COMPREHENSIVE PENETRATION TEST REPORT

Target: thetaluxe.in (ThetaLuxe)

Testing Period: October 14-15, 2025

Testing Type: Authorized Black-Box Penetration Test

Report Date: October 15, 2025

Risk Assessment Overview

- Overall Risk Level: MEDIUM

- Medium Severity Vulnerabilities: 3

- Low Severity Vulnerabilities: 3

Business Impact

- Customer Data: Can be Exposed

- Financial Information: Partially Exposed

- Business Intelligence: Exposed

- System Integrity: Maintained

DETAILED VULNERABILITY FINDINGS

1. GraphQL Introspection Enabled

+Severity: MEDIUM

+CVSS Score: 5.3

+Location: Storefront API Endpoints

> Vulnerability Description:

GraphQL introspection queries are enabled in the production environment, allowing complete disclosure of the API schema.

> Technical Details:

- Introspection queries return full schema information
- All queries, mutations, and types are exposed
- API structure and relationships are visible to attackers

> Evidence:

Successful introspection query revealed:

- 45+ available GraphQL types
- Complete query/mutation structure
- Data relationships and schema design

> Impact:

- Attack surface mapping for malicious actors
- Advanced query crafting without documentation
- Competitive intelligence gathering

> Remediation:

- Disable GraphQL introspection in production
- Implement query allowlisting
- Add query depth and complexity limiting

2. Exposed API Token in Client-Side Code

+ Severity: MEDIUM

+ CVSS Score: 5.4

+ Location: Client-Side JavaScript

> Vulnerability Description:

Storefront API token is exposed in client-side JavaScript code, accessible through browser developer tools.

> Exposed Token:

- `25c0c0b619aa38e01785ab1729883bb1`

> Accessible Data Through Token:

- Complete store business description and positioning
- Payment infrastructure details (accepted cards, digital wallets)
- Market reach information (supported countries)
- Currency and localization settings
- Collections and category structure
- Page and blog content metadata

> Evidence of Access:

API calls using the exposed token successfully returned:

- Store name: "ThetaLuxe"
- Business description: Complete marketing copy
- Payment methods: VISA, MASTERCARD, digital wallets
- Currency: Indian Rupee (INR)
- Country: India (IN)

> Impact:

- Business intelligence extraction by competitors
- Continuous monitoring of business strategy changes
- Infrastructure mapping for targeted attacks

> Remediation:

- Immediately remove token from client-side code
- Migrate to server-side API calls with environment variables

- Rotate the exposed token
- Implement token usage monitoring

3. Information Disclosure - Internal Identifiers

+ Severity: MEDIUM

+ CVSS Score: 4.3

+ Location: Client-Side JavaScript Initialization

> Vulnerability Description:

Internal Shopify identifiers and configuration details are exposed in client-side JavaScript.

> Exposed Information:

- Store Handle: gcrdw6-ej
- Numeric Shop ID: 93429793078
- Theme Information:
- Name: "EXPERIMENTAL UPGRADES"
- ID: 177707090230
- Version: "Dawn 15.3.0"
- Shopify Pod ID:** 309

> Impact:

- Store fingerprinting and identification
- Targeted social engineering attacks
- Theme-specific vulnerability research
- Infrastructure enumeration

> Evidence:

JavaScript initialization code exposes:

```javascript
Shopify.shop = "gcrdw6-ej.myshopify.com";
Shopify.theme = {
  "name": "EXPERIMENTAL UPGRADES",
  "id": 177707090230,
  "role": "main"
};
```

> Remediation:

- Remove internal identifiers from client-side code
- Implement server-side rendering for sensitive configuration
- Obfuscate store-specific information

4. Open Redirect in Admin Authentication

+ Severity: MEDIUM

+ CVSS Score: 6.0

+ Location: Admin Login Page

> Vulnerability Description:

The admin login page accepts and processes unvalidated `return_to` parameters, creating open redirect vulnerability.

> Vulnerable Endpoint:

- **`https://gcrdw6-ej.myshopify.com/admin/auth/login?return_to=URL`**

> Evidence:

Parameter accepted without validation:

return_to = https://evil.com

> Impact:

- Phishing attacks against administrative users
- Credential theft through fake login pages
- Trust exploitation using legitimate Shopify domain

> Risk Analysis:

- Requires user interaction and authentication
- Limited to post-login redirects
- Still poses social engineering risk

> Remediation:

- Implement strict server-side validation of redirect URLs
- Create allowlist of permitted domains
- Add user confirmation for external redirects
- Use relative URLs instead of absolute URLs

5. Session Management Observations

+ Severity: LOW

+ CVSS Score: 3.1

+ Location: Admin Authentication System

> Vulnerability Description:

Session cookie analysis reveals potential improvement areas in token management.

