Threat Modeling Report

Created on 1/16/2026 8:07:44 AM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	19
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	19
Total Migrated	0

Diagram: Diagram 1

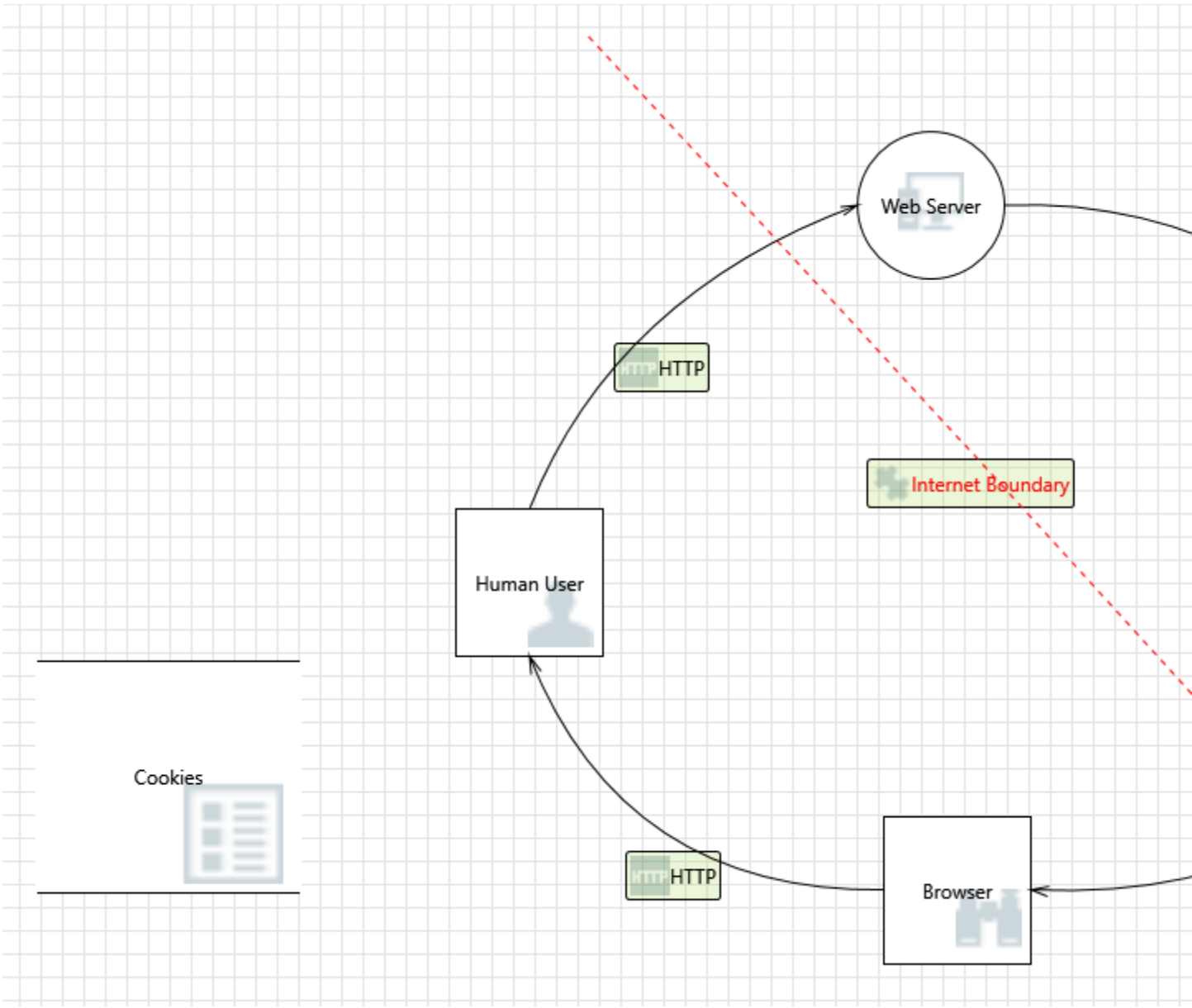
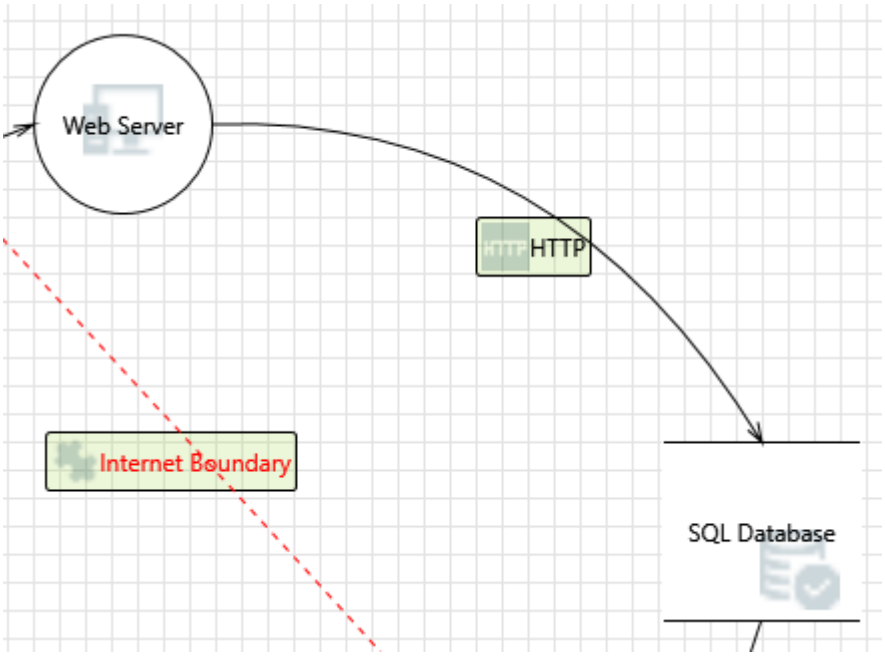


