Threat Modeling Report

Created on 1/16/2026 8:28:59 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	9
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	9
Total Migrated	0

Diagram: Diagram 1

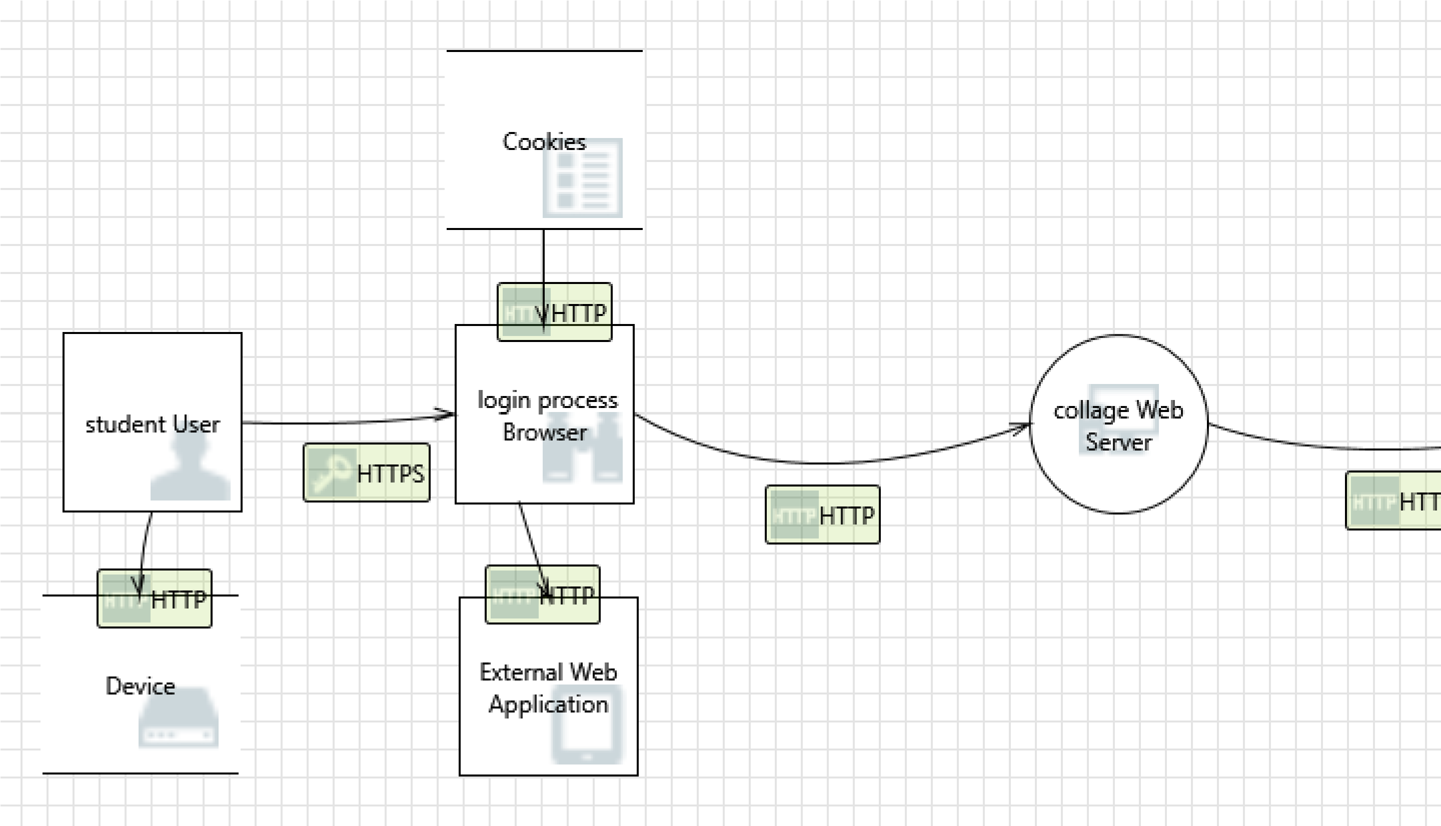
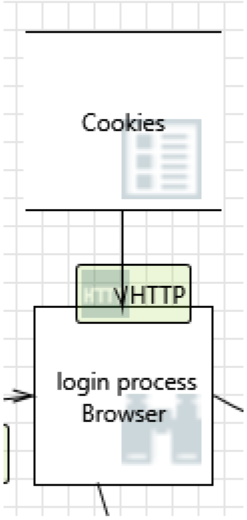


