

Secure Software Development

Threat Modelling, Design and Implementation of a Secure Website



April 8, 2015

Wayne Caruana

1BSC2S

Table of Contents

[Task 1 – Definition of requirements, Threat Modelling and Design (P2.1, P2.2) 2](#_Toc417920242)

[Assets 2](#_Toc417920243)

[Trust Levels 2](#_Toc417920244)

[Architecture Overview 2](#_Toc417920245)

[DFD Level 0 2](#_Toc417920246)

[Threats (At least 10) 2](#_Toc417920247)

[STRIDE 2](#_Toc417920248)

[Mitigation Strategy 2](#_Toc417920249)

[Task 2 – DFDs in Threat Modelling Document (M1.4) 3](#_Toc417920250)

[Task 3 – Implementation of Secure Website (P3.1) 3](#_Toc417920251)

[Task 4 – Documentation of security patterns and practices (P3.2, P4.3) 3](#_Toc417920252)

[Task 5 – Implementation of Further security techniques in website (M1.5) 3](#_Toc417920253)

[Task 6 – Documentation of alternative security patterns (M1.3) 3](#_Toc417920254)

[Task 7 – Security Patterns – Argue on what you cannot protect against (D1.2) 3](#_Toc417920255)

[Task 8 – Testing and Reviewing a 3rd Party application (P4.1, P4.2, P4.4) 3](#_Toc417920256)

[Task 9 – Perform Attacks on a third party application and document them (D1.3) 3](#_Toc417920257)

# Task 1 – Definition of requirements, Threat Modelling and Design (P2.1, P2.2)

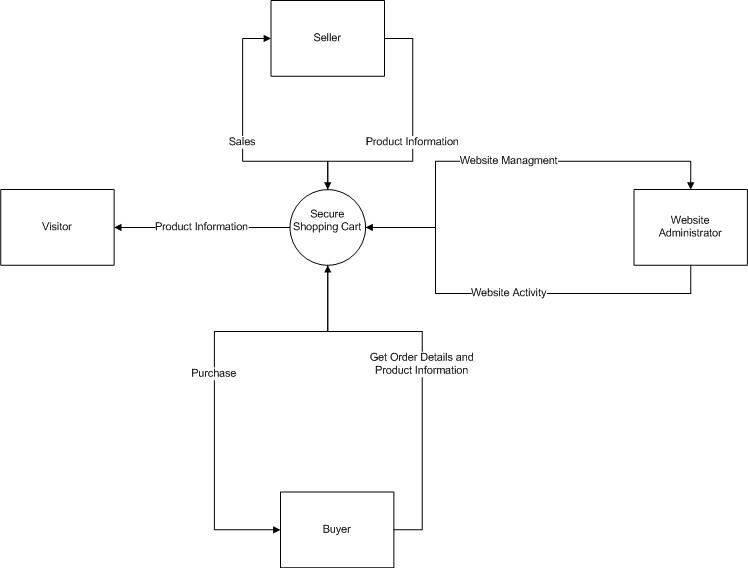
## Assets

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Trust Level |
| A1 | User | Assets that relate to a website user |  |
| A1.1 | User’s Login data | Users’ credentials username and password. This asset needs protection because if it is stolen another user would be able to do anything which the user can do. | T2 Authenticated user  T3 Website administrator |
| A1.2 | User’s Personal Data | User’s personal data including contact information. This needs protection because some personal data might be important such as telephone number. | T2 Authenticated user  T3 Website administrator |
| A1.3 | User’s public and private key | User public and private key are very valuable since one can easily decrypt valuable data | T3 Website administrator |
| A2 | Backend Database | Backend database includes all the data of all users registered into the system together with all the product and order details. All data can be found here. | T3 Website administrator |
| A3 | Product | All the products details that can be found in the database | T1 Remote anonymous user  T2 Authenticated user (Buyer)  T3 Website Administrator  T4 Authenticated user (Seller) |
| A3.1 | Products Details | All the product details that are found in the database. This includes all the product information such as prices and quantity bought. | T1 Remote anonymous user  T2 Authenticated user (Buyer)  T3 Website Administrator  T4 Authenticated user (Seller) |
| A3.2 | Product key and iv | The product key and iv which are used in order to decrypt encrypted files | T3 Website Administrator |
| A4 | Order Details | All the details that are inserted into the database that relates to the buyer. This includes all the information regarding the order such as the product bought, the price and the buyer who bought it | T2 Authenticated user(Buyer)  T3 Website Administrator |

## Trust Levels

|  |  |  |
| --- | --- | --- |
| ID | Name | Description |
| T1 | Remote anonymous user | A user who has not yet authenticated to the website |
| T2 | Authenticated user (Buyer) | A registered user who has valid credentials has only the right to buy certain items. |
| T3 | Website administrator | User who can do any operations on the website such as updating, deleting and inserting any products. |
| T4 | Authenticated user (Seller) | A registered user who can upload, edit or delete his own items in order to put them on the market. |

