UNIVERSITY OF ENGINEERING AND TECHNOLOGY
VIETNAME NATIONAL UNIVERSITY
STUDY CONFERENCE ON SCIENTIFIC RESEARCH 2016

-- [A SOLUTION FOR AUTOMATICALLY SCANNING WEB VULNERABILITY] --

Huu-Tung Nguyen and Van-Giap Le
Advisor: Assoc. Prof. Ngoc-Hoa Nguyen

INTRODUCTION

In August 2015, as global statistics from Internet Live Stat, there are currently almost one billion active Websites, with a huge amount of attacked ones every day, causing a both direct and big effect on nearly 3.3 billion Internet users around the world.

The deepest root of the problem is likely the low awareness of secure programming and a lacking of ability to find system vulnerabilities in today Web developers.

These current issues in Web application security raised a need for an automatic solution that allows Web developers and security researchers detect security-related problems in the easiest way.

It is main motivation for us to develop **GuruWS**, a solution for automatically scanning Web vulnerabilty and Webshell

BASIC PRINCIPLES

Vulnerability scanning in PHP Web Application:

+ Two main approaches of Scanning Web application: White-box/Black-box testing
+ Flaws in Web application: SQL Injection, Object Injection, Cross Site Scripting, Command Injection, XPATH Injection, File Inclusion, Arbitrary Eval Code Injection
+ Combining symbolic execution and taint analysis to detect vulnerabilities

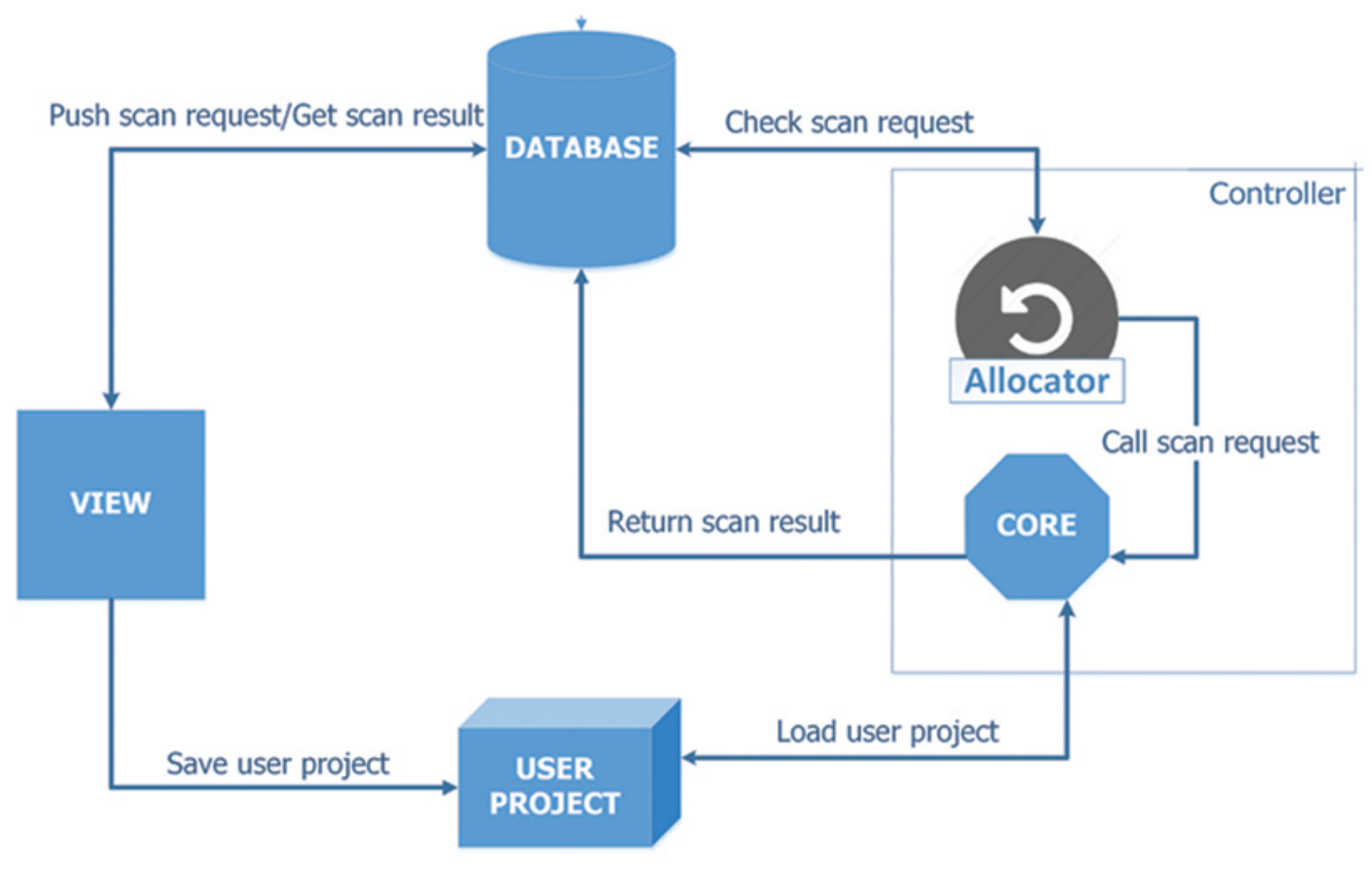
Web Shell Detecting Approaches:

