PROJECT ASSIGNMENT

By Chesta Dubey

PROJECT 1:

DVWA Security Level Comparison Project.

OBJECTIVE:

Compare how DVWA behaves at different security levels(Low,Medium,High,imposible)

TASKS:

1)Pick 2 vulnerabilities

2)Document payloads that work at **Low**.

3)Try the same payloads at **Medium/High**,

observe differences.

4)Identify what defense mechanism was

added (e.g., input sanitization,

parameterization).

5)Write a mini research report: *“How DVWA*

*implements defenses at different security*

*levels.”*

Introduction

This research report summarizes experiments on two vulnerabilities in DVWA (Damn

Vulnerable Web Application): Reflected XSS and Command Injection.

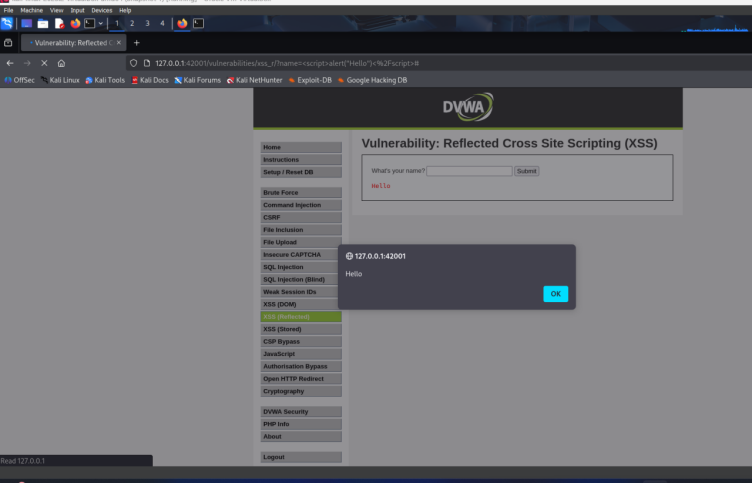
For each vulnerability we list payloads that work at LOW, test the same payloads at

MEDIUM/HIGH, observe differences, and identify the defense mechanism DVWA adds at higher security levels.

REFLECTED XSS

* Vulnerability:Reflected (XSS)
* LOW-LEVEL PAYLOAD:(works)

