Critique on
Davide Balzarotti, Marco Cova, Vika Felmetsger, Nenad Jovanovic, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. 2008. Saner: Composing Static and Dynamic Analysis to Validate Sanitization in Web Applications

Astha Sharma
asharma6@uno.edu

SUMMARY:

The paper describes about the problem associated with the lack of input validation technique in websites that was overlooked while writing a program. Input validation is done to check if any input from user is valid and not malicious (affecting the normal functionality of the system and sometimes leading to dangerous operations). This led to the requirement of input sanitization prior to its use. As the web based attacks(such as XSS or SQL injections) are very critical, the sanitization process must be equally effective. However, in reality, it was found that the sanitization process itself might not be fully correct or complete.

The authors of this paper, therefore, came up with an approach to check the correctness of the sanitization process. They had combined the static and dynamic analysis techniques in order to identify faulty sanitization processes which can be easily bypassed by the attackers. The authors implemented their concept in a tool - Saner - which was applied to a number of real world applications. The obtained result highlighted several vulnerabilities that was possible with an erroneous sanitization procedure.

STRENGTHS:

- The tool verifies the correctness of the sanitization process and automatically finds the input values that can exploit a vulnerability.
- Combines the power of two complementary analysis techniques - static and dynamic - for best results.
- Data flow graphs to find program statements related to the sanitization process were used.
- The tool eliminates many false positive results

WEAKNESSES:

- As the complexity of the tool is not defined, it cannot be known if it is scalable and can be used in large scale projects.
- The results are dependent on another tool, wiz., Pixy, that finds the paths between source and sink. Dependency limits the possibilities.