+ Pattern Matching
+ Combining lexical analysis and taint analysis
+ Statistical methods

SOLUTION

GuruWS consists of 2 main modules:

+ grVulnScanner
+ grMalwrScanner

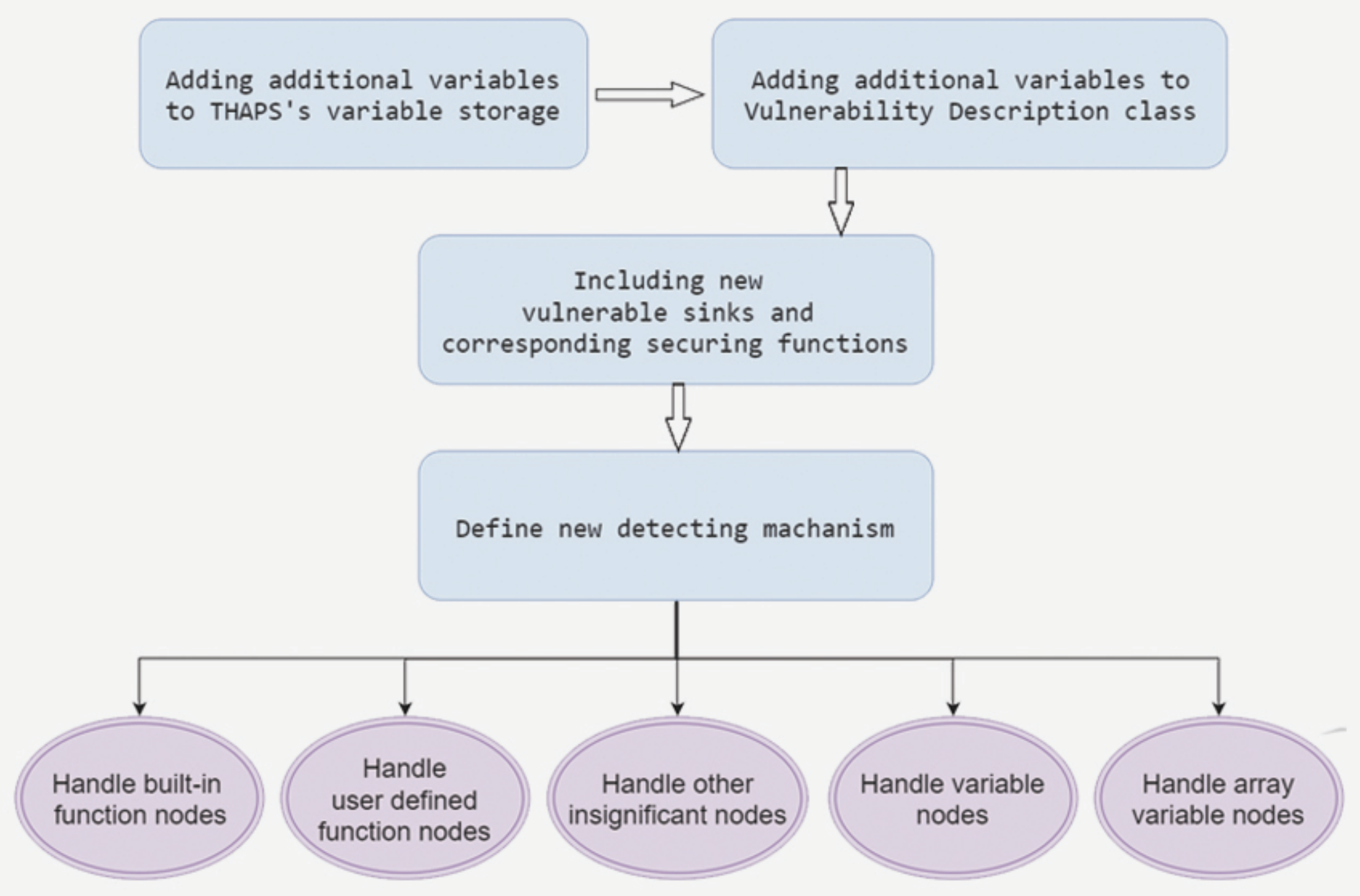


GuruWS system architecture diagram

-- [grVulnScanner] --

The core of grVulnScanner is the improved version of THAPS which is a vulnerability scanning tool for PHP Web applications. THAPS have the ability to automatically detect Cross-Site Scripting (XSS) and SQL Injectio (SQLI) vulnerability