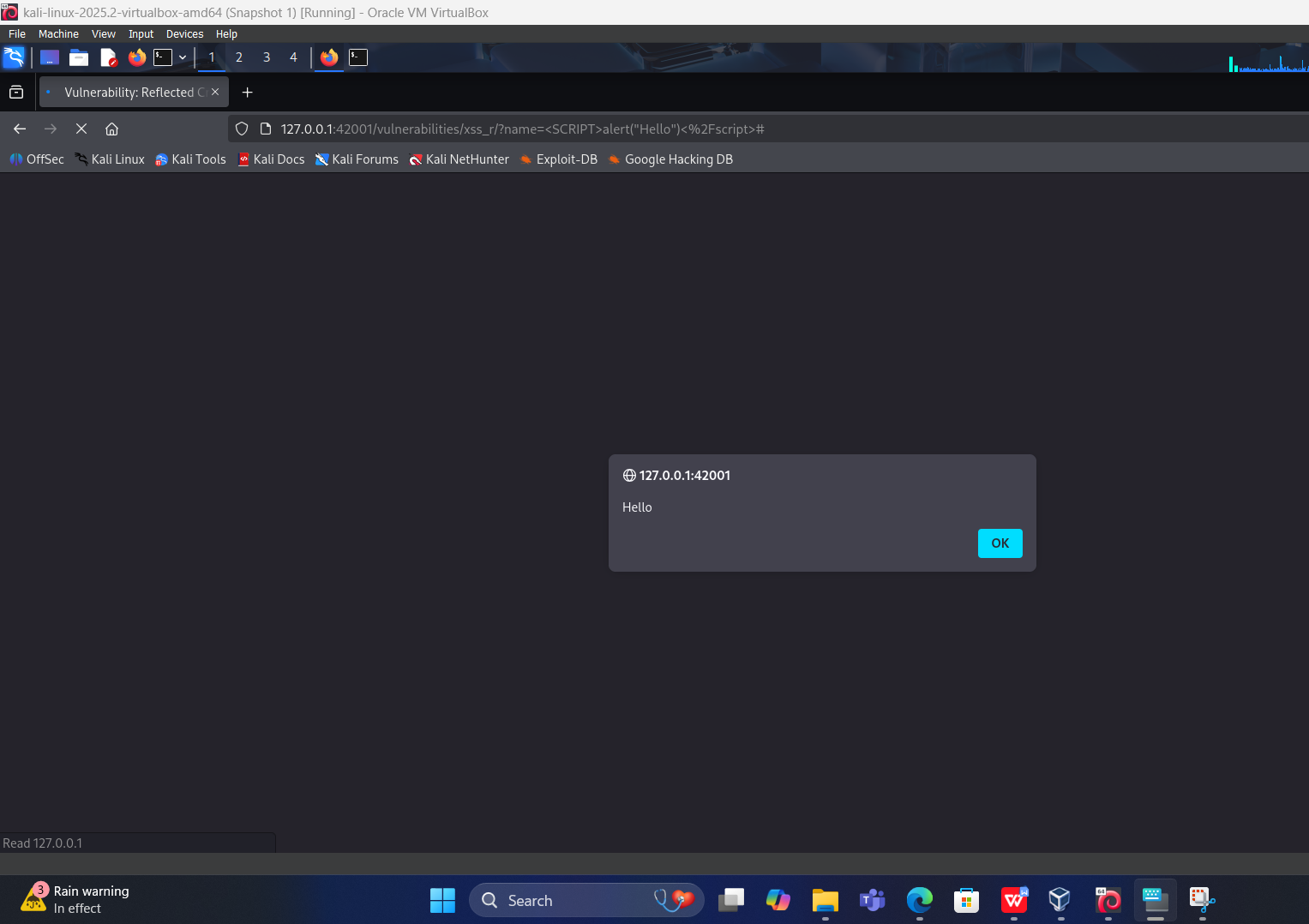
<script>alert(“hello”)</script>



* MEDIUM-LEVEL-OBSERVATION:The same payload may be filtered or case-normalized.

Example noted: <SCRIPT>alert("Hello")</script>

At MEDIUM, DVWA attempts basic filtering or encoding that blocks some script tags, but alternate casing can sometimes bypass it.

