Practical Assignment #2

João Neto – 2023234004

Vasco Alves – 2022228207

29 de maio de 2026

Índice

1 Introduction **3**

2 Arquitecture considered for the PA#3 (for both scenarios 1 and 2) **3**

2.1 Network structure . . . 3

2.2 Servers . . . 3

2.3 Services . . . 3

3 Web application security testing **5**

3.1 Information Gathering . . . 5

3.2 Configuration and Deployment Management Testing . . . 5

3.3 Identity Management Testing . . . 5

3.4 Authentication Testing . . . 5

3.5 Authorization Testing . . . 5

3.6 Session Management Testing . . . 5

3.7 Input Validation Testing . . . 5

3.8 Testing for Error Handling . . . 5

3.9 Testing for Weak Cryptography . . . 5

3.10 Business Logic Testing . . . 5

3.11 Client Side Testing . . . 5

4 Web application security firewall **5**

4.1 Information Gathering . . . 5

4.2 Configuration and Deployment Management Testing . . . 5

4.3 Identity Management Testing . . . 5

4.4 Authentication Testing . . . 5

4.5 Authorization Testing . . . 5

4.6 Session Management Testing . . . 5

4.7 Input Validation Testing . . . 5

4.8 Testing for Error Handling . . . 5

4.9 Testing for Weak Cryptography . . . 5

4.10 Business Logic Testing . . . 5

4.11 Client Side Testing 5

5 Conclusions **5**

1 Introduction

Este trabalho tem como objectivo realizar testes de penetração numa aplicação cobaia (o Juicebox) desenhada para aprendizagem.

2 Arquitecture considered for both stages

Utilizamos somente duas máquinas virtuais: um servidor a correr *CentOS 9* e um cliente a correr *Kali Linux*. O servidor contém o serviço *Apache* que age como *firewall* através do plugin *ModSecurity* e um servidor nodejs que contém o Juicebox; a aplicação que vai servir de "dummy" (cobaia).

Vão ser realizadas duas etapas de testes: primeiro, sem WAF (*Web Application Firewall*) e com foco em explorar vulnerabilidades na aplicação; e depois com uma WAF desenhada para sobreviver as várias vulnerabilidades que foram encontradas na etapa anterior.

2.1 Network structure

2.2 Servers

O router contém a firewall e o serviço juicebox.

2.3 Services

Juicebox no port 3000

3 Web application security testing

3.1 Information Gathering

3.2 Configuration and Deployment Management Testing

3.3 Identity Management Testing

3.4 Authentication Testing

3.5 Authorization Testing

3.6 Session Management Testing

3.7 Input Validation Testing

3.8 Testing for Error Handling

3.9 Testing for Weak Cryptography

3.10 Business Logic Testing

3.11 Client Side Testing

4 Web application security firewall

4.1 Information Gathering

4.2 Configuration and Deployment Management Testing

4.3 Identity Management Testing

4.4 Authentication Testing

4.5 Authorization Testing

4.6 Session Management Testing

4.7 Input Validation Testing

4.8 Testing for Error Handling

4.9 Testing for Weak Cryptography

4.10 Business Logic Testing

4.11 Client Side Testing

5 Conclusions