Diagram 1 Diagram Summary:

Not Started	9
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	9
Total Migrated	0

Interaction: HTTP



1. Spoofing of Source Data Store Cookies [State: Not Started] [Priority: High]

Category: Spoofing

Description: Cookies may be spoofed by an attacker and this may lead to incorrect data delivered to login process Browser. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

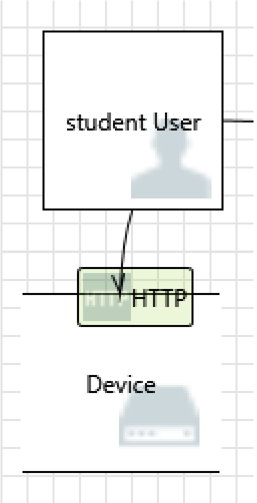
2. Weak Access Control for a Resource [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of Cookies can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: <no mitigation provided>

Interaction: HTTP



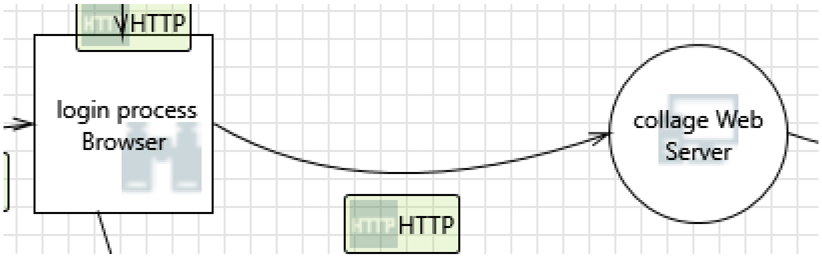
3. Spoofing of Destination Data Store Device [State: Not Started] [Priority: High]

Category: Spoofing

Description: Device may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Device. Consider using a standard authentication mechanism to identify the destination data store.

Justification: <no mitigation provided>

Interaction: HTTP



4. Spoofing the login process Browser External Entity [State: Not Started] [Priority: High]

Category: Spoofing

Description: login process Browser may be spoofed by an attacker and this may lead to unauthorized access to collage Web Server. Consider using a standard authentication mechanism to identify the external entity.

Justification: <no mitigation provided>

5. Cross Site Scripting [State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'collage Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: <no mitigation provided>

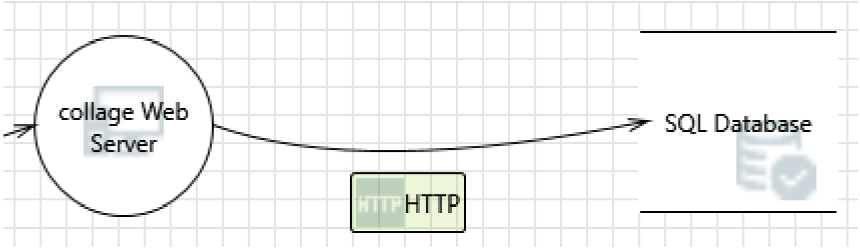
6. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: collage Web Server may be able to impersonate the context of login process Browser in order to gain additional privilege.

Justification: <no mitigation provided>

Interaction: HTTP



7. Spoofing of Destination Data Store SQL Database [State: Not Started] [Priority: High]

Category: Spoofing

Description: SQL Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database. Consider using a standard authentication mechanism to identify the destination data store.

Justification: <no mitigation provided>

8. Potential SQL Injection Vulnerability for SQL Database [State: Not Started] [Priority: High]

Category: Tampering

Description: SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.

Justification: <no mitigation provided>

9. Potential Excessive Resource Consumption for collage Web Server or SQL Database [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: Does collage Web Server or SQL Database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: <no mitigation provided>