Threat Modeling Report

Created on 12/10/2018 4:55:52 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	11
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	11
Total Migrated	0

Diagram: Diagram 1

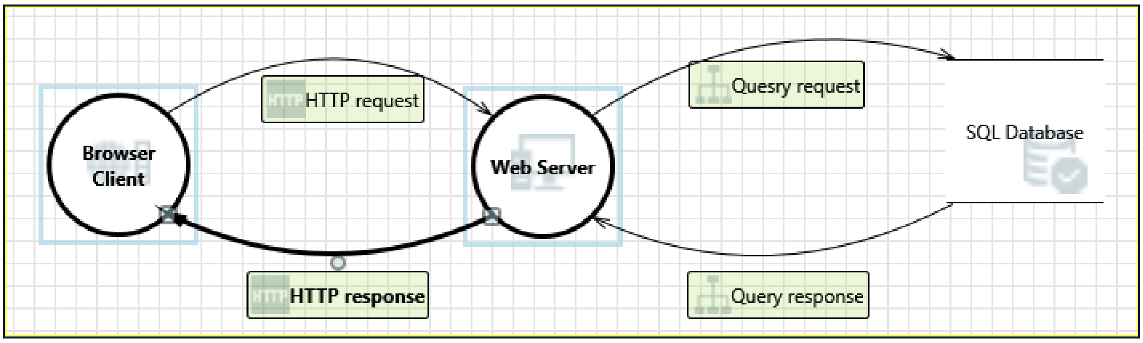
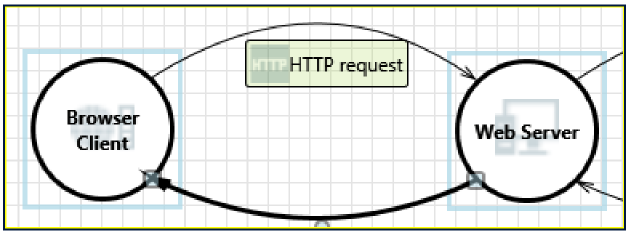


Diagram 1 Diagram Summary:

Not Started	11
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	11
Total Migrated	0

Interaction: HTTP request



1. 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: protected by CORS

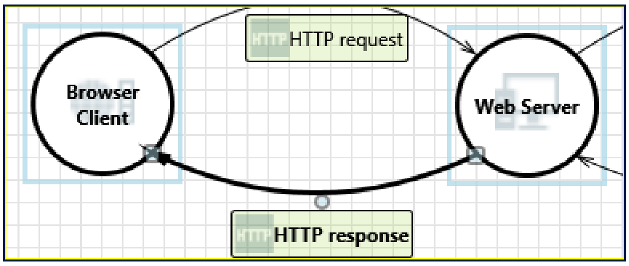
2. Elevation Using Impersonation [State: Not Started] [Priority: low]

Category: Elevation Of Privilege

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

Justification: Handled by JWT authorization with short expiration time

Interaction: HTTP response



3. Web Server Process Memory Tampered [State: Not Started] [Priority: High]

Category: Tampering

Description: If Web Server is given access to memory, such as shared memory or pointers, or is given the ability to control what Browser Client executes (for example, passing back a function pointer.), then Web Server can tamper with Browser Client. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it.

Justification: not important

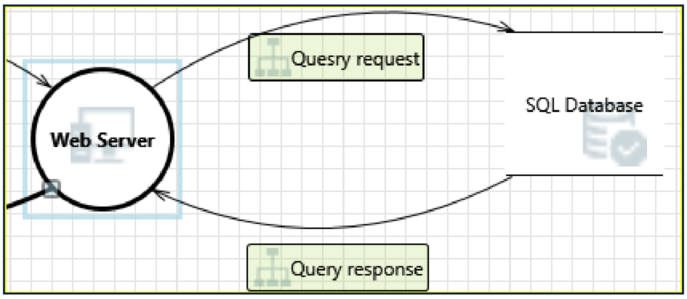
4. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

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

Justification: Handled by JWT authorization with short expiration time

Interaction: Query response



5. 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 Web Server. Consider using a standard authentication mechanism to identify the source data store.

Justification: not important

6. 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: protected by CORS

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

Category: Tampering

Description: The web server 'Web Server' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'SQL Database' inputs and output.

Justification: not important

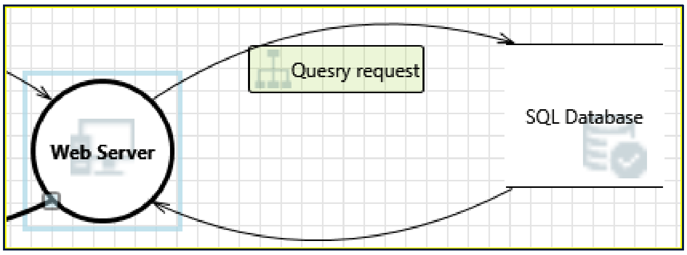
8. Weak Access Control for a Resource [State: Not Started] [Priority: High]

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: handled by JWT authorization

Interaction: Quesry request



9. 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: not important

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

10. 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: check for injections

11. 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: make timeout for db requests, but still dangerous.