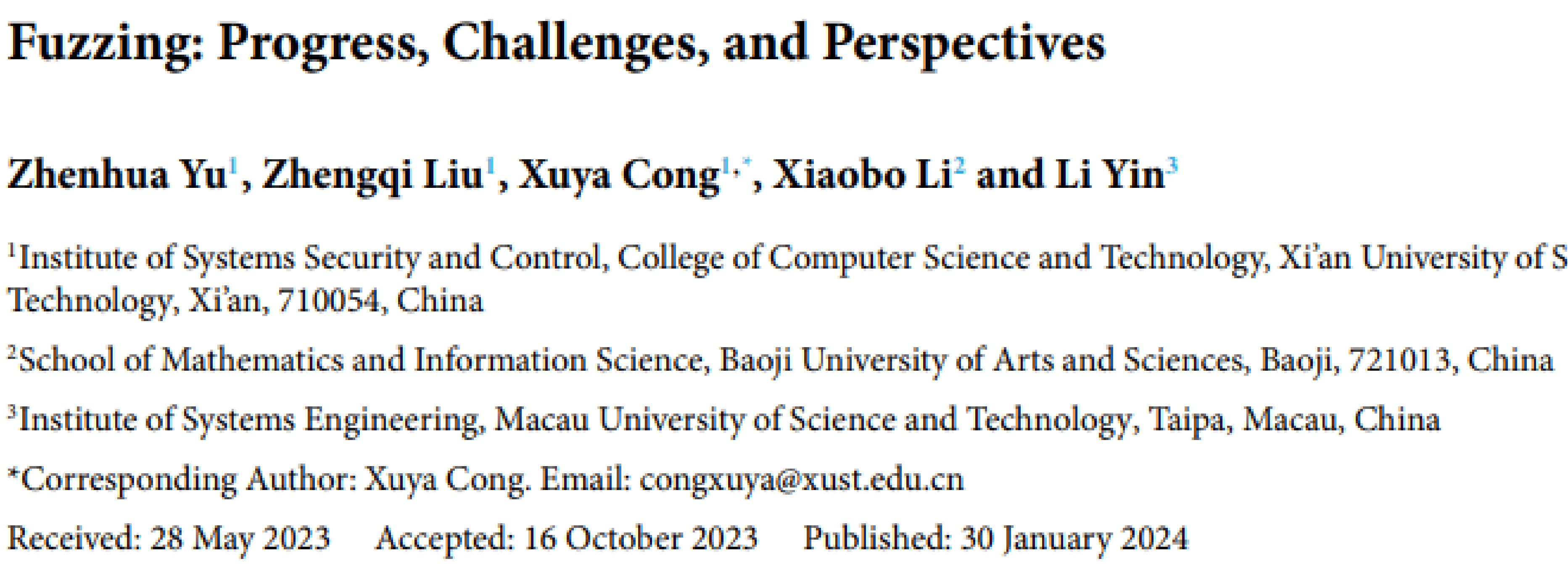
Resources followed:

- https://owasp.org/www-community/Fuzzing
- https://www.csoonline.com/article/568135/9-top-fuzzing-tools-finding-the-weirdest-application-errors.html
- https://www.freecodecamp.org/news/building-chrome-extension/
- https://medium.com/@techmindxperts/a-comprehensive-guide-to-ffuf-for-web-security-testing-207633f98217
- https://www.researchgate.net/publication/375873956_Fuzzing_Progress_Challenges_and_Perspectives

External tools used:

- https://wfuzz.readthedocs.io/en/latest/
- https://github.com/ffuf/ffuf
- https://developer.chrome.com/docs/extensions/reference/api/declarativeNetRequest

Research Paper:



Fuzzing: Progress, Challenges, and Perspectives

Zhenhua Yu[1], Zhengqi Liu[1], Xuya Cong[1,*], Xiaobo Li[2] and Li Yin[3]

[1]Institute of Systems Security and Control, College of Computer Science and Technology, Xi'an University of S
Technology, Xi'an, 710054, China

[2]School of Mathematics and Information Science, Baoji University of Arts and Sciences, Baoji, 721013, China

[3]Institute of Systems Engineering, Macau University of Science and Technology, Taipa, Macau, China

*Corresponding Author: Xuya Cong. Email: congxuya@xust.edu.cn

Received: 28 May 2023 Accepted: 16 October 2023 Published: 30 January 2024