SECURING DGKART SHOPPING CART APPLICATION

OVERVIEW OF SECURITY FINDINGS AND RECOMMENDATIONS

Presented by:
Nischal Subedi

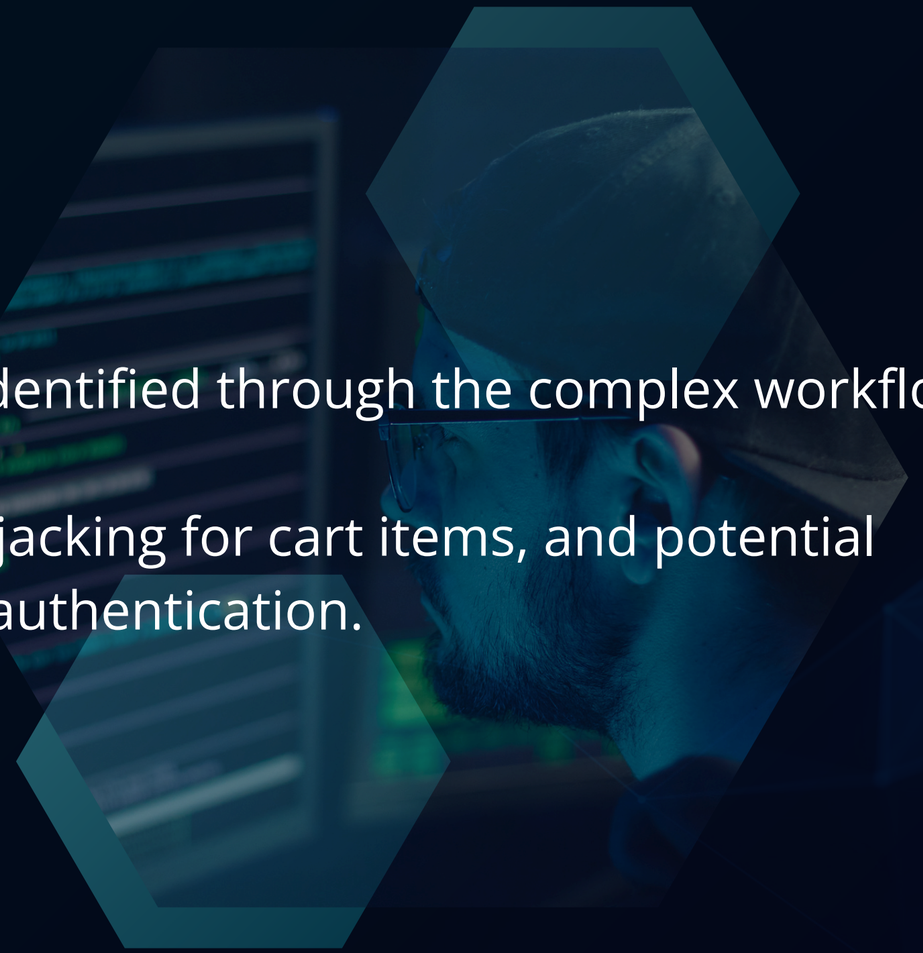
INTRODUCTION

- Brief Overview:
  - Purpose of the presentation is to provide an overview of the key security findings from the detailed report.
  - Focus on actionable recommendations for securing the DGKart platform.
- Agenda:
  - Complex workflows such as accessing the scoreboard, editing comments, etc.
  - Revised security questionnaire focusing on developers, IT team, and management, with yes/no objective questions.
  - New workflow steps based on OWASP Juice Shop.

KEY SECURITY FINDINGS

Top 3 Vulnerabilities Identified:

- SQL Injection
- Broken Authentication
- Sensitive Data ExposureNew vulnerabilities identified through the complex workflows (Scoreboard Access, Comment Editing).
- Ensure to cover workflows such as session hijacking for cart items, and potential vulnerabilities in browsing products without authentication.