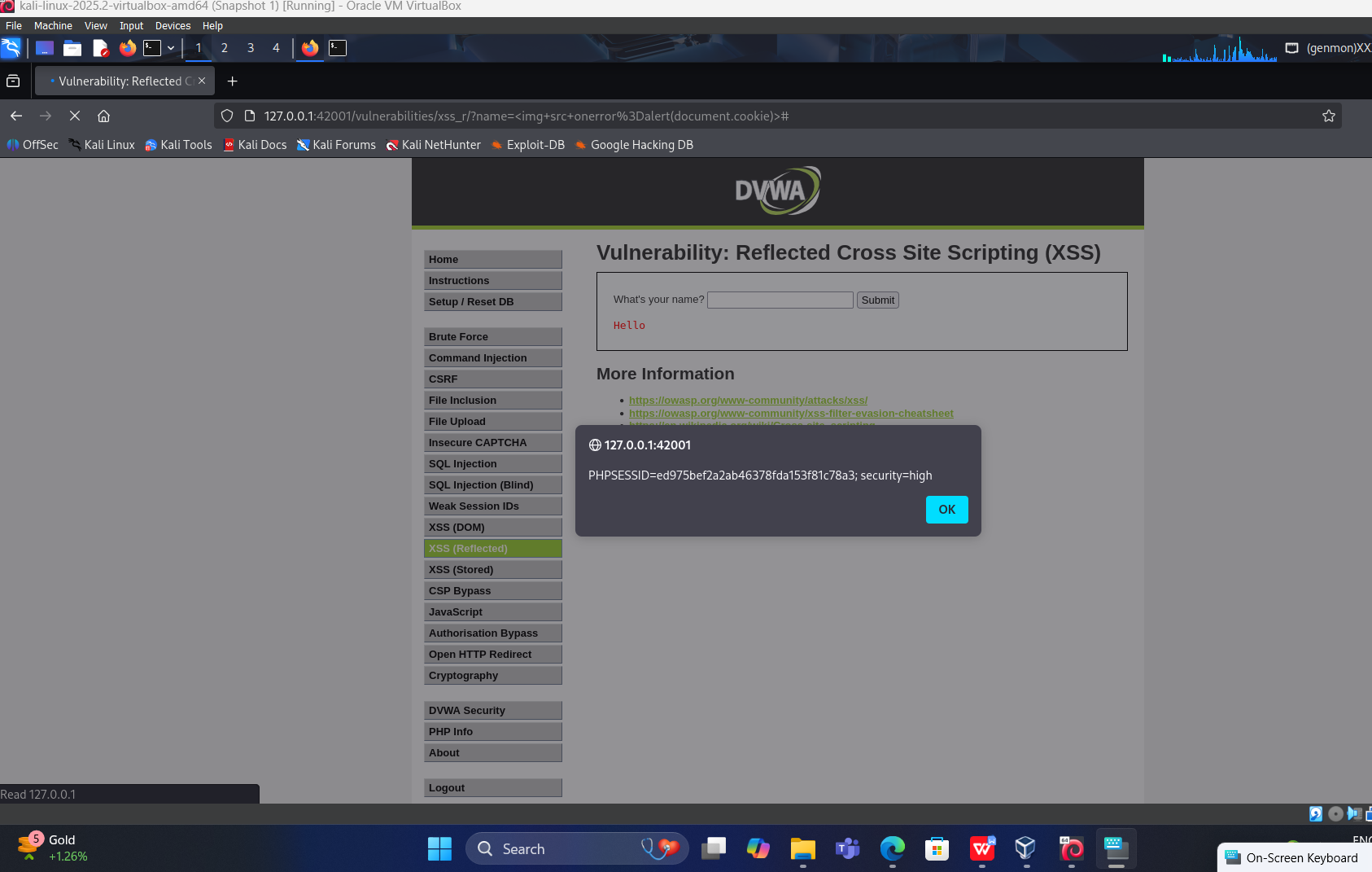


* HIGH-LEVEL OBSERVATION:

At HIGH, DVWA replaces direct script execution with outputs(e.g., stricter HTML-encoding).

Example payload: <img src onerror=alert(document.cookie)>

This shows attackers switch to event-handler attributes to test if filters are strict enough.



COMMAND INJECTION:

* VULNERABILITY:Command Injection
* LOW-LEVEL PAYLOAD:(works)

127.0.0.1; ls (appends a shell command seprated by ;)

* MEDIUM-LEVEL-OBSERVATION:

Payload example:127.0.0.1 & 0 ls

At MEDIUM, special characters like ; and & may be blocked or escaped, stopping the

injection.

