****

**Application Threat Modelling**

Indicative Template

****

Dr. Theodoros Ntouskas

tdouskas@unipi.gr

Table of Contents

[1 Introduction 3](#_Toc423780889)

[1.1 Purpose 3](#_Toc423780890)

[2 Application Overview 3](#_Toc423780891)

[2.1 Application Description 3](#_Toc423780892)

[2.2 Application Architecture 3](#_Toc423780893)

[2.3 Application Technologies 3](#_Toc423780894)

[3 Decompose the Application 3](#_Toc423780895)

[3.1 External Dependencies 3](#_Toc423780896)

[3.2 ENTRY POINTS 3](#_Toc423780897)

[3.3 ASSET REGISTER 5](#_Toc423780898)

[3.4 TRUST LEVELS 7](#_Toc423780899)

[3.5 DATA FLOW DIAGRAMS 8](#_Toc423780900)

[3.5.1 Search users process 8](#_Toc423780901)

[3.5.2 View User Details process 9](#_Toc423780902)

[4 THREAT CATEGORIZATION 9](#_Toc423780903)

[5 THREAT ANALYSIS 10](#_Toc423780904)

[5.1 Search User Process 10](#_Toc423780905)

[5.2 View User Details Process (User Details) 10](#_Toc423780906)

[6 DREAD 11](#_Toc423780907)

[6.1 Search user details 11](#_Toc423780908)

[6.2 View user details process 11](#_Toc423780909)

[7 SECURITY CONTROLS 12](#_Toc423780910)

[8 Mitigation Strategies 12](#_Toc423780911)

# Introduction

## Purpose

The scope and purpose of this study

# Application Overview

## Application Description

Main description of the application (such as main functionalities, roles etc.)

## Application Architecture

The overall application architecture

## Application Technologies

Please list the application technologies such as web server, DB server, frameworks etc.

# Decompose the Application

## External Dependencies

The external dependencies of the application (e.g. sso, ldap)

## ENTRY POINTS

In this section you have to describe the main entry points of the application as well as the corresponding trust levels that have access to each one of the entry point.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Trust Levels |
| 1 | HTTPS Port | The college library website will be only accessible via Https. All pages within the college library website are layered on this entry point.  | (1) Application administrator(2) Database Server administrator(3) Web server user process(4) Database read user(5) Database read/write user(6) Librarian(7) User with valid login credentials(8) User with Invalid Login credentials(9) Student(10) Tutor(11) Anonymous Web User |
| 1.1 | Application Main Page | The splash page for the Application is the entry point for all users. | (1) Application administrator(2) Database Server administrator(3) Web server user process(4) Database read user(5) Database read/write user(6) Librarian(7) User with valid login credentials(8) User with Invalid Login credentials(9) Student(10) Tutor(11) Anonymous Web User |
| 1.2 | application Login Page | All application roles must log in to the application before they can carry out any of the use cases.  | (1) Application administrator(2) Database Server administrator(3) Web server user process(4) Database read user(5) Database read/write user(6) Librarian(7) User with valid login credentials(8) User with Invalid Login credentials(9) Student(10) Tutor(11) Anonymous Web User |
| 1.2.1 | Login Function | The login function accepts User supplied credentials and authenticates with the e-class directory server | (1) Application administrator(2) Database Server administrator(3) Web server user process(4) Database read user(5) Database read/write user(6) Librarian(7) User with valid login credentials(8) User with Invalid Login credentials(9) Student(10) Tutor |
| 1.3 | Search User | This functionality allows users to search users | (7) User with valid login credentials(1) Application administrator |
| 1.4 | User Details | This functionality allows users to view and edit user details | 1. Application administrator

(7) User with valid login credentials |
| 1.5 | Print user details | This functionality allows users to print user details | 1. Application administrator

(7) User with valid login credentials |
| 1.6 | Export user's list | This functionality allows users to export the user's list to the desired format | 1. Application administrator