Diagram 1 Diagram Summary:

Not Started	19
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	19
Total Migrated	0

Interaction: HTTP



1. 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>

2. 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>

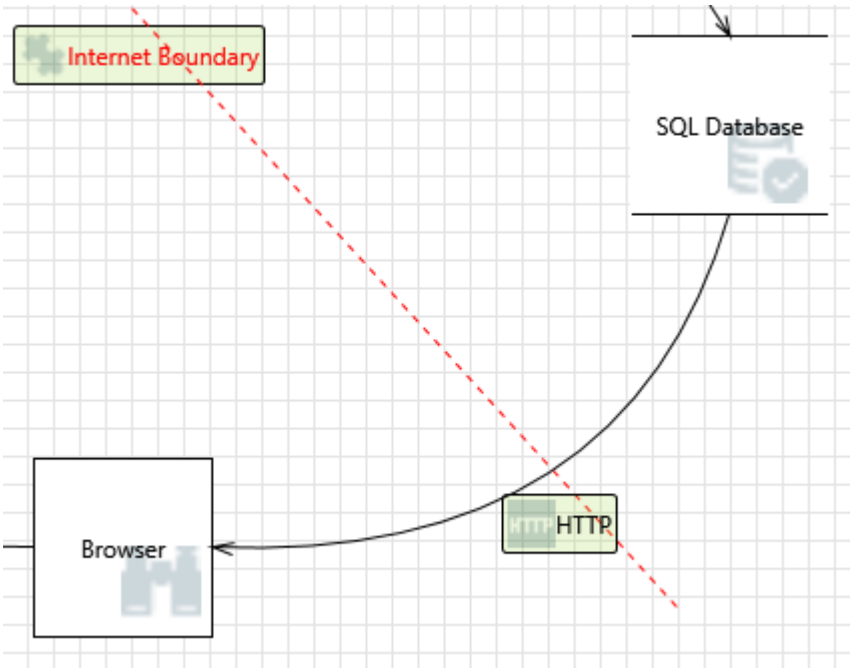
3. Potential Excessive Resource Consumption for Web Server or SQL Database [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: Does 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>

Interaction: HTTP



4. Data Store Inaccessible [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: An external agent prevents access to a data store on the other side of the trust boundary.

