Case Study

Group 8

GRUN, David
GUADALUPE, John Oliever
MAKAYAN, Amorsolo
MARIANO, Yuan Andrei

SECURITY VULNERABILITIES

Understanding Authentication Flow

- The authentication process **begins in login.php**, where a session is started and the user submits their username and password through a login form and validated.
- Access to index.php is **restricted by checking the existence of the session variable.** If the session is valid, the user is granted access; otherwise, they are redirected back to the login page.
- The logout process is **handled by logout.php,** which destroys the active session and effectively ends the user's authenticated state.

System Vulnerabilities

- The username and password for the database is **hard coded in the code base.**

- Credentials are **stored in plain text** and passwords are **not hashed.**

- System **lacks input validation**, session expiration, and CSRF token validation.

Error Handling

Simple error handling mechanisms are **set into the system using try, catch, and die**. Though implemented, this is not a user-friendly approach.

The use of the die() function **may expose sensitive error information to users**, which **can potentially compromise system security** if not properly managed.

The system **lacks logging features** for documentation and debugging.

Strengthening the Front Line: Input Validation

- Identify and control multiple user input points to **reduce the system's attack surface**.
- Eliminate reliance on outdated sanitization **to close security gaps** and **align with modern standards.**
- Protect data integrity and system trust by **enforcing consistent, robust input handling.**

Preventing Cross-Site Scripting (XSS)

Neutralize injected content by **treating all dynamic output as untrusted** at render time.

Enforce output escaping consistently to **prevent malicious scripts** from executing in the browser.

Strengthen defense in depth **to safeguard users even if upstream data sources** are compromised.

Securing User Sessions and Identity

- Harden session management **to prevent fixation, hijacking, and unauthorized access.**
- **Reduce exposure to credential theft** through secure cookies and session ID rotation.
- Limit risk on shared devices by **enforcing automatic inactivity-based session termination.**

Strategic Safeguards: CSRF and Proactive Logic

- Prevent unauthorized actions by **blocking forged requests** against authenticated users.
- Verify user intent on sensitive operations **through cryptographically** secure CSRF tokens.
- Minimize blast radius and operational risk **using least-privilege access** and activity monitoring.

BUSINESS INSIGHTS

How CLV Drives Smarter Business Decisions

- CLV tiers (Bronze–Platinum) **shift focus from short-term sales to long-term revenue contribution**, helping prioritize the customers that matter most.
- By quantifying future value, the business **can justify higher spend on retention, loyalty programs, and premium service** for high-CLV customers.
- CLV visibility **enables executives to allocate budget, sales effort, and marketing intensity** based on expected lifetime returns, not guesswork.

How Data & Segmentation Improve Revenue and Retention

- Customer segmentation and CLV tiers **enable targeted marketing, improving conversion rates** while reducing wasted spend on low-value audiences.
- High-value segments (e.g., Platinum, Gold) **support personalized offers and proactive retention strategies** that directly protect revenue.
- Exportable insights and dashboards **empower faster, data-driven decisions across marketing, sales**, and management without technical dependency.

Strategic Business Learnings and Future Value

Automation, APIs, and standardized exports **transform analytics into reusable business assets** that scale across teams and systems.

Strong testing and quality controls **ensure leaders can trust insights when making high-impact decisions** on pricing, campaigns, and growth.

The system positions the business to **move from descriptive reporting to predictive, CLV-driven strategy** for sustainable long-term growth.

Part 9 Business Insights

- Problem: System hits a performance limit at ~500K records, causing dashboard latency and reduced usability.
- Root Cause: Excessive CPU workload (≈75M operations per clustering run) and inefficient full-table scans for basic queries.
- Solution: Shift computation to the data layer using PostgreSQL indexing and materialized views, enabling faster, precomputed insights.
- Impact: Delivers an instant-response dashboard, supports 1M+ records without added infrastructure costs, and ensures stability during critical reporting periods.

Part 10 Business Insights

- Key Takeaway: The custom solution delivers more value than off-the-shelf tools because it clearly shows how customers grow with the brand—not just how much they spend today.
- Growth Opportunity: While most customers fall into lower-spending groups, two smaller premium segments represent a major revenue upside. Concentrating $45K on ~1,300 high-value customers offers the strongest return on marketing investment.
- Cost Advantage: Building in-house instead of paying for a large SaaS platform saves about $29K per year starting in Year 2. These savings can be redirected straight into marketing, effectively funding premium campaigns at no extra cost.
- Executive Focus: Tracking how customers move from lower to higher-value segments provides leadership with a clear view of future revenue and brand loyalty.