(7) User with valid login credentials |
| 1.7 | Add User | This functionality allows users to add a user to the application | 1. Application administrator

(7) User with valid login credentials |

## ASSET REGISTER

In this section you have to depict the assets of the application.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Name | Description | Trust Levels |
| 1 | **Application users** | **Assets relating to all the Application users** |  |
| 1.1 | Application administrator login details | The login credentials that an Application administrator uses to login to the application | (1) Application administrator(2) Database Server administrator(3) Web server user process(4) Database read user(5) Database read/write user |
| 1.2 | Personal Data | The personal information that will be stored in the registry database for all Application users | (1) Application administrator(2) Database Server administrator(3) Web server user process(4) Database read user(5) Database read/write user |
| 2 | **System** | **Assets relating to the underlying system.** |  |
| 2.1 | Availability of the application | The Application should be available 24 hours a day and should be accessible by all application users | (2) Database Server administrator(1) Application administrator |
| 2.2 | Ability to execute code as a Web Server User | The ability to execute privileged compiled code on the web server as a web server user | (3) Web server user process(1) Application administrator |
| 2.3 | Ability to Execute SQL as a Database Read User | This is the ability to execute SQL select queries on the database, and thus retrieve any information stored within the Application database | (2) Database Server administrator(4) Database read user(5) Database read/write user |
| 2.4 | Ability to Execute SQL as a Database Read/Write User | This is the ability to execute SQL select, insert, and update queries on the database and thus have read and write access to any information stored within the Application database | (2) Database Server administrator(5) Database read/write user |
| 3 | **Web Application (e-class)** | **Assets related to the Web Application**  |  |
| 3.1 | Ability to search users | This ability enables users to search users | (1) Application administrator |
| 3.2 | Ability to view and edit User Details | This ability enables users to view and edit user details | (1) Application administrator |
| 3.3 | Ability to print user details | This ability enables users to print user details | (1) Application administrator |
| 3.4 | Ability to export user's list | This ability enables users to export the user's list to the desired format | (1) Application administrator |
| 3.5 | Ability to add User | This ability enables users to add a user to the application | (1) Application administrator |
| 3.6 | Access to the Database Server | Access to the database server allows you to administer the database, giving you full access to the database users and all data contained within the database | (2) Database Server administrator |
| 3.7 | Access to audit and log data | The audit and log data shows all auditable events that occurred within the Application by any user | (1) Application administrator |
| 3.8 | Login Session | This is the login session of a user to the College Library website. This user could be a student, a member of the college faculty, or a Librarian. | (1) Application administrator(2) Database Server administrator(3) Web server user process(4) Database read user(5) Database read/write user(6) Librarian(7) User with valid login credentials(8) User with Invalid Login credentials(9) Student(10) Tutor |

## TRUST LEVELS

In the following table you have to describe the trust levels of the application

|  |  |  |
| --- | --- | --- |
| ID | Name | Description |
| 1 | Application administrator | **…** |
| 2 | Database Server administrator | … |
| 3 | Web server user process | **…** |
| 4 | Database read user | **…** |
| 5 | Database read/write user | **…** |
| 6 | Librarian | **…** |
| 7 | User with valid login credentials | A user who has connected to the college library website and has logged in using valid login credentials. |
| 8 | User with Invalid Login credentials | **…** |
| 9 | Student | **…** |
| 10 | Tutor | **…** |
| 11 | Anonymous Web User | A user who has connected to the college library website but has not provided valid credentials. |

## DATA FLOW DIAGRAMS

For each process we have to design the appropriate DFD

### Search users process

The following example describes the “Search Users Process”.