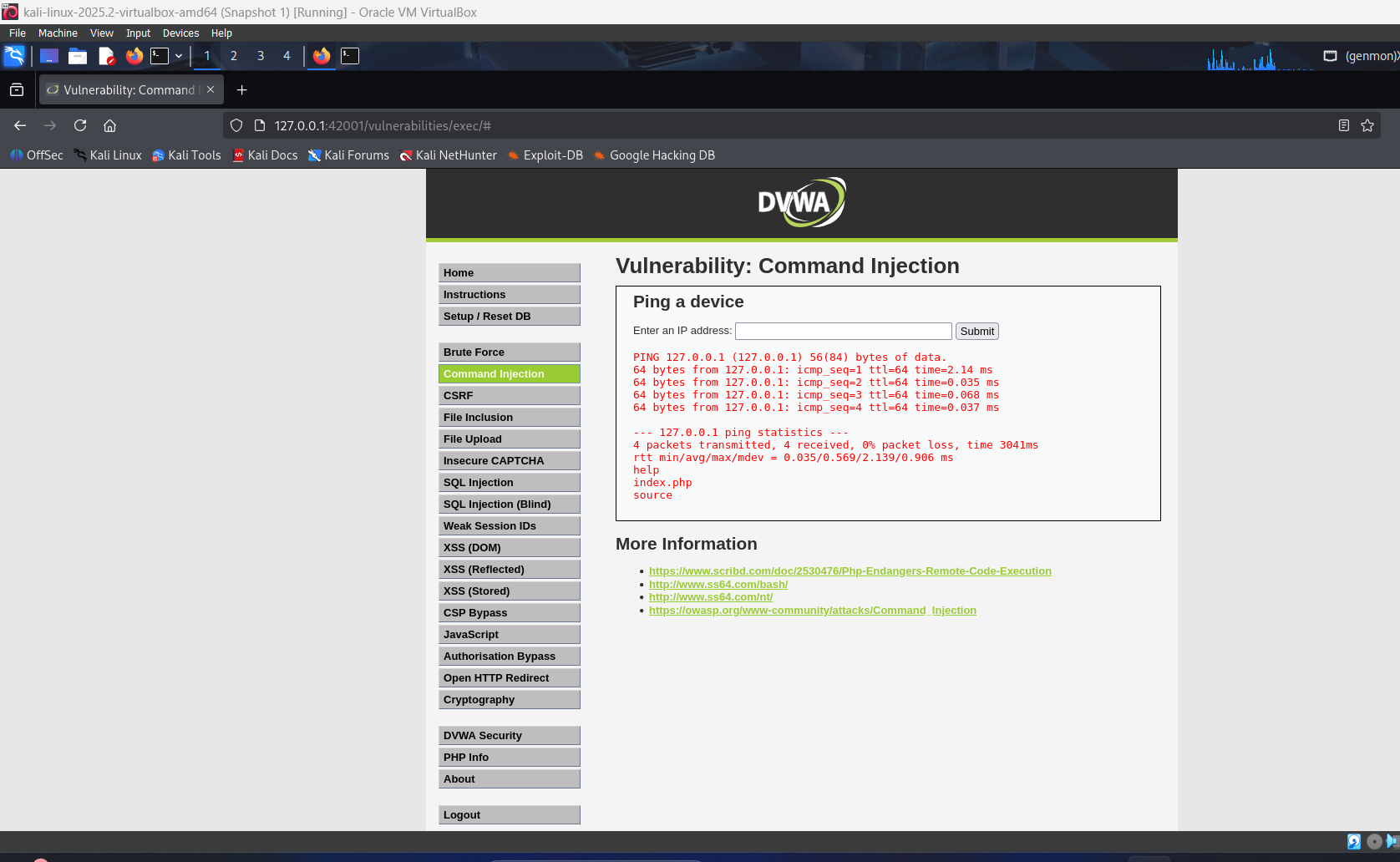
• High-level observation:

