

Answers

Reference answers for Lesson 05.

Part 1 — Lab Answers

Exercise 1 — HTTP Request Triage

Expected findings

- At least one endpoint that reflects user input in the response (XSS or template injection).
- One endpoint whose error response leaks a stack trace.
- A search/query parameter susceptible to SQL injection (error-based or time-based).
- An upload endpoint accepting an unexpected content type.

Exercise 2 — Nikto Output Ranking

Expected ratio

About 80% informational, 15% worth investigating, 5% critical. The critical findings usually include an exposed backup file, a default admin panel, or a known CVE on an identified server version.

Exercise 3 — Gobuster Directory Analysis

Expected findings

- One or more 200 responses on interesting paths (`/backup` , `/git` , `/admin` , `/.env`).
- 403s on paths worth revisiting with authentication.
- Size-clusters indicating aliases or default error pages.

Exercise 4 — Burp Finding Validation

Expected findings

- Several Burp "High" findings that are in fact Medium once you check Attack Complexity.
- At least one "Low" finding that should be High because it chains to another finding (e.g., a reflected XSS that enables CSRF + IDOR).

Final Exercise — Exploit Chain

Expected chain

Entry via an exposed path from Gobuster → credential or token capture from the HTTP request log → IDOR from Burp for privilege escalation → RCE via an endpoint found in manual testing. A good chain touches three or four sources.

Part 2 — Homework Answers

Task 1 — Burp Re-Scoring

Common disagreements

Burp often rates XSS as High; if the target site has no session context or sensitive data, Medium is more accurate. Conversely, Burp rates information disclosure as Low even when the leaked info is a credential — that should be Critical.

Task 2 — Chain Builder

Expected shape

~60 lines of Python. `--verify` mode should detect the characteristic response (status code, specific string, timing delta) and print a one-line verdict. No payload delivery — only probing.

Task 3 — Scanner Comparison

Expected priorities

Typical triage order: Gobuster first (fast attack surface), Nikto second (cheap low-hanging fruit), Burp third (depth on specific endpoints), manual last (judgment on suspicious findings). A common mistake is running Burp first — it is slow and noisy without a shortlist of targets.