Threat Modeling Report

Created on 10/2/2023 8:57:13 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	0
Not Applicable	5
Needs Investigation	4
Mitigation Implemented	1
Total	10
Total Migrated	0

Diagram: Diagram 1

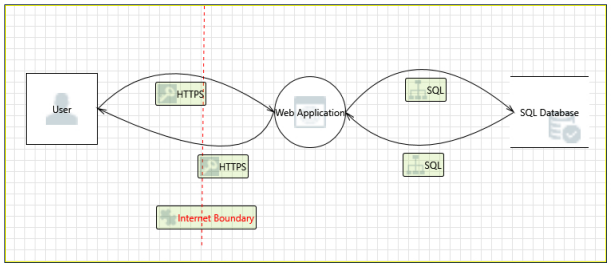
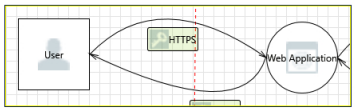


Diagram 1 Diagram Summary:

Not Started	0
Not Applicable	5
Needs Investigation	4
Mitigation Implemented	1
Total	10
Total Migrated	0

Interaction: HTTPS



1. Potential Process Crash or Stop for Web Application [State: Not Applicable] [Priority: High]

Category:	Denial Of Service
Description:	Web Application crashes, halts, stops or runs slowly; in all cases violating an availability metric.
Justification:	<no mitigation provided>
Countermeasure:	
Risk:	High
Team:	Team1

2. Potential Data Repudiation by Web Application [State: Not Applicable] [Priority: High]

Category:	Repudiation
Description:	Web Application claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification:	<no mitigation provided>
Countermeasure:	
Risk:	High
Team:	Team1

3. Potential Remote Code Execution [State: Not Applicable] [Priority: High]

Category:	Tampering
Description:	User may be able to remotely execute code for Web Application.
Justification:	PHP is not used
Countermeasure:	
Risk:	High
Team:	Team1

4. Cross-Site Scripting (XSS) [State: Needs Investigation] [Priority: High]

Category:	Tampering
Description:	The web server 'Web Application' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
Justification:	<no mitigation provided>
Countermeasure:	Encode Output in application / Apply CSP
Risk:	High
Team:	Team1

5. Spoofing the User External Entity [State: Needs Investigation] [Priority: High]

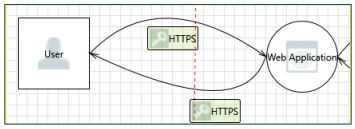
Category:	Spoofing
Description:	User may be spoofed by an attacker and this may lead to unauthorized access to Web Application. Consider using a standard authentication mechanism to identify the external entity.
Justification:	<no mitigation provided>
Countermeasure:	Should be handled by strong authentication method

Countermeasure: Should be handled by strong authentication method
Risk: High
Team: Team1

6. Invalid Internet Access (Demo) [State: Needs Investigation] [Priority: High]

Category: Compliance
Description: Web Applications should not directly connected to the Internet
Justification: <no mitigation provided>
Countermeasure:
Risk: High
Team: Team1

Interaction: HTTPS



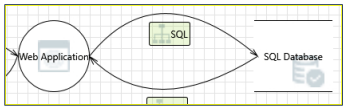
7. External Entity User Potentially Denies Receiving Data [State: Not Applicable] [Priority: High]

Category: Repudiation
Description: User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification: <no mitigation provided>
Countermeasure:
Risk: High
Team: Team1

8. Spoofing of the User External Destination Entity [State: Not Applicable] [Priority: High]

Category: Spoofing
Description: User may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of User. Consider using a standard authentication mechanism to identify the external entity.
Justification: <no mitigation provided>
Countermeasure:
Risk: High
Team: Team1

Interaction: SQL



9. Potential SQL Injection Vulnerability for SQL Database [State: Needs Investigation] [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>
Countermeasure: Hibernate + Criterias should be used as persistance layer
Risk: High
Team: Team1

10. Weak Access Control for a Resource [State: Mitigation Implemented] [Priority: High]

Category: Information Disclosure
Description: Improper data protection of Web Application can allow an attacker to read information not intended for disclosure. Review authorization settings.
Justification: Already handled by OPS
Countermeasure:
Risk: High
Team: Team1