Approaches


Adding additional variables to THAPS's variable storage
Adding additional variables to Vulnerability Description class
Including new vulnerable sinks and corresponding securing functions
Define new detecting machanism
Handle built-in function nodes
Handle user defined function nodes
Handle other insignificant nodes
Handle variable nodes
Handle array variable nodes

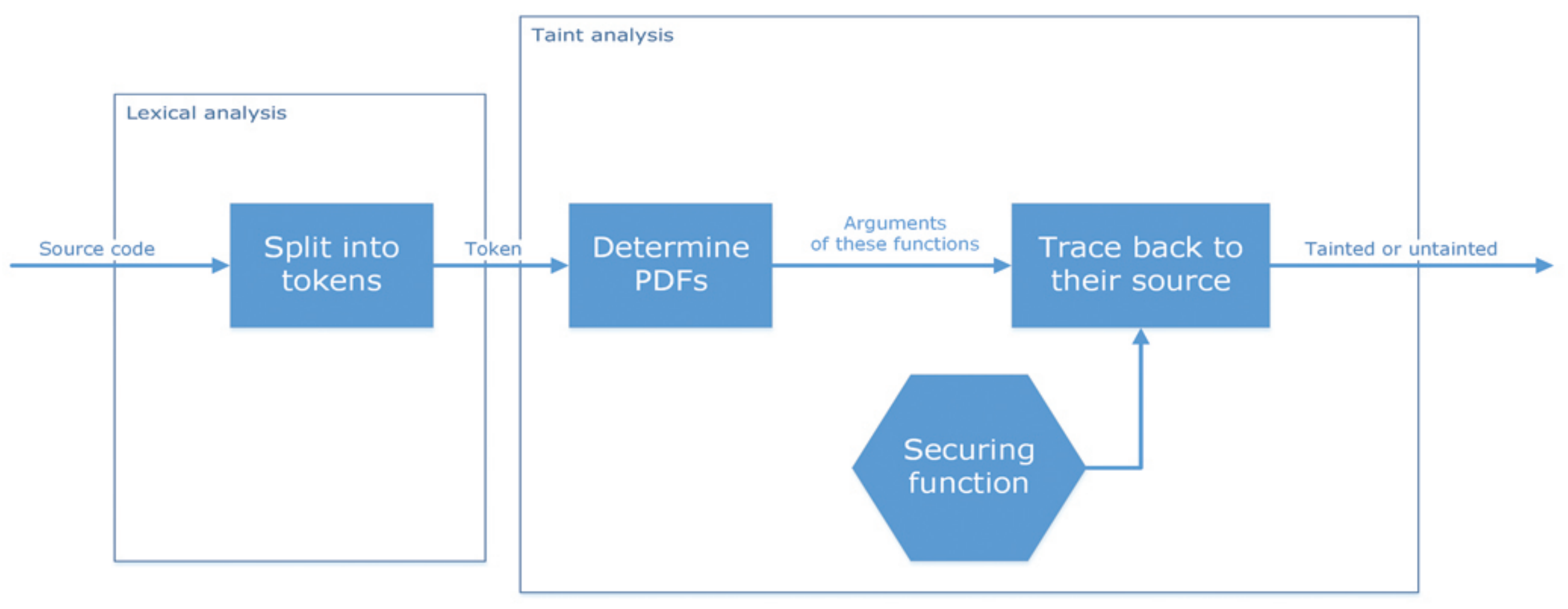
Process of adding new detecting mechanism

