# Command Injection Exploitation – DVWA

## Overview

This section focuses on exploiting command injection vulnerabilities in DVWA at high security level.

The target was to execute arbitrary system commands via insecure input handling.

## Tools Used

- Burp Suite (to intercept and modify HTTP POST requests)

- Linux CLI (to validate command execution)

## Techniques Applied

- Bypassing insecure blacklist filters (`|cat /etc/passwd`)

- File disclosure from the server

- Verifying execution privilege (www-data)

## Key Payloads

- `127.0.0.1|cat /etc/passwd`

- `127.0.0.1|whoami`

## Screenshots

Exploitation steps and responses are documented in the `/screenshots` folder.

---