# TLC Security Plan

Systems 4

Viacheslav Knyazev

Winter 2020

2020-04-16

Contents

[TLC Security Plan 1](#_Toc37952588)

[Introduction 3](#_Toc37952589)

[Security process 3](#_Toc37952590)

[Security issues 3](#_Toc37952591)

[User Authentication 3](#_Toc37952592)

[User Authorization 3](#_Toc37952593)

[Encryption 3](#_Toc37952594)

[Confidentiality of data 3](#_Toc37952595)

[Use of a security certificate (SSL) on the server 3](#_Toc37952596)

[Backup of data 3](#_Toc37952597)

[Privacy considerations 3](#_Toc37952598)

[Database security 3](#_Toc37952599)

[Protection against path truncation and reverse directory transversal 3](#_Toc37952600)

[Protection again cross-site scripting and SQL injection 4](#_Toc37952601)

[Input Validation 4](#_Toc37952602)

[Testing techniques 4](#_Toc37952603)

[Conclusion 4](#_Toc37952604)

## Introduction

This document is the security plan for the TLC project done by the third-year students. It is intended to cover processes used within the TLC project as well as the major security-related areas of concerns are.

## Security process

To ensure the security of our system, we reviewed several potential security faults, such as those listed below.

## Security issues

### User Authentication

This will have to be tested on each page, as there are many that un-authenticated users shouldn’t access.

### User Authorization

This is very important for our project as there is actions and data that only teachers are allowed accessing.

### Encryption

The system enforces connections via TLS, which guarantee strong encryption in transit. The system does not store confidential data and as such does not require any encryption on the back-end or database.

### Confidentiality of data

As stated above, all our data stored is made by the system, so it is not confidential

### Use of a security certificate (SSL) on the server

IIS integrates an SSL security certificate to ensure the safety of passwords in transit.

### Backup of data

Our system generates reports which contain all the data which users of the system may need, while the rest of the data is volatile by nature and not valuable to preserve.

### Privacy considerations

The system does not expose any personal information, and explicitly excludes student names from other students’ view.

### Database security

Access to the database is limited via Clara views, and is controlled via application pools.

### Protection against path truncation and reverse directory transversal

Our system is protected from such attacks by the ASP.NET framework.

### Protection again cross-site scripting and SQL injection

Our input is managed safely and SQL injection is avoided by the not using any raw SQL by delegating data access to the Entity Framework ORM.

### Input Validation

User input is never used for computations and is managed safely in order to avoid XSS attacks. This is not an attack vector.

### Testing Techniques

Our security is testing using a mix of manual testing by team members and integration tests which test the security of flows.

## Conclusion

To conclude, our primary concerns are authentication-related and are dealt with a mix of manual and automated testing to ensure security.