-- [grMalwrScanner] --

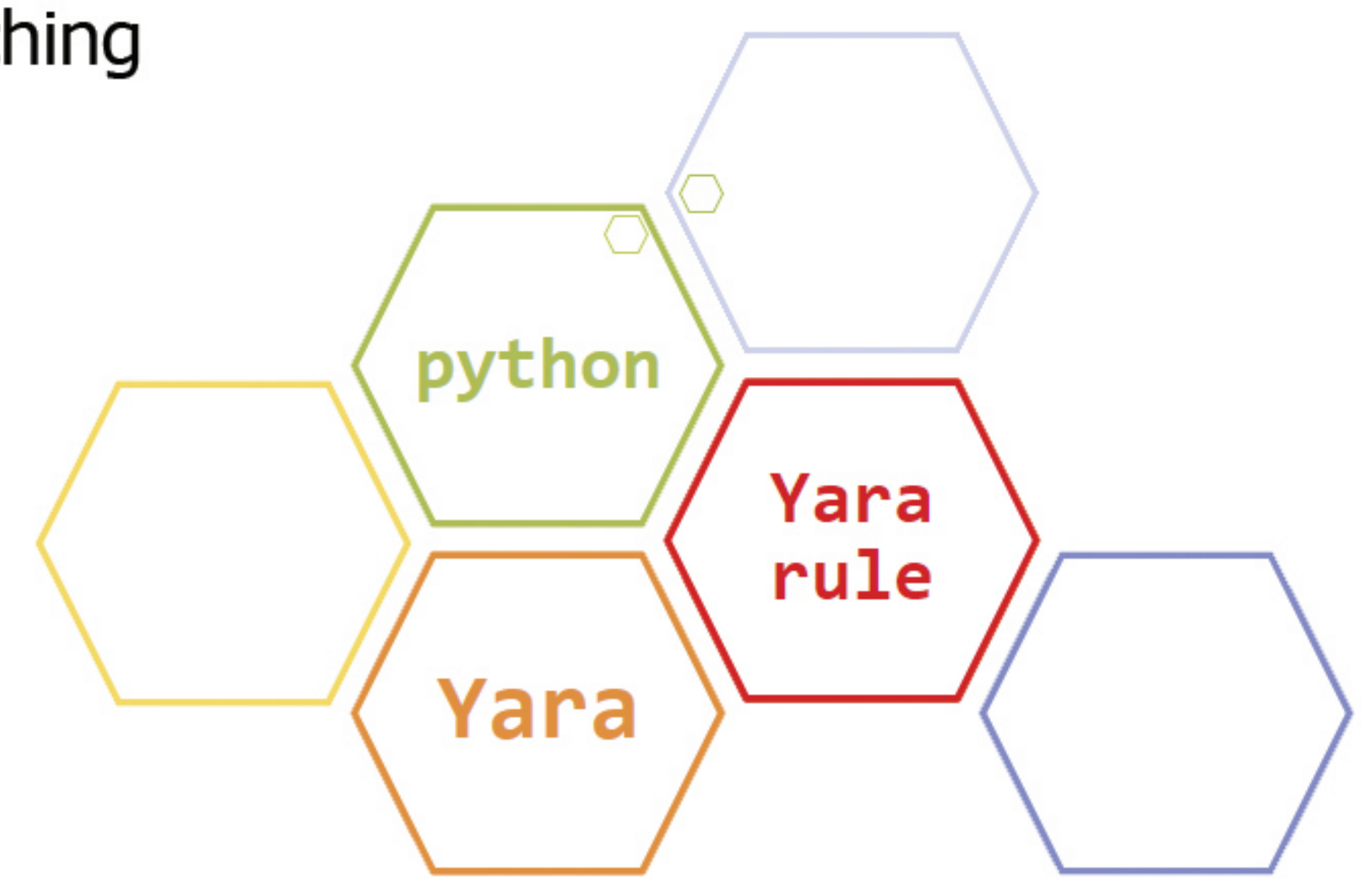
The objective of grMalwrScanner is supporting developers, Webmasters and security specialists detect malicious files in their system.