1. Application Admin clicks “User Management” link
2. The User Management page is displayed
3. Application Admin enters search criteria and clicks “Submit”
4. Application Admin is able to view the users list based on the requested search criteria
5. Application Admin is able to click the “Details” button for a specific user (in order to see the selected user details)
6. Application Admin is able to click the “print” button (in order to print the list)
7. Application Admin is able to click the “Export” button (in order to export the list)
8. Application Admin is able to click the “Add” button (in order to add a new user)
9. Application Admin is able to click the “Delete” button for a specific user (in order to delete the user)



### View User Details process

# THREAT CATEGORIZATION

A threat categorization such as STRIDE is useful in the identification of threats by classifying attacker goals such as:

* Spoofing
* Tampering
* Repudiation
* Information Disclosure
* Denial of Service
* Elevation of privilege.

 More information

<https://www.owasp.org/index.php/Application_Threat_Modeling>

<http://www.sans.org/reading-room/whitepapers/securecode/threat-modeling-process-ensure-application-security-1646>

# THREAT ANALYSIS

For each application process we have to identify the possible threats.

For example:

## Search User Process

|  |  |  |
| --- | --- | --- |
| ID | Threat | THREAT TYPE |
| T.. |  |  |
| T.. |  |  |
| T.. |  |  |
| T.. |  |  |

## View User Details Process (User Details)

|  |  |  |
| --- | --- | --- |
| ID | Threat | THREAT TYPE |
| T1 | Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system. | Elevation of privilege |
| T2 | User views other user details without having the appropriate credentials | Elevation of privilegeTampering |
| T3 | Malicious actor accesses all database data | Elevation of privilege |
| T4 | Malicious user views confidential information of students, faculty members and librarians | Information DisclosureElevation of privilege |

# DREAD

For each process and for each threat we have to calculate the DREAD Risk Value

## Search user details

..

## View user details process

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Threat | Vulnerability | Countermeasures | DREAD |
| T1 | Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system. | Elevation of privilege | V2- Authentication[[1]](#footnote-1) Verification RequirementsV4 – Access Control Verification Requirements | Damage | 8 |
| Reproducibility | 10 |
| Exploitability | 7 |
| Affected Users | 10 |
| Discoverability | 10 |
| **OVERALL RISK** | **9** |
| T2 | User views other user details without having the appropriate credentials | Elevation of privilegeTampering | V2- Authentication[[2]](#footnote-2) Verification RequirementsV4 – Access Control Verification Requirements | Damage | 8 |
| Reproducibility | 7 |
| Exploitability | 8 |
| Affected Users | 10 |
| Discoverability | 7 |
| **OVERALL RISK** | **8** |

# SECURITY CONTROLS

ASVS 3.0

<https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf>

<https://www.owasp.org/images/b/b2/ASVS-excel.xlsx>

# Mitigation Strategies

The objective of risk management is to reduce the impact that the exploitation of a threat can have to the application. This can be done by responding to a threat with a risk mitigation strategy. In general there are five options to mitigate threats

1. **Do nothing:** for example, hoping for the best
2. **Inform about the risk:** for example, warning user population about the risk
3. **Mitigate the risk:** for example, by putting countermeasures in place
4. **Accept the risk:** for example, after evaluating the impact of the exploitation (business impact)
5. **Transfer the risk:** for example, through contractual agreements and insurance
6. **Terminate the risk:** for example, shutdown, turn-off, unplug or decommission the asset

**MORE INFORMATION:**

<https://www.owasp.org/index.php/Application_Threat_Modeling>

<http://msdn.microsoft.com/en-us/library/ff649779.aspx>

<http://msdn.microsoft.com/en-us/library/ff648866.aspx>

<http://msdn.microsoft.com/en-us/library/ff647894.aspx>

<https://www.sans.org/reading-room/whitepapers/securecode/threat-modeling-process-ensure-application-security-1646>

<https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf>

Useful tools

* SDL Threat Modelling:
* <http://www.microsoft.com/en-us/download/details.aspx?id=2955>
* Microsoft Threat Modeling Tool 2014:
* <http://www.microsoft.com/en-us/download/details.aspx?id=42518>
1. You have to select the countermeasures based on the OWASP ASVS 3.0 [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)