DVWA — Command Injection (low)

Security Micro-Scan

Client: DVWA Lab
Date: 2025-09-26
Author: Braxton Beck (Ben-Frank17)
Severity: High — Command injection allows arbitrary OS command execution.

Summary

The Command Injection module forwards user-supplied input to a shell without proper sanitization. This allows command chaining and execution under the web server user.

PoC

Payload: `127.0.0.1 && whoami`
Steps

1. Login to DVWA and set Security = **low**.
2. Navigate to **Vulnerabilities** → **Command Injection**.
3. Enter payload in the IP field and click **Submit**.
4. The page returns `whoami` output `veritaspc\beckb`, proving command execution.

Evidence

- Screenshot: `dvwa_cmd_injection.png` (shows `veritaspc\beckb`)

Impact

Arbitrary command execution can lead to system compromise, data theft, lateral movement, or privilege escalation depending on server config.

Remediation

- Never pass raw input to a shell. Use safe APIs that avoid shell interpretation.
- Implement strict whitelisting (e.g., IP regex) for allowed input.
- Run required commands in minimal-privilege environments and log executions.

Retest

Confirm server rejects command separators and returns a validation error rather than executing commands.