At HIGH, DVWA validates input strictly (only digits or IP patterns) or uses

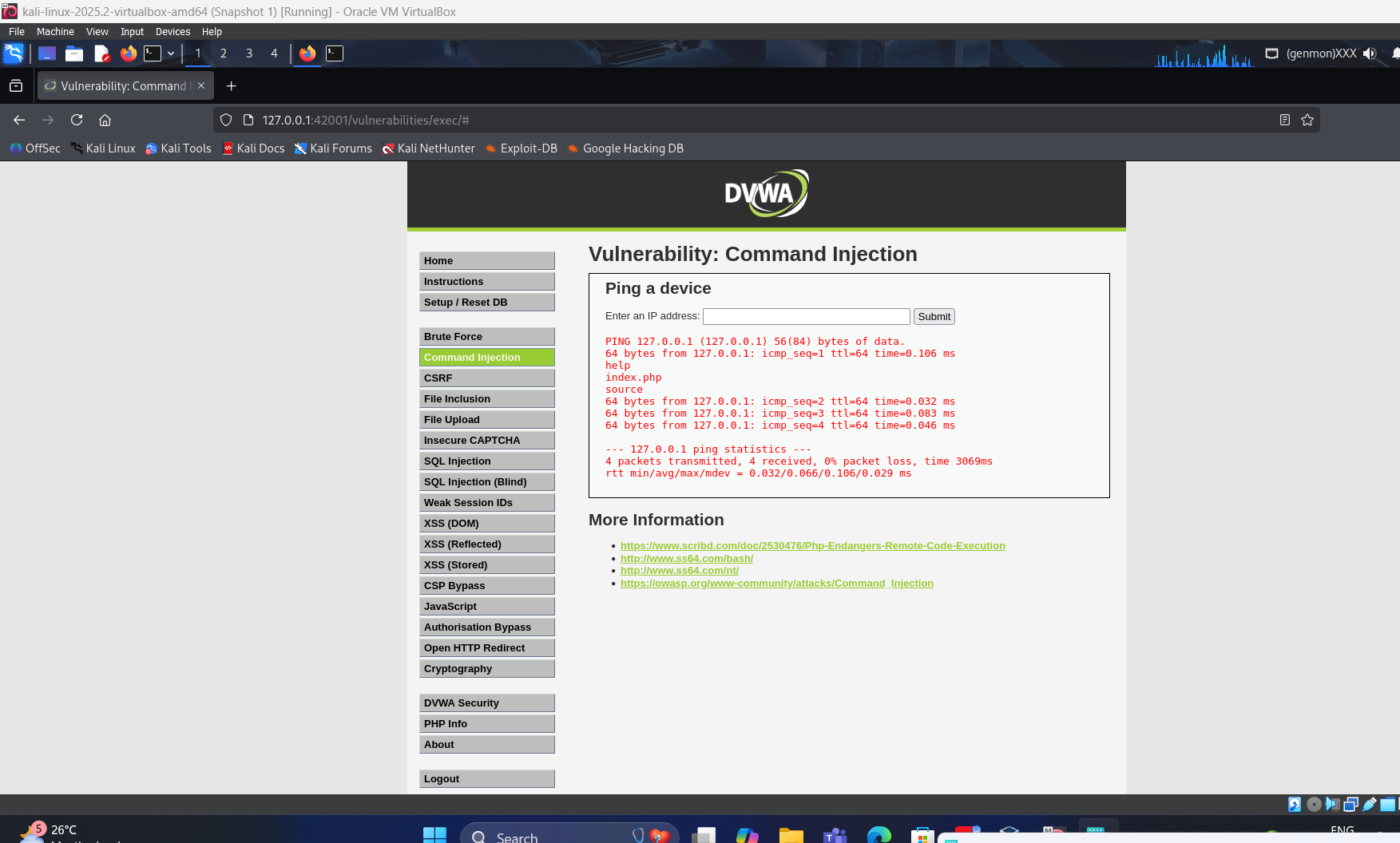
parameterized execution rather than direct shell commands.

This prevents metacharacters (; & ||) from being executed.

