Threat Modeling Report

Created on 4/18/2023 8:00:49 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	36
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	36
Total Migrated	0

Diagram: Diagram 1

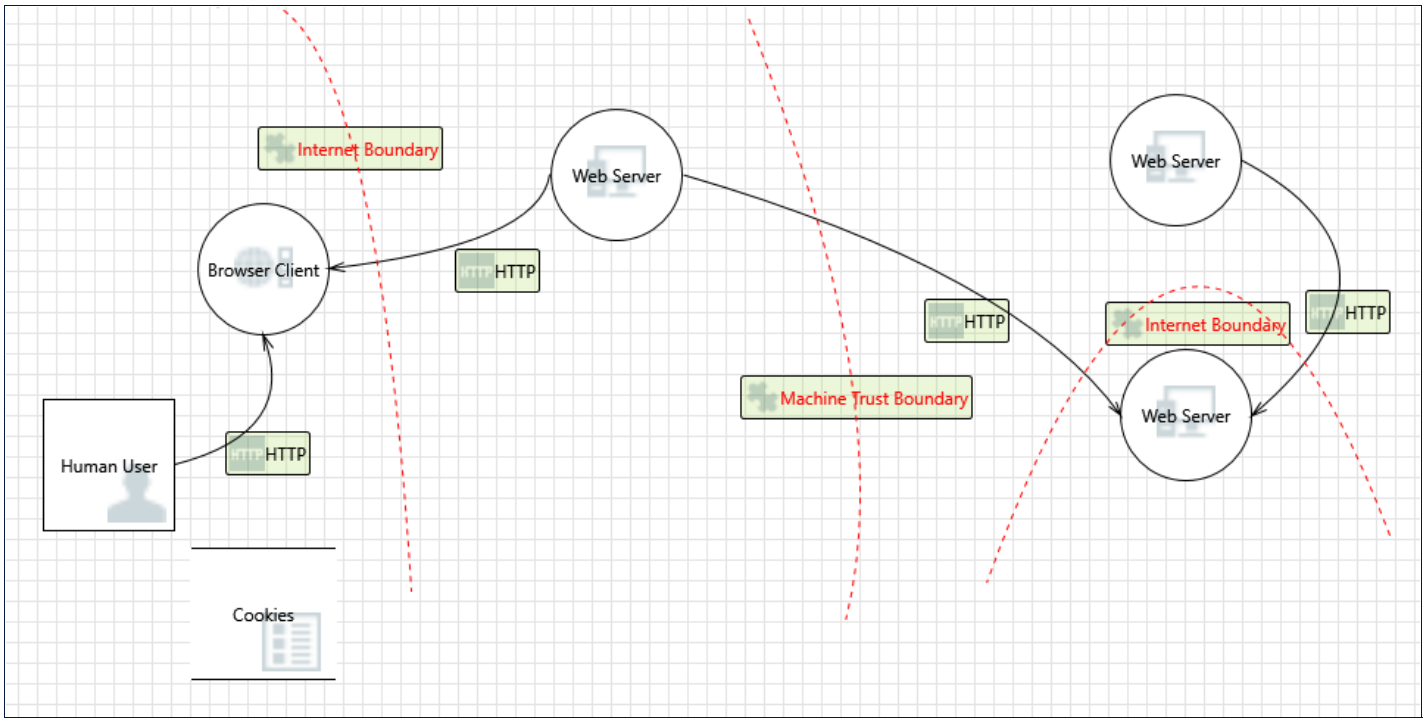
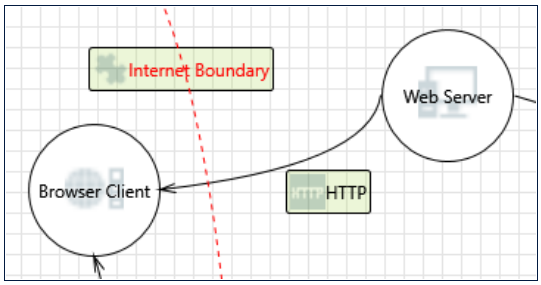


Diagram 1 Diagram Summary:

Not Started	36
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	36
Total Migrated	0

Interaction: HTTP



1. 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 unauthorized access to Browser Client. Consider using a standard authentication mechanism to identify the source process.
Justification: <no mitigation provided>

2. Spoofing the Browser Client Process [State: Not Started] [Priority: High]

Category: Spoofing
Description: Browser Client may be spoofed by an attacker and this may lead to information disclosure by Web Server. Consider using a standard authentication mechanism to identify the destination process.
Justification: <no mitigation provided>

3. Potential Lack of Input Validation for Browser Client [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 Browser Client or an elevation of privilege attack against Browser Client or an information disclosure by Browser Client. 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>

4. 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: <no mitigation provided>

5. Potential Data Repudiation by Browser Client [State: Not Started] [Priority: High]

Category: Repudiation
Description: Browser Client 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>

