

Threat Modeling Report

Created on 2/12/2022 10:20:01 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	1
Not Applicable	0
Needs Investigation	11
Mitigation Implemented	0
Total	12
Total Migrated	0

Diagram: Diagram 1

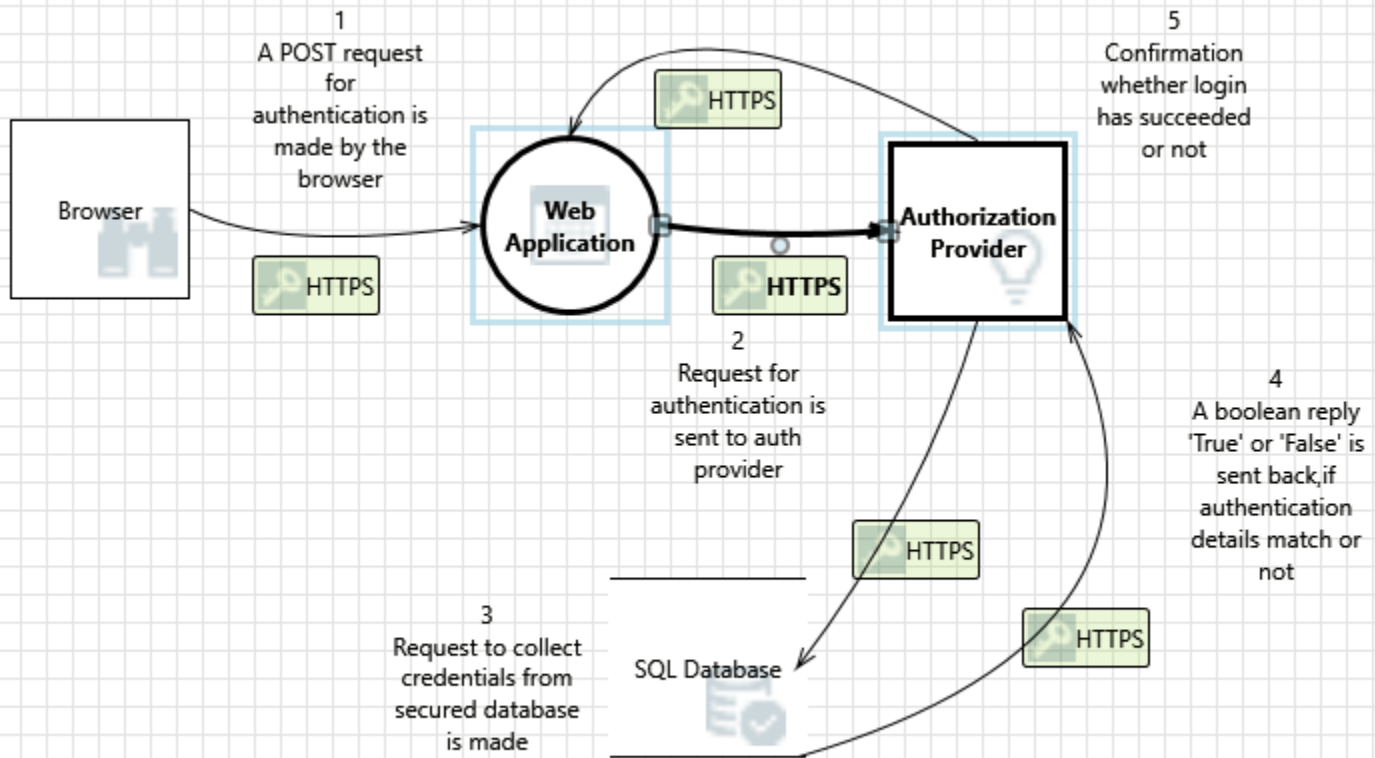
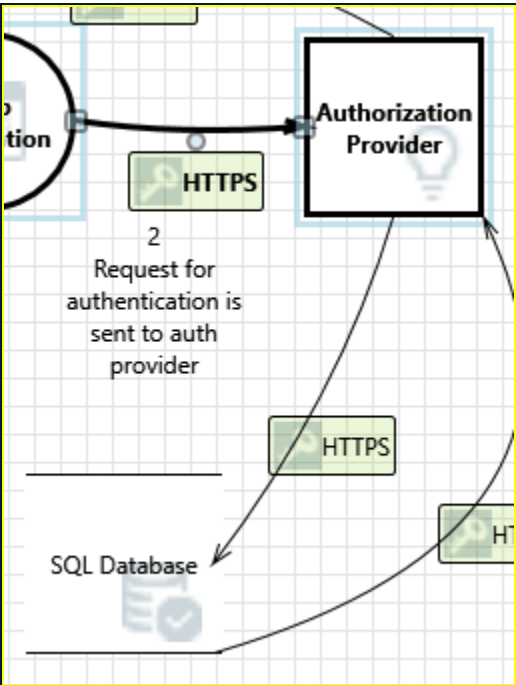


Diagram 1 Diagram Summary:

Not Started	1
Not Applicable	0
Needs Investigation	11
Mitigation Implemented	0
Total	12
Total Migrated	0

Interaction: HTTPS



1. Spoofing of Destination Data Store SQL Database [State: Needs Investigation]

[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: An attack possibility
2. Possible SQL Injection Vulnerability for SQL Database [State: Needs Investigation]