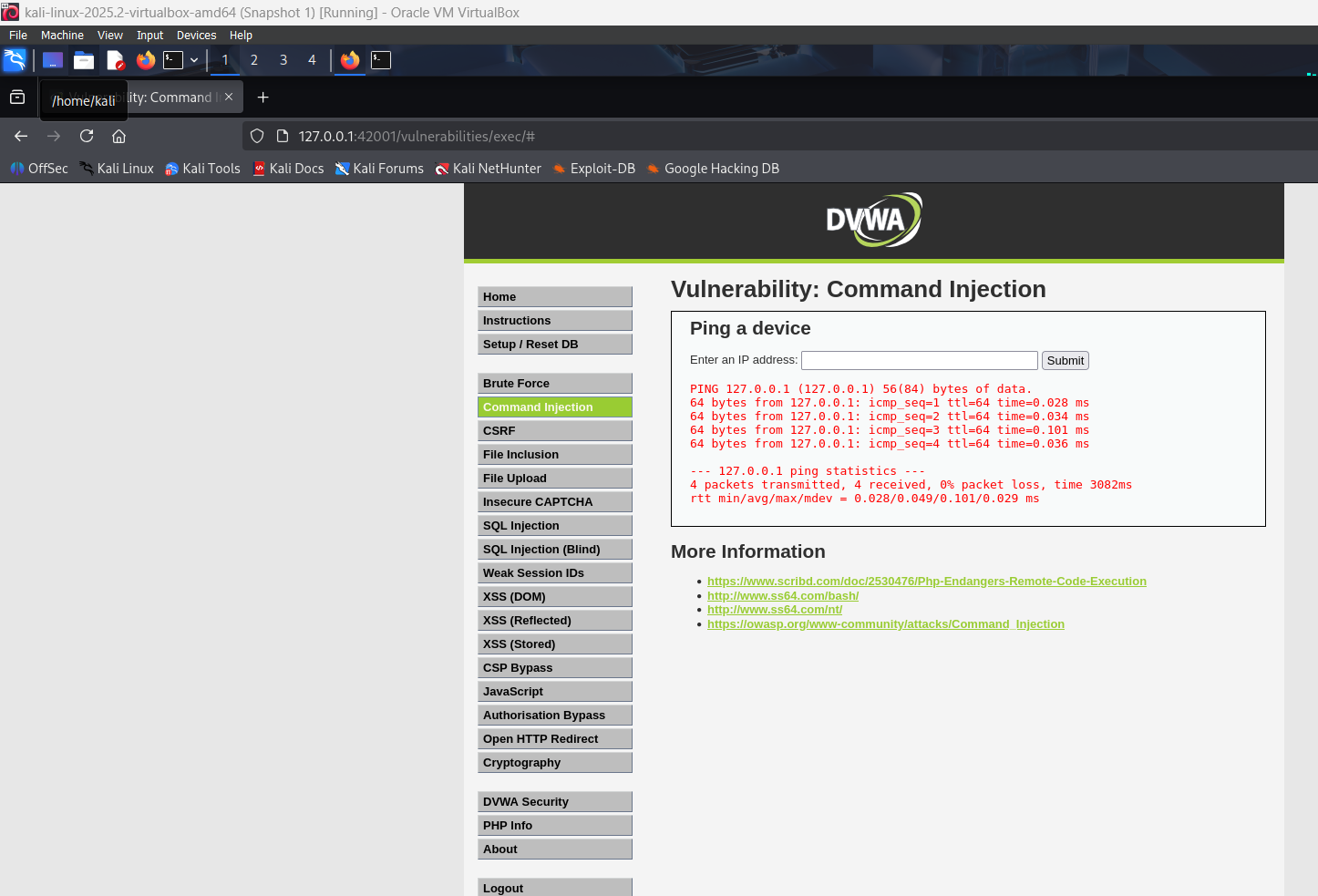
Security level Low:127.0.0.1; ls



Security level Medium:127.0.0.1&ls



Security level high :127.0.0.1



Summary & Recommendations

• DVWA shows how defenses improve step-by-step across LOW → MEDIUM → HIGH.

• Common defenses used:

o Output encoding

o Input sanitization / whitelisting

o Escaping special characters

o Avoiding direct shell commands (using parameterized APIs instead)