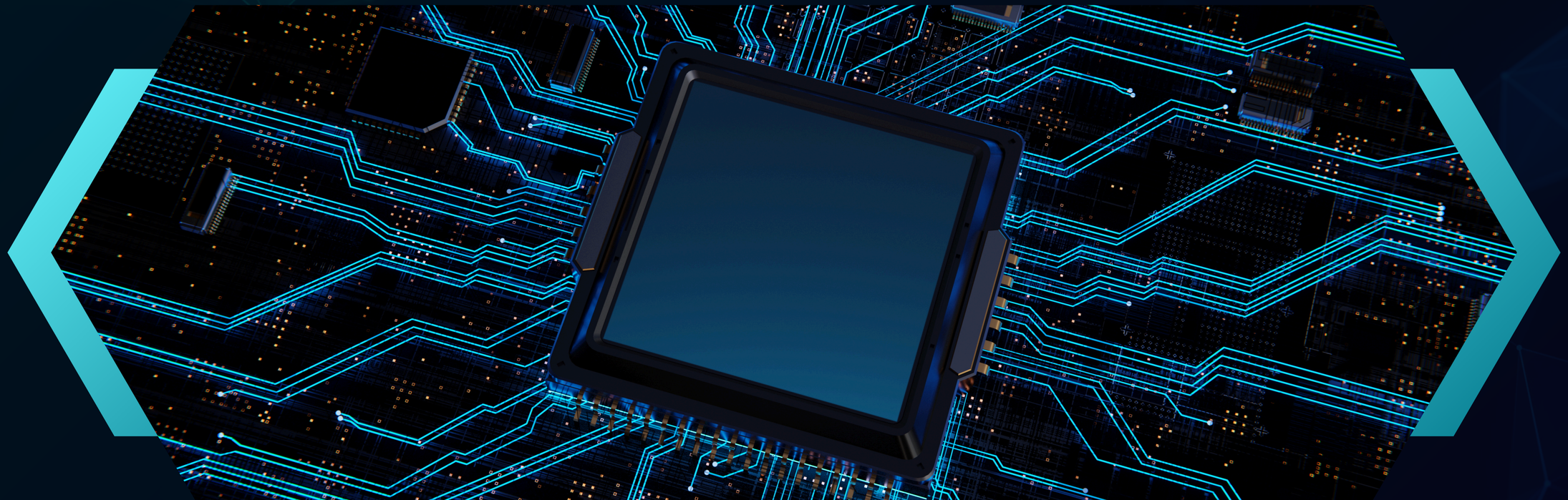


High-Risk Impacts:

Data breaches, unauthorized access, financial loss.

VULNERABILITY 1 — SQL INJECTION

- **Severity: High (9.0 CVSS Score)**
- **Impact: Unauthorized database access leading to data leakage.**
- **Recommendation: Use parameterized queries and prepared statements to prevent SQL Injection.**



VULNERABILITY 2 — BROKEN AUTHENTICATION

- Severity: High (8.5 CVSS Score)
- Impact: Unauthorized access due to weak password policies and no MFA.
- Recommendation: Enforce strong password policies and implement Multi-Factor Authentication (MFA).

VULNERABILITY 3 — SENSITIVE DATA EXPOSURE

- Severity: Medium (7.0 CVSS Score)
- Impact: Financial fraud and identity theft due to unencrypted sensitive data.
- Recommendation: Encrypt sensitive data both in transit and at rest using HTTPS and secure storage.

RECOMMENDATIONS

01

Fix SQL Injection vulnerabilities during scoreboard access and cart item modification.

02

Enforce strong password policies and implement MFA, especially in critical workflows like comment editing and payment checkout.

03

Add recommendations related to session security during workflows like adding items to the cart and accessing the scoreboard.

NEXT STEPS

- Timeline for Implementation:
  - Prioritize high-severity vulnerabilities (SQL Injection, Authentication) within the next 2 weeks.
  - Medium-severity issues (Sensitive Data Exposure) addressed within 4 weeks.

- Follow-up Audits:
  - Schedule regular security audits every 6 months.

THANK YOU