GRAPHWAVE

Detecting similar CFG-paths from HTTP responses

Tijme Gommers
Northwave B.V.

tijme.gommers@northwave.com

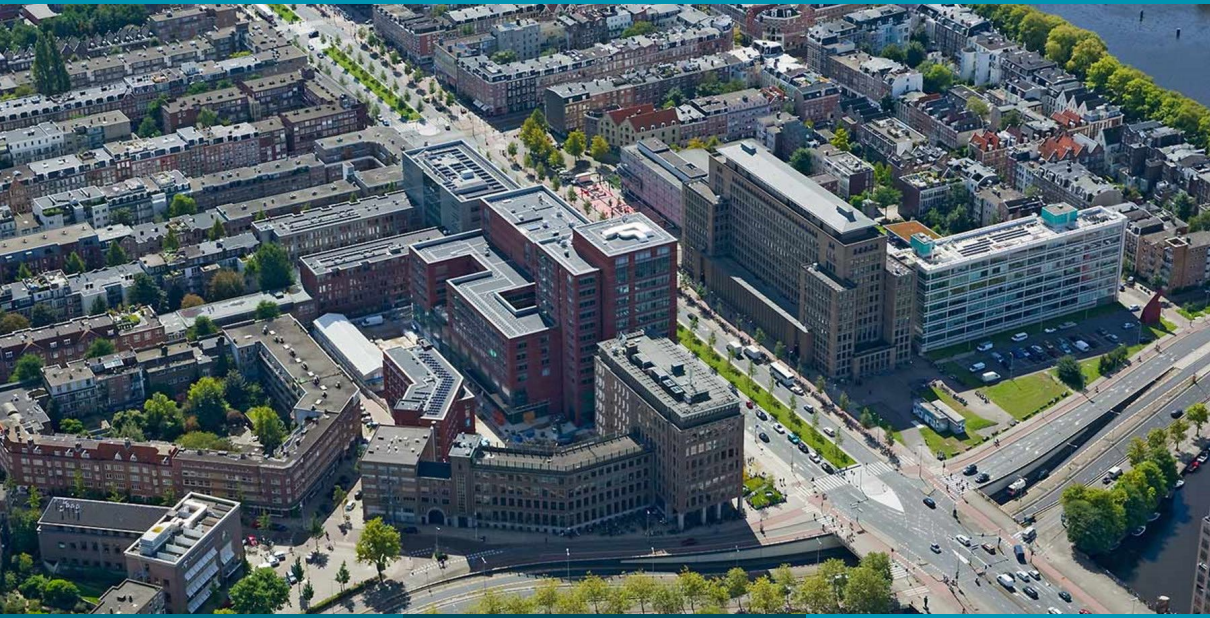
2018-05-03

Overview

Introduction
Context

Northwave

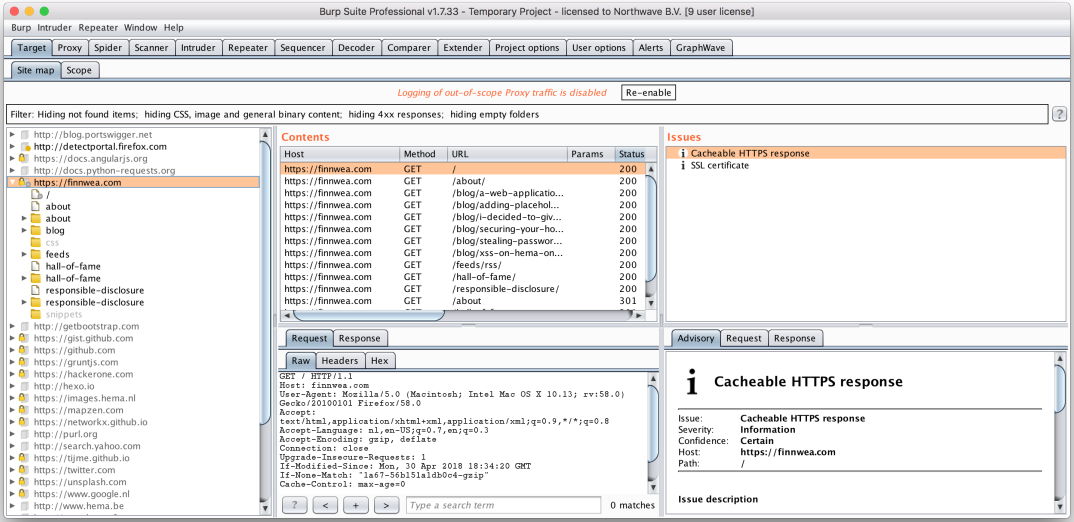
Amsterdam University of Applied Sciences



École D'ingénieurs du Monde Numérique

Introduction
Research

Automated Web Application Vulnerability Scanners



Efficiency & Effectiveness

- Efficiency = Time to finish
- Effectiveness = Vulnerabilities found

Situation at Northwave

- Scans take up to 36 hours

Motivation

Goal

- Generic open-source solution
- Improve efficiency
- Maintain effectiveness

Scope

- Only generic solutions, **not** scanner specific
- Improve efficiency, **not** effectiveness
- Only web application scanners, not all scanners
- Only scanners that allow behaviour modifications

Introduction
Questions

Main question

Which user friendly product can be developed to improve the efficiency of Automated Web Application Vulnerability Scanners while maintaining effectiveness?

Sub-questions 1

How can the efficiency and effectiveness of Automated Web Application Vulnerability Scanners be measured?

Sub-questions 2

Which key concept of the Automated Web Application Vulnerability Scanners can improve efficiency the most while maintaining effectiveness?

Sub-questions 3

Which technologies can be used to improve the most in efficiency varying key concept in an automated way?

Sub-questions 4

In which user friendly way can the most efficient and effective technology be integrated with Automated Web Application Vulnerability Scanners?

Theory
Automated Web Application Vulnerability Scanners

Burp Suite

Acunetix

Not Your Average Web Crawler

Theory
Key concepts

Target scope (reduction)

Multi-threading

Time To First Byte

Persistent HTTP connections

Theory
Measurements

Efficiency

Effectiveness

Research
Methodology

For every sub-question diff meth

explain iterating sub-questions. each one with different method.

Research
Iterations

Efficiency and effectiveness measurements

Already answered

The efficiency of scanner concepts

Qua research

Technologies to improve the efficiency

Qua research

A user friendly product

Qua research

Results
The efficiency of scanner concepts

Data

Show the excel results table

BurpSuite persistent HTTP connections

Acunetix persistent HTTP connections

Multi-threading rows

Results
Technologies to improve the efficiency

Data

Show the excel results table

HTML tree similarity measure

Piecewise response hashing

A custom undirected graph

Results
A user friendly product

Data

Show the excel results table

Conclusion

Goal

Efficiency and effectiveness measurements

The efficiency of scanner concepts

Technologies to improve the efficiency

A user friendly product

Improving the efficiency of scanners

Product

Product

GraphWave Demo

Discussion

The research is valid

Unexpected results

Possible explanation

Advice for follow-up research

Questions

The End