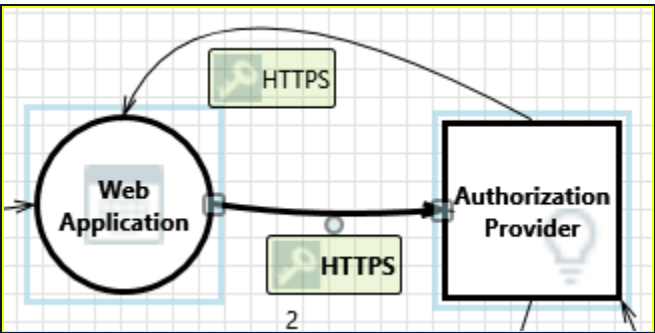
[Priority: High]

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: SQL Injection is an attack possibility,if user input is not sanitized by the server side

Interaction: HTTPS



3. Spoofing the Authorization Provider External Entity [State: Needs Investigation]

[Priority: High]

Category: Tampering

Description: Authorization Provider 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: A possible attack
4. Cross Site Scripting [State: Needs Investigation] [Priority: High]

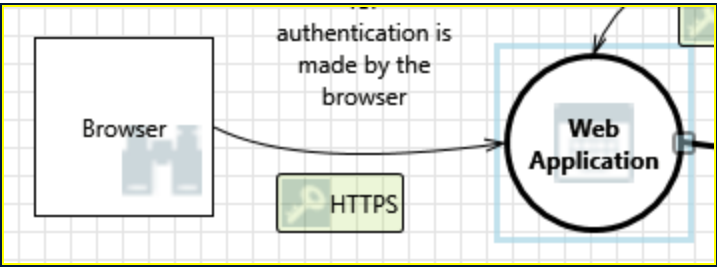
Category: Tampering

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

Justification: Unless the user input is sanitized or by disabling Javascript,XSS is a real attack possibility
5. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege
Description: Web Application may be able to impersonate the context of Authorization Provider in order to gain additional privilege.
Justification: Possible attacker motive

Interaction: HTTPS



6. Spoofing the Browser External Entity [State: Needs Investigation] [Priority: High]

Category: Spoofing
Description: Browser 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: Possible attacker motive

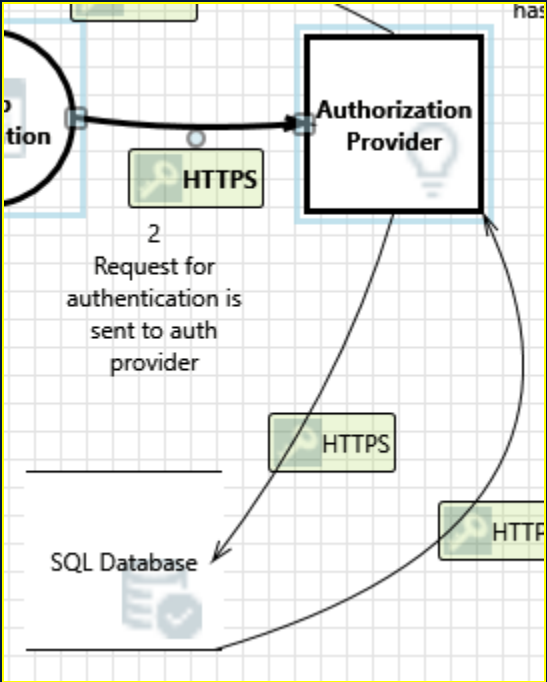
7. Cross Site Scripting [State: Not Started] [Priority: High]

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: Unless the user input is sanitized or by disabling Javascript,XSS is a real attack possibility

8. Elevation Using Impersonation [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege
Description: Web Application may be able to impersonate the context of Browser in order to gain additional privilege.
Justification: Nefarious attacker's motive to exploit a web server

Interaction: HTTPS



9. Spoofing of Source Data Store SQL Database [State: Needs Investigation] [Priority: High]

Category: Spoofing

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

Justification: SQL Injection is an attack possibility,if user input is not sanitized by the server side

10. Weak Access Control for a Resource [State: Needs Investigation] [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: Data breach is a real possibility,if security configuration is not done in the right manner

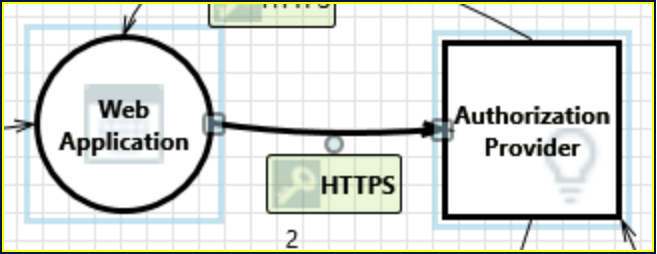
11. Weakness in SSO Authorization [State: Needs Investigation] [Priority: High]

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Weak SSO solutions can exploit the CIA triad,putting digital identity of users at risk

Interaction: HTTPS



12. Weakness in SSO Authorization **[State: Needs Investigation]** **[Priority: High]**

Category: Elevation Of Privilege

Description: Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.

Justification: Weak SSO solutions can exploit the CIA triad,putting digital identity of users at risk