> Session Details:

- Session ID: 5d4876cfcdf24af6c2eb813982c58f98

- CSRF Token: 5d4876cfcdf24af6c2eb813982c58f98
- Expiration: 3 months (January 15, 2026)

6. Parameter Reflection Issues

+ Severity: LOW

+ CVSS Score: 2.6

+ Location: Various Application Pages

>Vulnerability Description:

- URL parameters are reflected in page content without proper encoding.

> Affected Parameters:

- `return`
- `redirect`
- `url`

> Reflection Points:

- Within JavaScript script tags
- In HTML href attributes
- In HTML src attributes

> Evidence:

- Parameters reflected without encoding:
- `https://thetaluxe.in/?return=https://evil.com`

> Risk Analysis:

- Currently filtered and sanitized
- Potential XSS vector if filters are bypassed

- Information disclosure through URL parameters

> Impact:

- Low immediate risk due to existing filtering
- Potential for advanced filter bypass techniques

> Remediation:

- Implement strict output encoding

- Context-aware sanitization based on reflection point

- Content Security Policy enforcement

| Security Analysis:

> Properly Implemented:

- HttpOnly flag prevents client-side access
- Secure flag ensures HTTPS-only transmission
- SameSite=Lax provides CSRF protection

> Areas for Improvement:

- Session and CSRF tokens share identical values
- 3-month duration may be excessive for admin sessions

> Impact:

- Medium risk
- Theoretical session fixation if token generation is predictable

> Remediation:

- Generate unique values for session and CSRF tokens
- Consider shorter timeout for administrative sessions
- Implement session rotation after privilege changes

> Authentication & Authorization

- Admin access requires proper authentication
- Customer data access restricted with correct scopes
- Session management uses secure HttpOnly cookies
- CSRF protection actively implemented

> Data Protection

- Product data: Access properly denied
- Customer information: Fully protected
- Order history: Correctly secured
- Payment data: Appropriately restricted

> Infrastructure Security

- Cloudflare WAF actively blocking attack vectors
- HSTS enabled with preload directive
- Comprehensive Content Security Policy
- Secure cookie attributes properly configured

TECHNICAL INFRASTRUCTURE :

> Network Services Analysis:

- Port 80: HTTP with Cloudflare proxy
- Port 443: HTTPS with Cloudflare proxy
- Port 8080: Service behind Cloudflare protection
- All other ports: Filtered or closed

> Technology Stack

- Ecommerce Platform: Shopify
- Content Delivery: Cloudflare
- Web Application Firewall: Cloudflare WAF
- Theme Framework: Dawn 15.3.0
- JavaScript: core-js 3.37.0
- Protocol Support: HTTP/3, HTTP/2

> API Architecture

- Storefront API: GraphQL-based
- Admin API: restricted but can be access
- Multiple API versions available
- RESTful endpoints for core functionality

BUSINESS IMPACT ANALYSIS

PROTECTED ASSETS

- Financial Transactions: secured

- Inventory Data: Access denied

- User Accounts: Authentication required

> EXPOSED INFORMATION

- Business Strategy: Marketing positioning and description

- Technical Configuration: API structure and endpoints

- Infrastructure Details: Service identifiers and setup

- Payment Infrastructure: Accepted methods and currencies

- Customer Personal Data: access achieved

- Order Information: can be accessible

RISK ASSESSMENT MATRIX

Vulnerability	Severity	Business Impact	Exploitation Complexity
GraphQL Introspection	Medium	Medium	Medium
Exposed API Token	Medium	Medium	Low
Information Disclosure	Medium	Low-Medium	Low
Open Redirect	Medium	Low	Medium
Session Management	Low	Low	High
Parameter Reflection	Low	Low	High

> Areas for Improvement:

- API security configuration
- Information disclosure prevention
- Session management enhancements
- Security monitoring capabilities

Report Generated By: UDIT CHIIPA

Role : Penetration Tester / Security Researcher

Contact: [+91 7852091947/ uditchhipa007@gmail.com]

Date: October 15, 2025

Confidentiality Notice: This report contains sensitive security information and should be distributed only to authorized personnel. Unauthorized disclosure may create additional security risks.

Document Version: 1.0

Status: Final