**Threat-Risk Model**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Contents**

Security Objectives.......................................................................................................................... 2

Application Overview....................................................................................................................... 2

Roles............................................................................................................................................... 2

Key Scenarios................................................................................................................................. 2

Technologies.................................................................................................................................... 3

Application Security Mechanisms.................................................................................................... 3

Application Decomposition.............................................................................................................. 3

Trust Boundaries............................................................................................................................. 3

Data Flows...................................................................................................................................... 3

Entry Points..................................................................................................................................... 4

Exit Points........................................................................................................................................ 4

Threats ........................................................................................................................................... 4

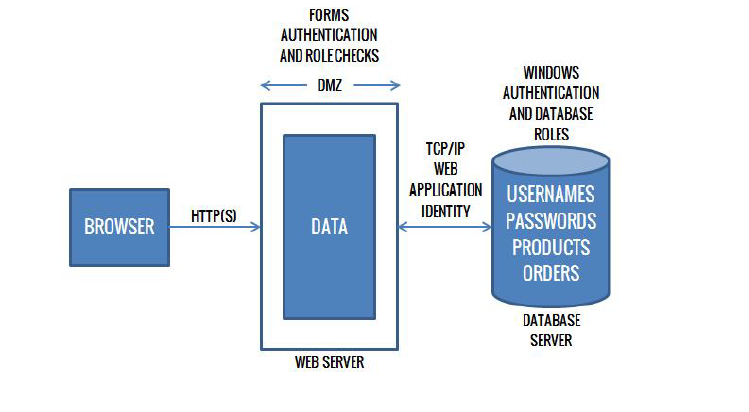
Vulnerabilities ................................................................................................................................. 5

**Security Objectives**

* Protect customer account details and customer credit history.
* Ensure that the application is available 99.99 percent of the time.
* Prevent unauthorized users from modifying product catalog information, especially prices.

**Application Overview**

The application is an Internet-facing Web application with a SQL Server back end. The Web server is located in a perimeter network. Business and data access logic resides on the Web server. The application enables Internet users to browse and purchase products from the company's product catalog.



**Roles**

* Customers
* Account Administrator
* Product Manager
* Accounting Manager

**Key Scenarios**

* Customer browses the product catalog to view product details.
* Customer searches to locate a specific product.
* Customer adds an item to the shopping cart.
* Customer logs in to authenticate prior to placing an order.
* Customer user creates a new account prior to placing an order.
* Customer places an order.
* Account administrator creates a new product manager account
* Account administrator creates a new accounting manager account
* Accounting Manager views all financial records
* Product Manager adds a new product
* Product Manager edits an existing product
* Product Manager deletes an existing product

**Technologies**

* Web Server: Apache Tomcat
* Presentation logic: Java Servlet Programming (JSP)
* Business logic: Java Class Libraries
* Data access logic: Parameterized Queries
* Database Server: MySQL Server 5.7

**Application Security Mechanisms**

* The most important application security mechanisms known at this time are:
* Users are authenticated with Forms authentication.
* Roles are used to authorize access to business logic.
* Administration can be performed only by physically logging on to the administrator account. No remote administration access is provided.

**Application Decomposition**

**Trust Boundaries**

* The perimeter firewall.
* The database server trusts calls from the Web application's identity.
* The data access components trust the business components to pass fully validated data.
* An entry point to catalog administration business component.

**Data Flows**

* A customer user browses the product catalog. The catalog page calls the catalog business component, which calls the catalog data access component to request a catalog listing. The first page of product details are retrieved from the database and returned to the catalog business component. The data is bound to a data grid control and displayed on the catalog page.
* A Customer submits a search string. The home page accepts the search string and validates it by using a regular expression. The search string must be less than 50 characters in length and may include any combination of letters or numbers. The search string is passed to the data access component. The data access component creates a prepared statement and passes the search string to the prepared statement.
* The user logs on. The user submits a name and password through the logon form. The username and password are handled by the logon page and passed to the membership business logic component. This component passes the data to the data access component, which verifies the credentials with the database to determine their validity.
* A catalog administrator logs on and accesses the restricted catalog administration page. The catalog administration component checks the user role at the business layer. If the user is authorized, the business component interacts with the catalog data access component to view and amend product details.

**Entry Points**

* Port 80 for Web requests.
* Port 443 for SSL.
* All other ports are restricted by the firewall.
* The logon page, which is accessible to all Internet users. Logon is validated by using client-side and server-side validation controls, together with a common validation library.
* The amend customer details page, which is accessible to authenticated users only. Users are validated by using client-side and server-side validation controls, together with a common validation library. This page invokes functionality that can update customer details.
* The catalog administration page.

**Exit Points**

* The search page, which writes the client's search string and the corresponding results.
* The catalog page, which displays product details.

**Threats**

* Brute force attacks occur against the dictionary store.
* Network eavesdropping occurs between the browser and Web server to capture client credentials.
* An attacker captures an authentication cookie to spoof identity.
* SQL injection occurs, enabling an attacker to exploit an input validation vulnerability to execute commands in the database and thereby access and/or modify data.
* Cross-site scripting occurs when an attacker succeeds in injecting script code.
* Cookie replay or capture occurs, allowing an attacker to spoof identity and access the application as another user.
* Information is disclosed and sensitive exception details are revealed to the client.
* An attacker manages to take control of the Web server, gain unauthorized access to the database, and run commands against the database.
* An attacker obtains the encryption keys used to encrypt sensitive data (including client credit card numbers) in the database.
* An attacker or client obtains unauthorized access to Web server resources and static files.

**Vulnerabilities**

* User password storage.
* Lack of password complexity enforcement.
* Lack of password retry logic.
* Missing or weak input validation at the server.
* Failure to validate cookie input.
* Failure to sanitize data read from a shared database.
* Failure to encode output leading to potential cross-site scripting issues.
* Exposing an administration function through the customer-facing Web application.
* Exposing exception details to the client.