

Homework — DLP While Using AI

~20 minutes · 3 prompts to redact

For each prompt below, (1) classify it using the four-class model, (2) produce the minimum-viable redacted version that still lets an AI help, (3) list what you removed and why.

Task 1 — Python stack trace

A coworker sends you the following stack trace and asks for help figuring out why the checkout endpoint is failing in production. They want to paste it into an AI assistant.

```
Traceback (most recent call last):
  File "/srv/acme/orders/api.py", line 142, in checkout
    user = db.get_user("jane.smith@acme.corp")
  File "/srv/acme/orders/db.py", line 58, in get_user
    conn = psycopg2.connect(DATABASE_URL)
psycopg2.OperationalError: could not connect to server:
  Connection timed out
  Is the server running on host "db-prod-3.internal.acme.corp"
  and accepting TCP/IP connections on port 5432?

Request headers:
  Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiI0MiJ9.aB7xQ
  X-Request-Id: 7f3b2c9a-1d4e-4a8b-9c01-ee22ff445566
```

Answer the three questions:

1. Which of the four classes does this belong to?
2. Write the minimum-viable redacted version you would be comfortable pasting into an AI.
3. List every value you removed and explain why.

✓ **Self-check:** your redacted version no longer contains any real hostnames, email addresses, or tokens, but the model can still tell this is a Postgres

connection timeout from a checkout endpoint.

Task 2 — SQL query

An analyst wants help optimizing the following query, which is slow in production. They plan to paste it into an AI assistant to ask for index suggestions.

```
SELECT o.order_id, o.total, o.status, o.created_at
FROM orders_prod_2026 o
WHERE o.customer_id = 'cust_84312'
      AND o.created_at >= '2026-01-15'
      AND o.created_at < '2026-02-15'
      AND o.status IN ('paid', 'shipped', 'refunded')
ORDER BY o.created_at DESC
LIMIT 100;
```

Answer the three questions:

1. Which of the four classes does this belong to?
2. Write the minimum-viable redacted version that still lets the AI suggest indexes.
3. List every value you removed and explain why.

✓ **Self-check: your redacted version no longer contains the real production table name or the real customer ID, but the AI can still recommend an index on the remaining filter columns.**

Task 3 — Auth bug report

A support engineer drafts the following bug report and wants to paste it into an AI assistant to brainstorm possible causes.

Bug: session refresh broken for alice@acme.corp

User alice@acme.corp reports that POST /api/v2/sessions/refresh is returning HTTP 401 for her even though her session cookie SESSION=abc123xyz789qrs456tuv000mno111pqr222 is still well inside its configured 24h TTL. She can log in fresh without

issue, but refresh always fails. I reproduced this on my side using her exported cookie jar.

cc @platform-core @identity-team — any ideas before I open an incident?

Answer the three questions:

1. Which of the four classes does this belong to?
2. Write the minimum-viable redacted version, or explain why there is no acceptable redacted version.
3. List every value you removed and explain why.

✓ **Self-check: your answer recognizes that a live session cookie belonging to a real user is in the "never" class, and your redacted version (if any) describes the bug in abstract terms without quoting the cookie value at all.**