6. 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>

7. Potential Process Crash or Stop for Browser Client [State: Not Started] [Priority: High]

Category: Denial Of Service
Description: Browser Client crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: <no mitigation provided>

8. 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>

9. 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: <no mitigation provided>

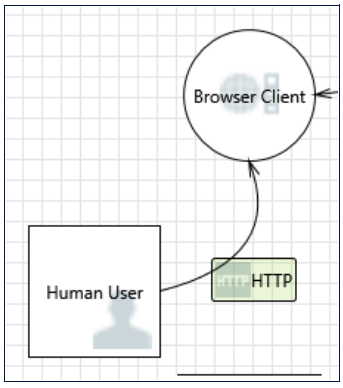
10. Browser Client May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Web Server may be able to remotely execute code for Browser Client.
Justification: <no mitigation provided>

11. Elevation by Changing the Execution Flow in Browser Client [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: An attacker may pass data into Browser Client in order to change the flow of program execution within Browser Client to the attacker's choosing.
Justification: <no mitigation provided>

Interaction: HTTP



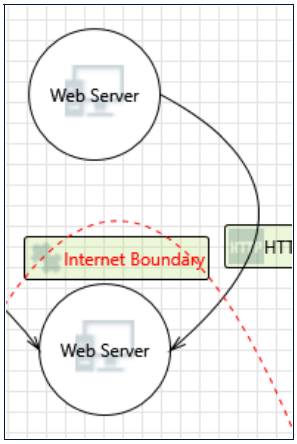
12. Elevation Using Impersonation [State: Not Started] [Priority: High]

Category: Elevation Of Privilege
Description: Browser Client may be able to impersonate the context of Human User in order to gain additional privilege.
Justification: <no mitigation provided>

13. 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 Browser Client. Consider using a standard authentication mechanism to identify the external entity.
Justification: <no mitigation provided>

Interaction: HTTP



14. 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>

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

Category: Elevation Of Privilege
Description: Web Server may be able to impersonate the context of Web Server in order to gain additional privilege.
Justification: <no mitigation provided>

16. 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>

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

Category: Elevation Of Privilege
Description: Web Server may be able to remotely execute code for Web Server.
Justification: <no mitigation provided>

18. 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>

19. 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>

20. 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>

21. 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>

22. 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>

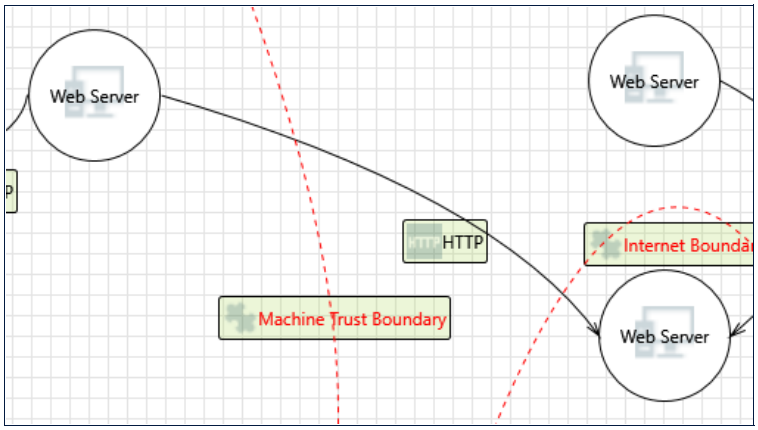
23. Spoofing the Web Server Process [State: Not Started] [Priority: High]

Category: Spoofing
Description: Web Server may be spoofed by an attacker and this may lead to information disclosure by Web Server. Consider using a standard authentication mechanism to identify the destination process.
Justification: <no mitigation provided>

24. 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 unauthorized access to Web Server. Consider using a standard authentication mechanism to identify the source process.
Justification: <no mitigation provided>

Interaction: HTTP



25. 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>

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

Category: Elevation Of Privilege
Description: Web Server may be able to impersonate the context of Web Server in order to gain additional privilege.
Justification: <no mitigation provided>

27. 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 unauthorized access to Web Server. Consider using a standard authentication mechanism to identify the source process.

Justification: <no mitigation provided>

28. 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 Web Server. Consider using a standard authentication mechanism to identify the destination process.

Justification: <no mitigation provided>

29. 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>

30. 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>

31. 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>

32. Weak Credential Transit [State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Credentials on the wire are often subject to sniffing by an attacker. Are the credentials re-usable/re-playable? Are credentials included in a message? For example, sending a zip file with the password in the email. Use strong cryptography for the transmission of credentials. Use the OS libraries if at all possible, and consider cryptographic algorithm agility, rather than hardcoding a choice.

Justification: <no mitigation provided>

33. 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>

34. 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>

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

Category: Elevation Of Privilege

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

Justification: <no mitigation provided>

36. 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>