Universiteit van Amsterdam
System and Network Engineering

Effectiveness of Automated Application Penetration Testing Tools

Alexandre Ferreira Harald Kleppe

Overview

- Introduction
- Background
- Target Application
- Vulnerability Scanners
- Test Results
- Conclusion
- Questions

Introduction

- **Are automated penetration testing tools effective?**
  - What and how is automated with these tools?
  - How much manual intervention is required from the results? (false positives / negatives)
  - What are the most effective tools?
  - What level of effectiveness is acceptable / necessary to properly support pentesters?

Background

- OWASP Top 10 Project
- What is a Penetration Test?
- What is a Penetration Testing Tool?

Target Application

- Why a new application?
  - Other tools (HacmeBank, WebGoat, ...)
  - Known implementations
- How and which vulnerabilities are implemented?
  - Lets have a look!

Target Application (2)

- SQL Injection
  - In URL and in HTML form
- Cross Site Scripting (XSS)
  - Stored and relected
- Cross Site Request Forgery (CSRF)
- Path traversal
- Failure to restrict URL access
- Printed error

Vulnerability Scanners

- Tool selection
  - Both open source and commercial tools
  - Established tools
  - New players
  - Some tools: €10 000 per year

Vulnerability Scanners (2)

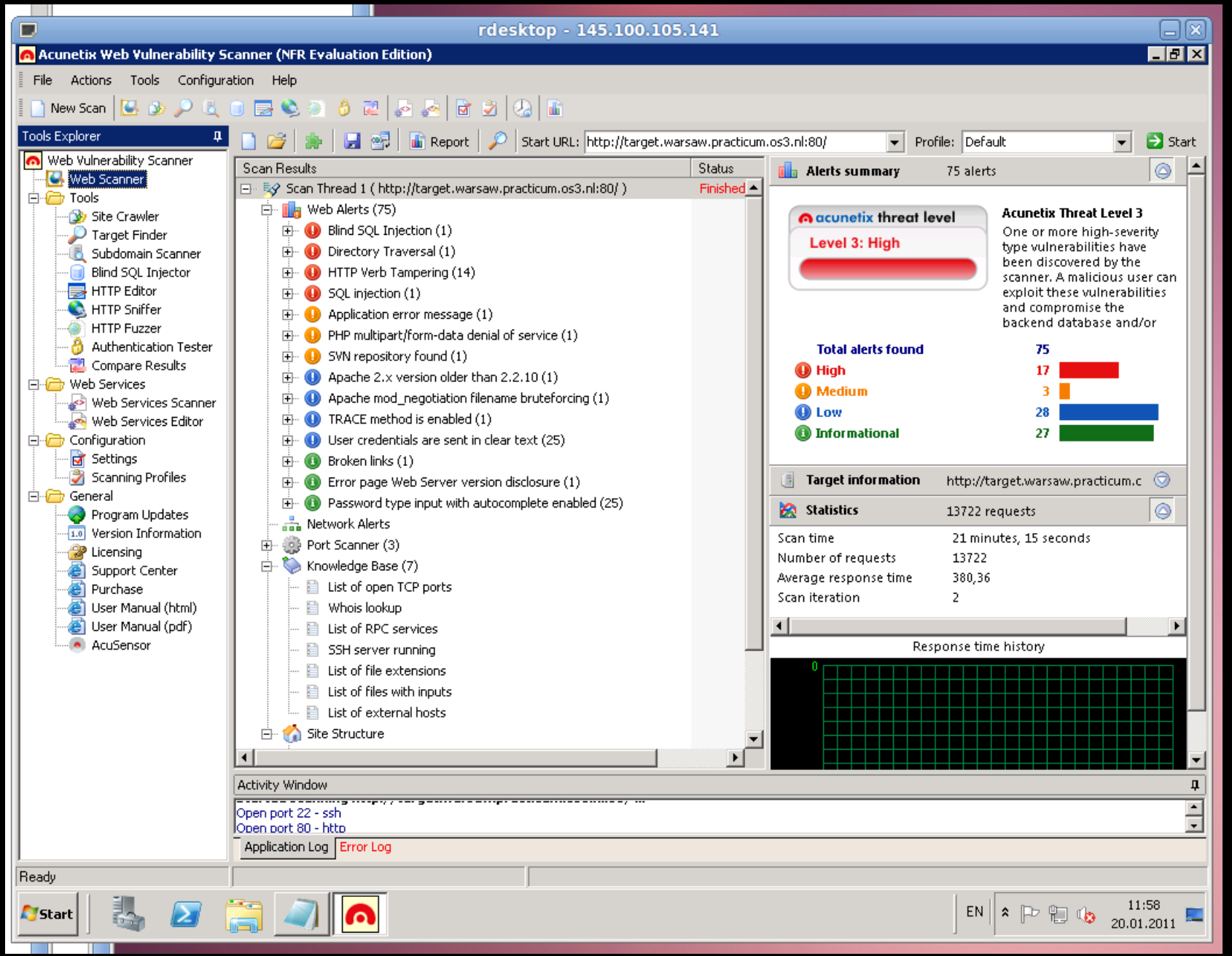
Commercial

- Acunetix
- BurpSuite Pro
- Core Impact
- IBM AppScan
- NTOSpider
- ParosPro
- Qualys