Approaches

+ Combining lexical analysis and taint analysis

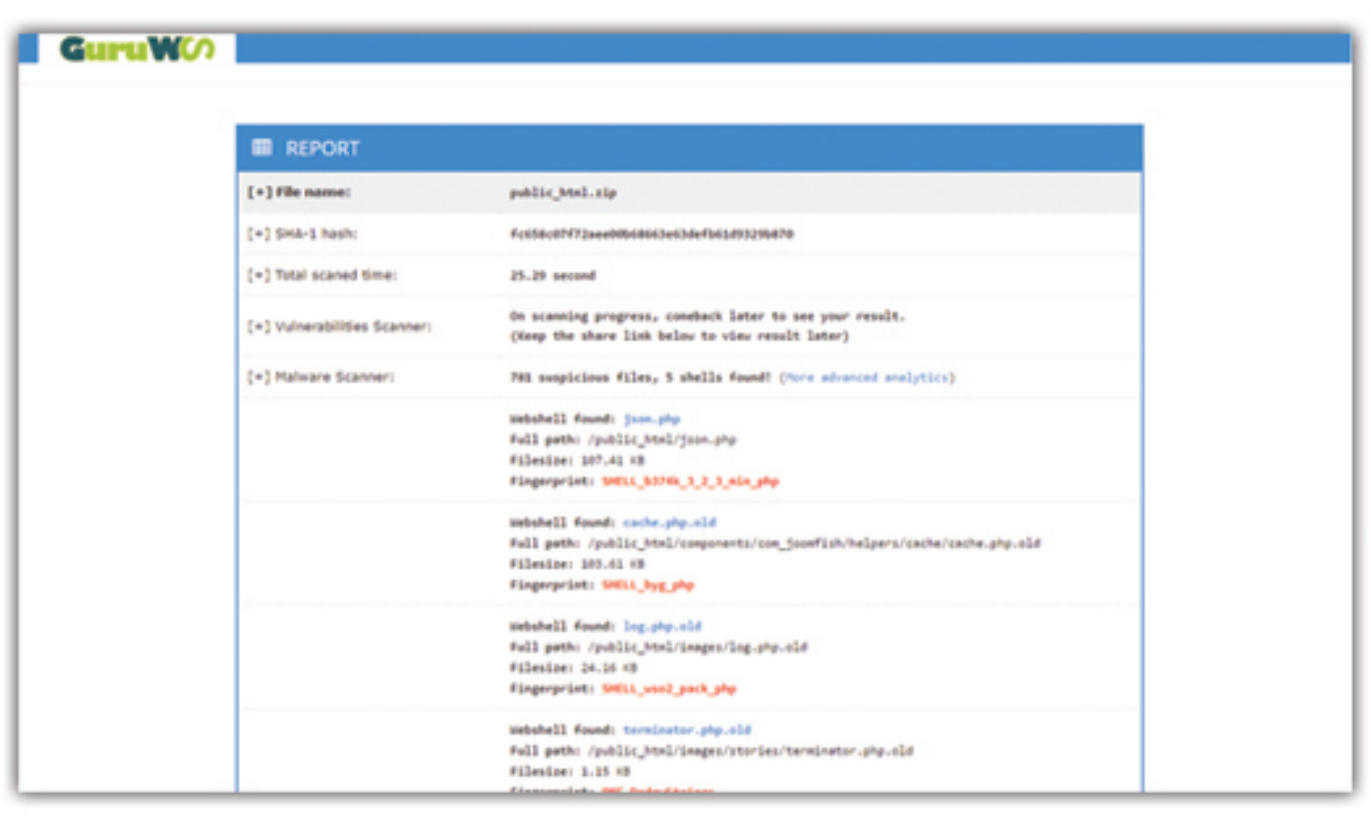


+ Pattern matching

