Kiwi Kloset — Deliverable 3 Summary

■ Security Protections

1. SQL Injection Protection — Prevents attackers from injecting malicious SQL code into database queries. Prepared statements ensure input is treated only as data, never as executable code.

```
$stmt = $pdo->prepare('SELECT * FROM rentals WHERE costume_id = ?');
$stmt->execute([$costume_id]);
```

2. XSS (Cross-Site Scripting) Protection — Escapes user input so that malicious JavaScript cannot execute in browsers, converting unsafe symbols to harmless text.

```
function h($s) { return htmlspecialchars($s, ENT_QUOTES, 'UTF-8'); }
```

3. HTTP Security Headers — Adds browser-level protection to prevent clickjacking, MIME type spoofing, and unauthorized external scripts.

```
header('X-Frame-Options: SAMEORIGIN');
header('X-Content-Type-Options: nosniff'); header('Referrer-Policy:
strict-origin-when-cross-origin'); header("Content-Security-Policy:
default-src 'self';");
```

■ Easy Tweaks for Custom Statistics

Least Rented Costumes (SQL)

```
SELECT costume_id, COUNT(*) AS times_rented FROM rentals GROUP BY
costume_id ORDER BY times_rented ASC LIMIT 10;
```

Lowest Revenue (SQL)

```
SELECT costume_id, SUM(total_cost) AS revenue FROM rentals GROUP BY
costume_id ORDER BY revenue ASC LIMIT 1;
```

Top 5 Categories (SQL)

```
SELECT c.name, COUNT(r.rental_id) AS total FROM category c JOIN
costumemodel m ON m.category_id = c.category_id JOIN rentals r ON
r.costume_id = m.model_id GROUP BY c.name ORDER BY total DESC LIMIT 5;
```

Monthly Rentals per Branch (PHP)

```
$stmt = $pdo->prepare('SELECT branch_id, COUNT(*) AS total FROM
rentals WHERE MONTH(rented_at)=MONTH(CURDATE()) GROUP BY branch_id');
```

Developed by: Taj Dhillon — COMPX Deliverable 3

University of Waikato | Project: Kiwi Kloset