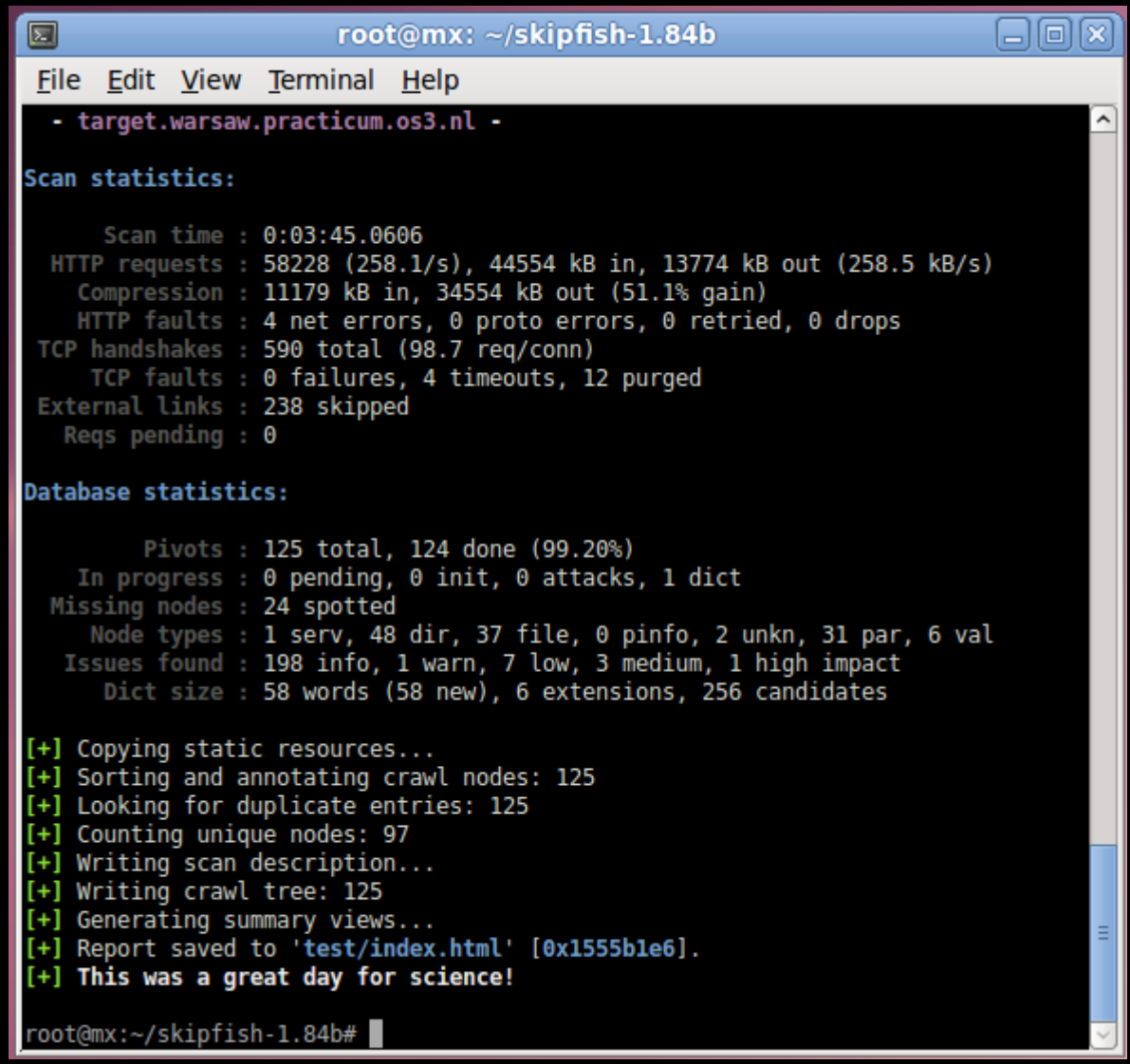
Open Source

- Paros
- Skipfish
- w3af
- ZAProxy

Vulnerability Scanners (3)



Vulnerability Scanners (4)



Test Results

- Low hitrate, differ from other research
- None of the tools “passed” this test

Test Results (2)

Vulnerability Type / Tools	Path traversal	CSRF	Reflected XSS	Stored XSS	Failure to restrict URL access	SQL Injection (in URL)	SQL Injection (in HTML form)	Printed error message
Commercial								
Commercial								
Commercial								
Commercial								
Commercial								
Commercial								
Open Source								
Commercial								
Commercial								
Open Source								
Open Source								
Open Source								

Test Results (3)

- Insufficient dataset to compare the tools generally
- Relying on crawling engines proves to be dangerous

Conclusion

- **Scanners are conditionally effective**
  - Nearly the entire scan *can* be automated
  - Quite some intervention is required
  - For our application: Skipfish + BurpSuite
  - Necessary effectiveness

Conclusion (2)

- Further research
  - Crawling abilities of different scanners
  - Selective scanning

Questions

Vragen

Perguntas

?

Въпроси

Pytania

Spørsmål

Ερωτήσεις

Fragen