## DFD Level 0



## Entry Points

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Trust level |
| E1 | Web server listening port | Port on which the web server listens. All web pages are layered on this port. | T1 Remote anonymous user  T2 Authenticated user (Buyer) |
| E1.1 | Login Page | The page where a user can login or register. | T1 Remote anonymous user |
| E1.1.1 | Register Method | Create a new user login | T1 Remote anonymous user |
| E1.1.2 | Login Method | Compares user credentials to those stored in database and session is created. | T1 Remote anonymous user |
| E2 | Store Page | The page where all the products are listed | T1 Remote anonymous user  T2 Authenticated user (Buyer) |
| E2.1 | Add to Cart Method | Add a product to shopping cart | T1 Remote anonymous user  T2 Authenticated user (Buyer) |
| E3 | Manage Products Page | The page where one can add or edit products | T3 Website Administrator  T4 Authenticated user (Seller) |
| E3.1 | Create new Product Method | Creating new product. Stores a new product in the database with all its details including the file. | T3 Website Administrator  T4 Authenticated user (Seller) |
| E3.2 | Edit an existing Product | Edit new product. Updating an existing product in the database with all its details including the file. | T3 Website Administrator  T4 Authenticated user (Seller) |

## Threats

|  |  |
| --- | --- |
| ID | TR1 |
| Name | Adversary tries to supply malicious data when logging in |
| Description | Adversary tries to input special characters to be able to pose as another user, or logs in without having an appropriate username and password. Handling of data is critical in this regards. |
| STRIDE | Tempering, Elevation of Privileges |
| Entry Points | (E1.1) Login Page |
| Assets | (A1.2) User’s personal data, (A2) Backend database |
| Mitigation/Strategy | Using Stored Procedures, parameterized queries or LINQ |
|  |  |
| ID | TR2 |
| Name | Adversary manages to get a valid username and password. |
| Description | If an Adversary manages to get a valid username and password he can do what that particular user can do. |
| STRIDE | Information disclosure, Tempering, Elevation of Privileges |
| Entry Points | (E1.1) Login Page |
| Assets | (A1.2) User’s personal data, (A1.1) User’s Login Data |
| Mitigation/Strategy | Strong passwords should be enforced, encryption should take place, and database should be protected from external access. |
|  |  |
| ID | TR3 |
| Name | Adversary tries to change URL in order to get other user information. |
| Description | When an attacker tries to change a URL in a way to get information of other users. For example changing id. |
| STRIDE | Information disclosure, Tempering, Elevation of Privileges |
| Entry Points | (E1.1) Login Page |
| Assets | (A1.2) User’s personal data, (A3.1) Product Details |
| Mitigation/Strategy | URL Rewriting, Authorization |

|  |  |
| --- | --- |
| ID | TR4 |
| Name | Adversary tries SQL Injection |
| Description | Adversary tries to input some SQL in any of the entry points in order steal data. |
| STRIDE | Information disclosure, Tempering, Elevation of Privileges |
| Entry Points | (E1.1) Login Page, (E3) Manage Products Page |
| Assets | (A1.2) User’s personal data, (A3.1) Product Details |
| Mitigation/Strategy | Using LINQ, Using Stored Procedures |
|  |  |
| ID | TR5 |
| Name | Attacker Tries to upload a malicious file |
| Description | Attacker tries to upload a bad file that might contain something to break the system |
| STRIDE | Information disclosure, Elevation of Privileges |
| Entry Points | (E3) Manage Products Page |
| Assets | (A1.2) User’s personal data, (A3.1) Product Details, (A4) Order Details |
| Mitigation/Strategy | Using specialized tools to detect bad files, filtering of data |
|  |  |
| ID | TR6 |
| Name | Attacker tries to use cross-site scripting to steal information |
| Description | When an attacker use an entry point in order to steal valuable information |
| STRIDE | Information disclosure, Tempering of data |
| Entry Points | (E1.1) Login Page, (E3) Manage Products Page |
| Assets | (A1.2) User’s personal data, (A3.1) Product Details |
| Mitigation/Strategy | Using specialized tools to detect bad files, filtering of data |
|  |  |
| ID | TR7 |
| Name | An attack tries to hack your system using backdoors |
| Description | When the Adversary will access your system with default data such as testing username and password |
| STRIDE | Information disclosure, Elevation of Privileges, Tempering of data |
| Entry Points | (E1.1) Login Page |
| Assets | (A1.2) User’s personal data, (A3.1) Product Details, (A4) Order Details |
| Mitigation/Strategy | Make sure that any default username and passwords are removed, do not allow any week passwords |

|  |  |
| --- | --- |
| ID | TR8 |
| Name | An adversary tries to skip the client side validation |
| Description | When an attacker tries to skip validation by disabling java script form the browser in order to try and eliminate validations |
| STRIDE | Information disclosure, Elevation of Privileges, Tempering of data |
| Entry Points | (E1.1) Login Page, (E3) Manage Products Page |
| Assets | (A1.2) User’s personal data, (A3.1) Product Details, (A4) Order Details |
| Mitigation/Strategy | Make sure to also include server side validations. |

# Task 2 – DFDs in Threat Modelling Document (M1.4)

# Task 3 – Implementation of Secure Website (P3.1)

This Task can be found attached at the back of the assignment.

# Task 4 – Documentation of security patterns and practices (P3.2, P4.3)

The Presentation can be found attached at the back of the assignment.

# Task 5 – Implementation of Further security techniques in website (M1.5)

# Task 6 – Documentation of alternative security patterns (M1.3)

# Task 7 – Security Patterns – Argue on what you cannot protect against (D1.2)

# Task 8 – Testing and Reviewing a 3rd Party application (P4.1, P4.2, P4.4)

# Task 9 – Perform Attacks on a third party application and document them (D1.3)