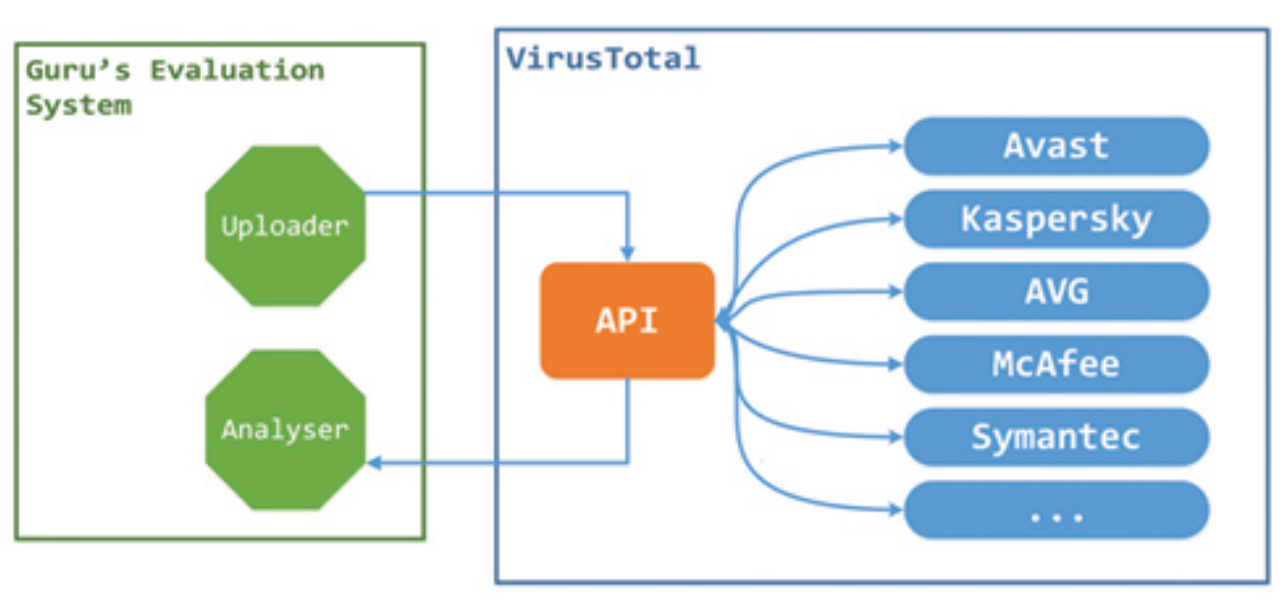


EXPERIMENT

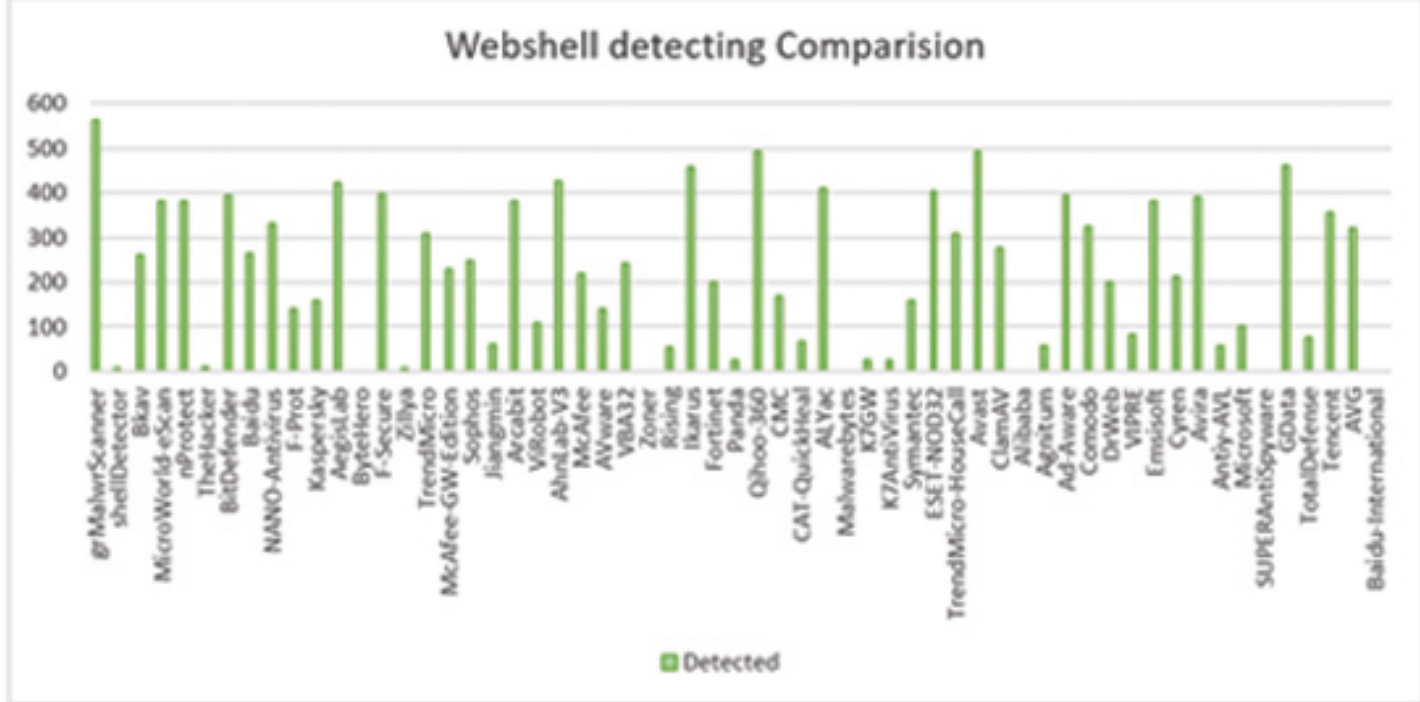
Our solution now available on http://guruws.tech

