

**SECURDE**

Threat Model Document

|  |  |
| --- | --- |
| **Section** | S20 |
| **Team Members** | Fernandez, Ryan Austin  Hade, Alden Luc R.  Poblete, Clarisse Felicia M.  Syfu, Jonah E. |
| **Date Submitted** | July 13, 2016 |

**Table of Contents**

I. Security Objectives

II. Application Profile

III. Threat Documentation

1. Threat List
2. STRIDE/DREAD Model

IV. References

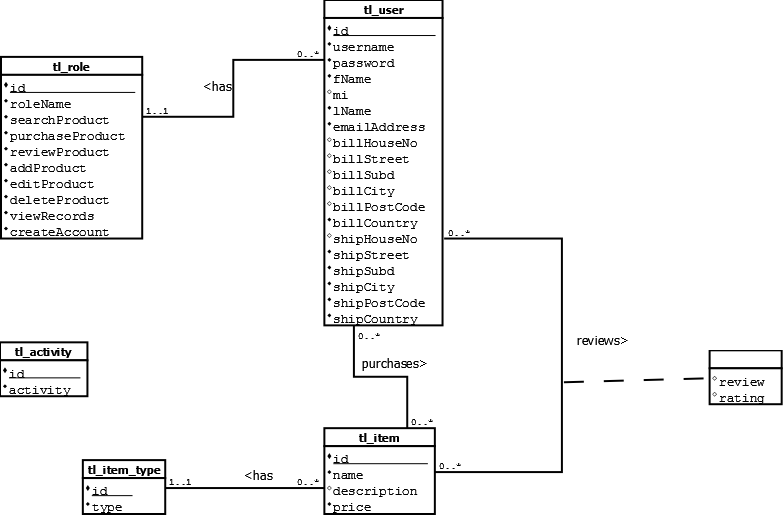
**I. Security Objectives**

**II. Application Profile**

This section is a profile of the Talaria Footwear Online Portal. This section is divided into four parts, the ERD Model, User Roles, the Class Diagram, and the Data Flow diagram

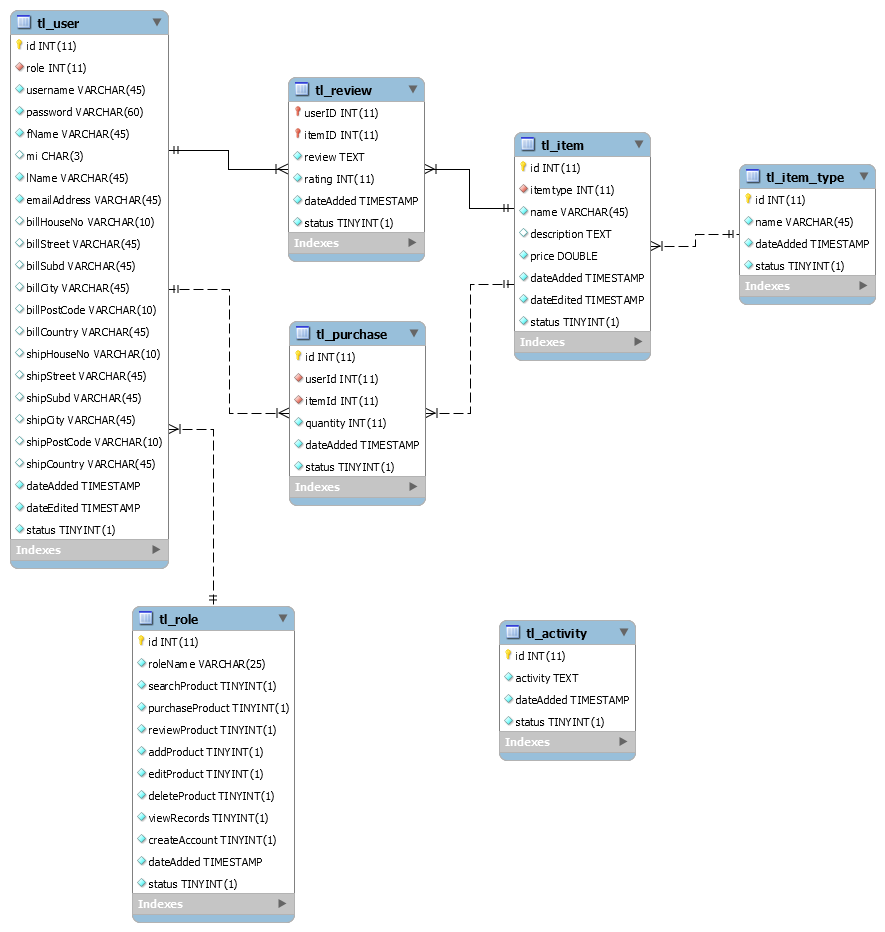
**ERD Model**

Figure 1 shows the ERD of the Talaria Footwear online portal.



**Figure 2.1. – Entity-Relationship Model of Talaria Footwear Online Portal**

Users have a username, password, first name, middle initial, last name, email address, billing address (house no., street, subdivision, city, post code, country), and shipping address(house no., street, subdivision, city, post code, country).



**Figure 2.2. – Relational Model of Talaria Footwear Online Portal**

**User Roles**

|  |  |
| --- | --- |
| Role | Description of Tasks |
| Customer | * Search product * Purchase Product * Review product (that they have purchased) |
| Product Manager | * Add Product * Edit Product * Delete Product |
| Financial Manager | * View purchase records: total sales, sales per product type, or sales per product. |
| Admin | * Create product manager or financial manager account |

**III. Threat Documentation**

This chapter is divided into two parts: the threat list documents each threat in detail; the DREAD Model prioritizes each threat by using the PxI scoring method.

1. **Threat List**

**Bypass Authorization in**

* Review Product
* Add Product
* Edit Product
* Delete Product
* View Records
* Create Special Account

STRIDE Classification: Elevation of Privilege

**DoS Attack in**

* Register Page
* Login Page

STRIDE Classification: Denial of Service

**Faulty Password Timeout**

STRIDE Classification: Spoofing

**Lack of Verbosity in Audit Logs**

STRIDE Classification: Repudiation

**Lack of Password Complexity**

STRIDE Classification: Spoofing

**Login Bypass**

STRIDE Classification: Elevation of Privilege

**Session Hijacking**

STRIDE Classification: Spoofing

**SQL Injection in**

* Login Page
* Search Page
* Purchase Product URL
* Register Page
* Add Product Page
* Edit Product Page
* Delete Product Page
* Create Special Account

STRIDE Classification: Tampering of Data, Information Disclosure

**XSS Attack in**

* Login Page
* Search Page
* Register Page
* Add Product Page
* Edit Product Page
* Delete Product Page
* Create Special Account

STRIDE Classification:

1. **DREAD Model**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Threat** | **D** | **R** | **E** | **A** | **DI** | **P** | **I** | **P x I** |
| Bypass Authorization |  |  |  |  |  |  |  |  |
| DoS Attack |  |  |  |  |  |  |  |  |
| Faulty Password Timeout |  |  |  |  |  |  |  |  |
| Lack of Verbosity in Audit Logs |  |  |  |  |  |  |  |  |
| Lack of Password Complexity |  |  |  |  |  |  |  |  |
| Login Bypass |  |  |  |  |  |  |  |  |
| Session Hijacking |  |  |  |  |  |  |  |  |
| SQL Injection |  |  |  |  |  |  |  |  |
| XSS Attack |  |  |  |  |  |  |  |  |