WAF basic test report - Example-Project

This PDF documents the basic tests to verify that the WAF (ModSecurity + OWASP CRS) blocks obvious SQ

Environment:
- WAF exposed on host port 8080 (http://localhost:8080)
- Backend proxied to https://finalexam.narongsak.site (user-provided)
- Command examples to run locally in terminal on the host where docker-compose is running.

Test 1: benign request
Command:
    curl -i http://localhost:8080/

Expected result: HTTP 200 from backend; no ModSecurity blocking.

Test 2: SQL injection attempt
Command:
    curl -i "http://localhost:8080/?id=1' OR '1'='1"

Expected result: If OWASP CRS rule set is fully loaded and active, ModSecurity should detect the pattern ar

Audit log location (container): /var/log/modsec_audit.log (depends on configuration)

Notes:
- The included CRS files in this template are minimal placeholders; to test real blocking you must populate `v
- Alternatively, use a community prebuilt Docker image that bundles nginx+modsecurity+CRS and point the