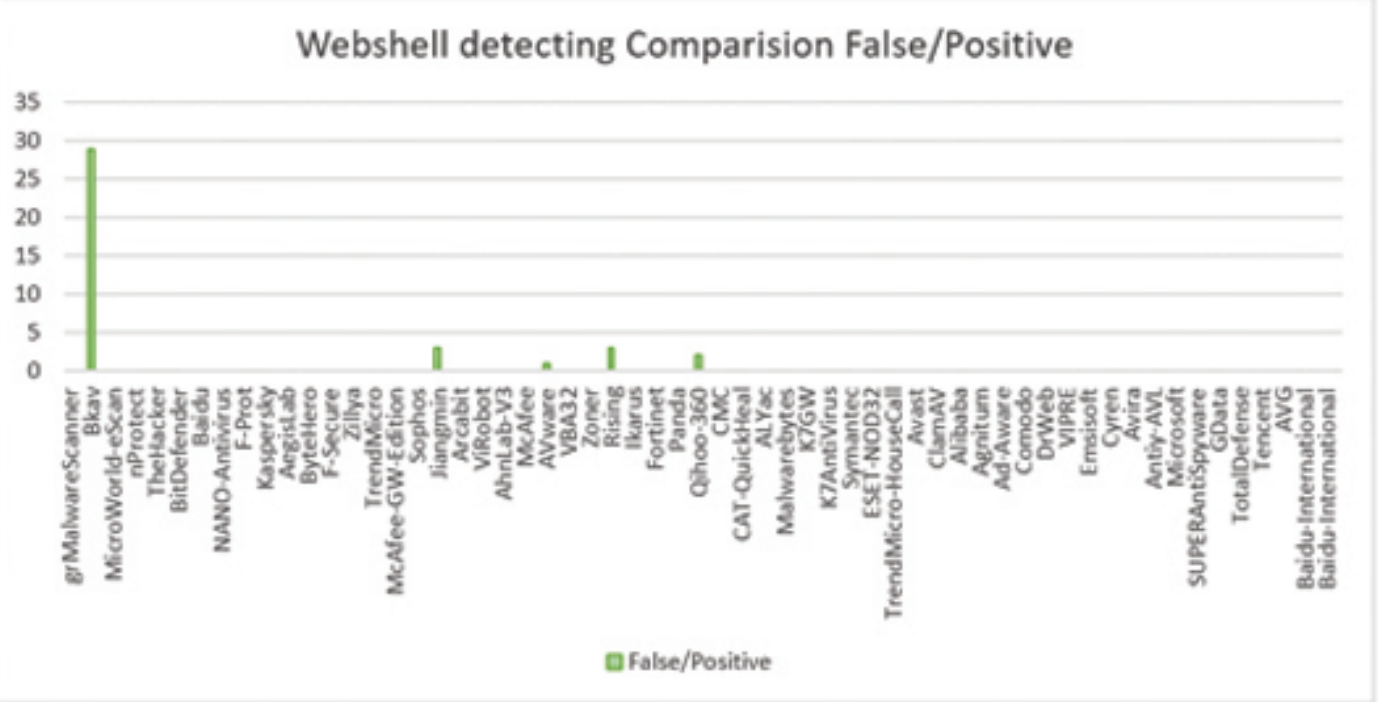


To compare our solution with other prevalent products, we built an Evaluation System, that interacts with VirusTotal's anti-virus products via its Public API, as below figure:



Here is the final result for the test set of 693 Web Shells and 14527 untainted files:





WhiteHat Grand Prix 2014 scanning result (Found / Confirm)		
Using scanner	Cross Site Scripting (XSS)	SQL Injection (SQLI)
RIPS	2 / 1	11 / 11
THAPS	2 / 2	0 / 0
E-THAPS	2 / 2	11 / 11

WhiteHat Contest 8 scanning result (Found / Confirm)		
Using scanner	Cross Site Scripting (XSS)	SQL Injection (SQLI)
RIPS	3 / 1	3/1
THAPS	3 / 1	0/0
E-THAPS	3 / 1	3/1

WhiteHat Contest 10 scanning result (Found / Confirm)		
Using scanner	Cross Site Scripting (XSS)	SQL Injection (SQLI)
RIPS	2 / 2	2 / 1
THAPS	2 / 2	0 / 0
E-THAPS	2 / 2	1 / 1

CONCLUSION AND FUTURE WORKS

GuruWS has impressive features:

+ Effective vulnerability scanner
+ Included malicious Web Shell detection
+ Working as an online service
+ Working on any device
+ Fast scan process
+ Friendly user interface (UI)
+ Accessible for everyone

In the future, we have plan to:

+ Make grVulnScanner become a gray-box scanner
+ Test the capacity of grVulnScanner in a wider range
+ Enhance grMalwrScanner capability
+ Improve Web Shell pattern sets for grMalwrScanner

CONTACT

GuruTeam [Huu-Tung Nguyen, Van-Giap Le]
University of Engineering and Technology
Official Website: http://guruws.tech
Email: {tungnh_57, giaplv_57}@vnu.edu.vn
Twitter: @tungpun_ @Hawking131

REFERENCES

+ Stefan Kals, Engin Kirda, Christopher Kruegel, and Nenad Jovanovich: SecuBat: A Web Vulnerability Scanner.
+ Torben Jensen, Heine Pedersen, Mads Chr. Olesen, Rene Hansen: THAPS: Automated Vulnerability Scanning of PHP Applications
+ Johannes Dahse: RIPS - A static source code analyser for vulnerabilities in PHP scripts.
+ Rahul Sasi: Web Backdoors - Attack, Evasion And Detection
+ S.Ramya, Dr. N.Radha: Diagnosis of Chronic Kidney Disease Using Machine Learning Algorithms