Justification: <no mitigation provided>

5. Data Flow HTTP Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: <no mitigation provided>

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

Category: Information Disclosure

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

Justification: <no mitigation provided>

7. External Entity Browser Potentially Denies Receiving Data [State: Not Started] [Priority: High]

Category: Repudiation

Description: Browser 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>

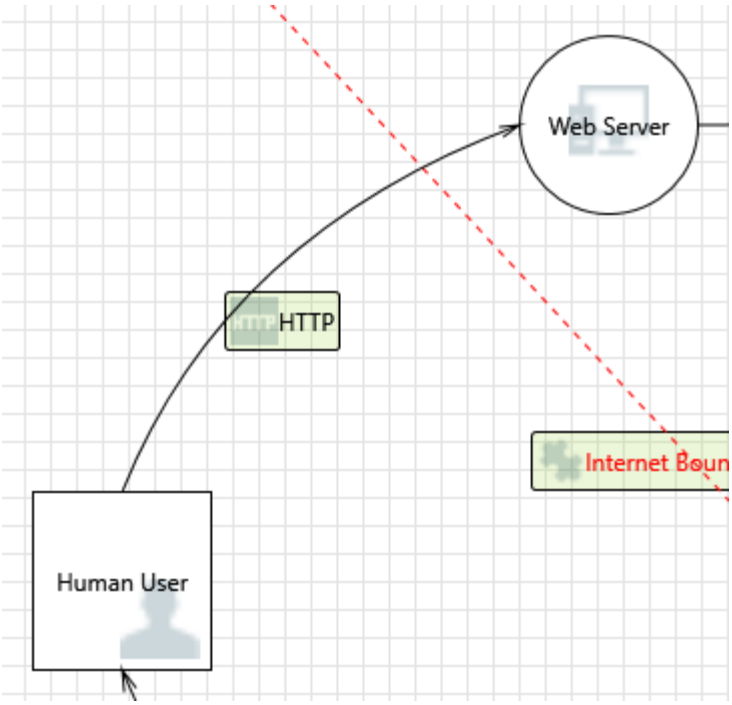
8. Spoofing of Source Data Store SQL Database [State: Not Started] [Priority: High]

Category: Spoofing

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

Justification: <no mitigation provided>

Interaction: HTTP



9. Spoofing the Web Server Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: Web Server may be spoofed by an attacker and this may lead to information disclosure by Human User. Consider using a standard authentication mechanism to identify the destination process.

Justification: <no mitigation provided>

10. Spoofing the Human User External Entity [State: Not Started] [Priority: High]

Category: Spoofing

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

Justification: <no mitigation provided>

11. Potential Lack of Input Validation for Web Server [State: Not Started] [Priority: High]

Category: Tampering

Description: Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Web Server or an elevation of privilege attack against Web Server or an information disclosure by Web Server. Failure

to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.

Justification: <no mitigation provided>

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

Category: Tampering

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

Justification: <no mitigation provided>

13. Potential Data Repudiation by Web Server [State: Not Started] [Priority: High]

Category: Repudiation

Description: Web Server 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>

14. Data Flow Sniffing [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Data flowing across HTTP may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.

Justification: <no mitigation provided>

15. Potential Process Crash or Stop for Web Server [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: Web Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: <no mitigation provided>

16. Data Flow HTTP Is Potentially Interrupted [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: An external agent interrupts data flowing across a trust boundary in either direction.

Justification: <no mitigation provided>

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

Category: Elevation Of Privilege

Description: Web Server may be able to impersonate the context of Human User in order to gain additional privilege.

Justification: <no mitigation provided>

18. Web Server May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Human User may be able to remotely execute code for Web Server.

Justification: <no mitigation provided>

19. Elevation by Changing the Execution Flow in Web Server [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into Web Server in order to change the flow of program execution within Web Server to the attacker's choosing.

Justification: <no mitigation provided>