



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)

The screenshot displays the Acunetix Web Vulnerability Scanner (NFR Evaluation Edition) interface. The main window shows the results of a scan performed on the target URL `http://target.warsaw.practicum.os3.nl:80/`. The scan is finished, and the results are categorized into Web Alerts (75) and Network Alerts (3).

Web Alerts (75):

- Blind SQL Injection (1)
- Directory Traversal (1)
- HTTP Verb Tampering (14)
- SQL injection (1)
- Application error message (1)
- PHP multipart/form-data denial of service (1)
- SVN repository found (1)
- Apache 2.x version older than 2.2.10 (1)
- Apache mod_negotiation filename bruteforcing (1)
- TRACE method is enabled (1)
- User credentials are sent in clear text (25)
- Broken links (1)
- Error page Web Server version disclosure (1)
- Password type input with autocomplete enabled (25)

Network Alerts (3):

- Port Scanner (3)

Knowledge Base (7):

- List of open TCP ports
- Whois lookup
- List of RPC services
- SSH server running
- List of file extensions
- List of files with inputs
- List of external hosts

Site Structure

Alerts summary: 75 alerts

Acunetix threat level: Level 3: High

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or

Total alerts found: 75

| Severity | Count |
|---------------|-------|
| High | 17 |
| Medium | 3 |
| Low | 28 |
| Informational | 27 |

Target information: `http://target.warsaw.practicum.c`

Statistics: 13722 requests

| Metric | Value |
|-----------------------|------------------------|
| Scan time | 21 minutes, 15 seconds |
| Number of requests | 13722 |
| Average response time | 380,36 |
| Scan iteration | 2 |

Response time history: A graph showing response time history with a grid and a single data point at 0.

Activity Window:

- Open port 22 - ssh
- Open port 80 - http
- Application Log
- Error Log

The Windows taskbar at the bottom shows the system clock at 11:58 on 20.01.2011.

Vulnerability Scanners (4)

```
root@mx: ~/skipfish-1.84b
File Edit View Terminal Help
- target.warsaw.practicum.os3.nl -
Scan statistics:
    Scan time : 0:03:45.0606
    HTTP requests : 58228 (258.1/s), 44554 kB in, 13774 kB out (258.5 kB/s)
    Compression : 11179 kB in, 34554 kB out (51.1% gain)
    HTTP faults : 4 net errors, 0 proto errors, 0 retried, 0 drops
    TCP handshakes : 590 total (98.7 req/conn)
    TCP faults : 0 failures, 4 timeouts, 12 purged
    External links : 238 skipped
    Reqs pending : 0
Database statistics:
    Pivots : 125 total, 124 done (99.20%)
    In progress : 0 pending, 0 init, 0 attacks, 1 dict
    Missing nodes : 24 spotted
    Node types : 1 serv, 48 dir, 37 file, 0 pinfo, 2 unkn, 31 par, 6 val
    Issues found : 198 info, 1 warn, 7 low, 3 medium, 1 high impact
    Dict size : 58 words (58 new), 6 extensions, 256 candidates
[+] Copying static resources...
[+] Sorting and annotating crawl nodes: 125
[+] Looking for duplicate entries: 125
[+] Counting unique nodes: 97
[+] Writing scan description...
[+] Writing crawl tree: 125
[+] Generating summary views...
[+] Report saved to 'test/index.html' [0x1555b1e6].
[+] This was a great day for science!
root@mx:~/skipfish-1.84b#
```

Test Results

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

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

Perguntas

Pytania

Ερωτήσεις



Vragen

Въпроси

Spørsmål

Fragen