Threat Modeling Report

Created on 11/16/2025 3:24:30 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

Threat Model Summary:

Not Started	38
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	38
Total Migrated	0

Diagram: Diagram 1

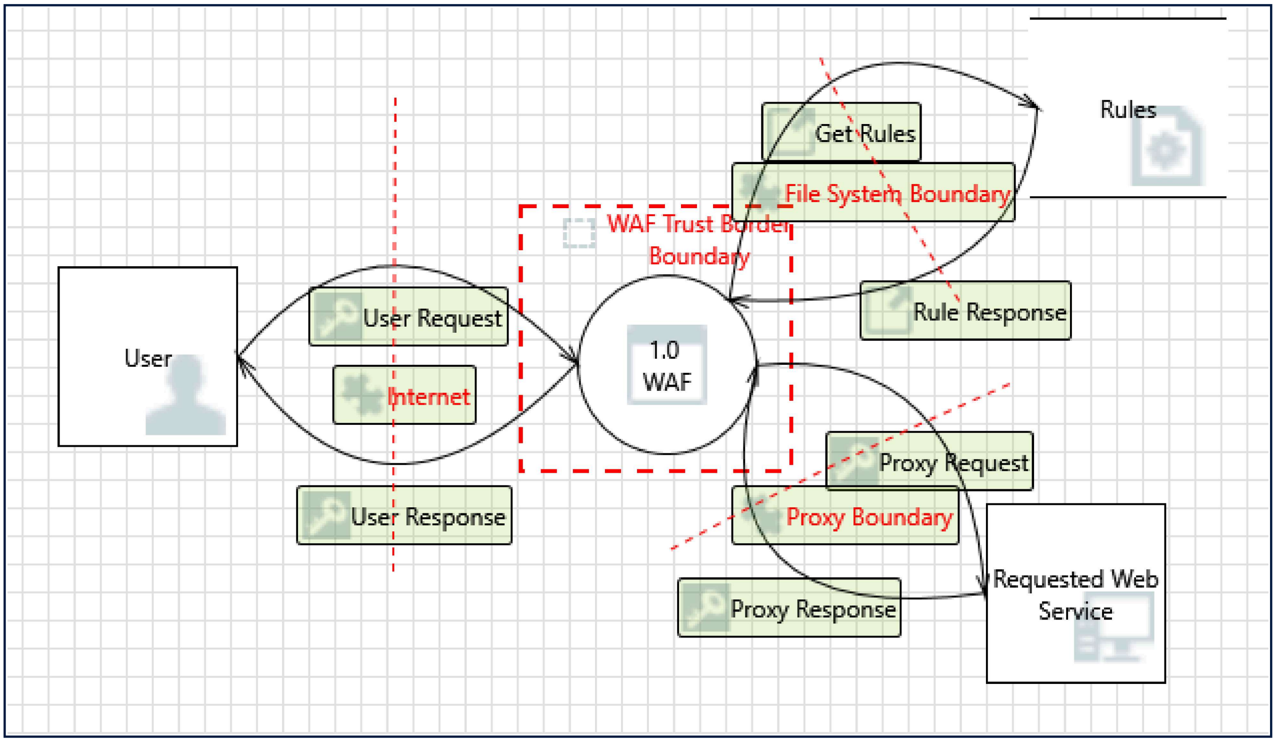
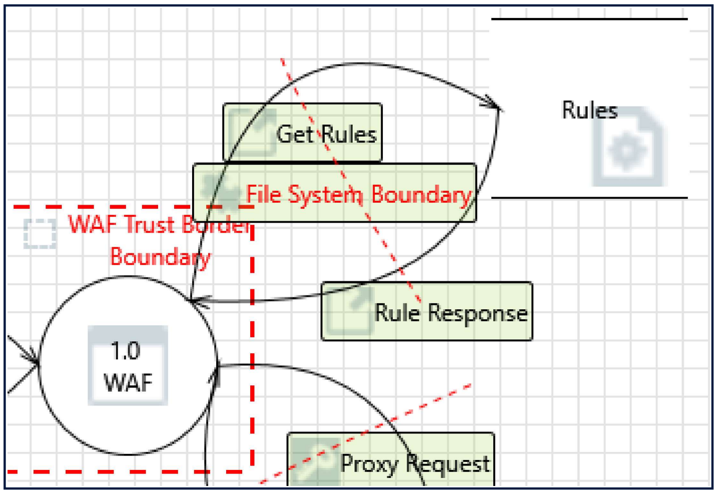


Diagram 1 Diagram Summary:

Not Started	38
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	38
Total Migrated	0

Interaction: Get Rules



1. Spoofing of Destination Data Store Rules [State: Not Started] [Priority: High]

Category: Spoofing

Description: Rules may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Rules. Consider using a standard authentication mechanism to identify the destination data store.

Justification: <no mitigation provided>

2. Potential Excessive Resource Consumption for 1.0 WAF or Rules [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: Does 1.0 WAF or Rules 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>

3. 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>

4. Data Flow Get Rules 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>

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

Category: Information Disclosure

Description: Data flowing across Get Rules 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>

6. Data Store Denies Rules Potentially Writing Data [State: Not Started] [Priority: High]

Category: Repudiation

Description: Rules claims that it did not write data received from an entity 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>

7. The Rules Data Store Could Be Corrupted [State: Not Started] [Priority: High]

Category: Tampering

Description: Data flowing across Get Rules may be tampered with by an attacker. This may lead to corruption of Rules. Ensure the integrity of the data flow to the data store.

Justification: <no mitigation provided>

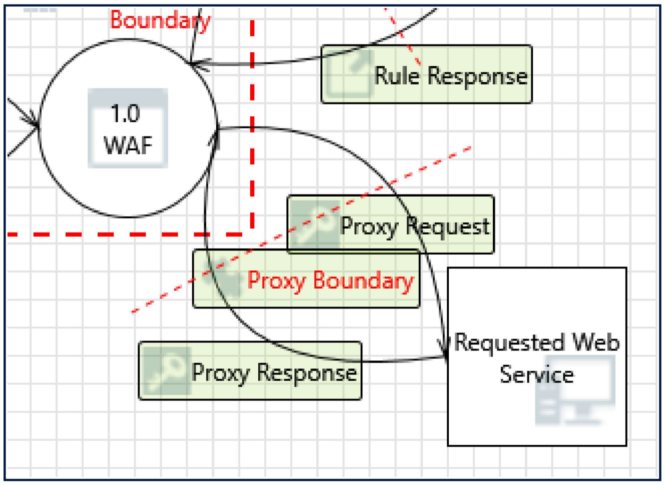
8. Spoofing the 1.0 WAF Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: 1.0 WAF may be spoofed by an attacker and this may lead to unauthorized access to Rules. Consider using a standard authentication mechanism to identify the source process.

Justification: <no mitigation provided>

Interaction: Proxy Request



9. Data Flow Proxy Request 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>

10. External Entity Requested Web Service Potentially Denies Receiving Data [State: Not Started] [Priority: High]

Category: Repudiation

Description: Requested Web Service 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>

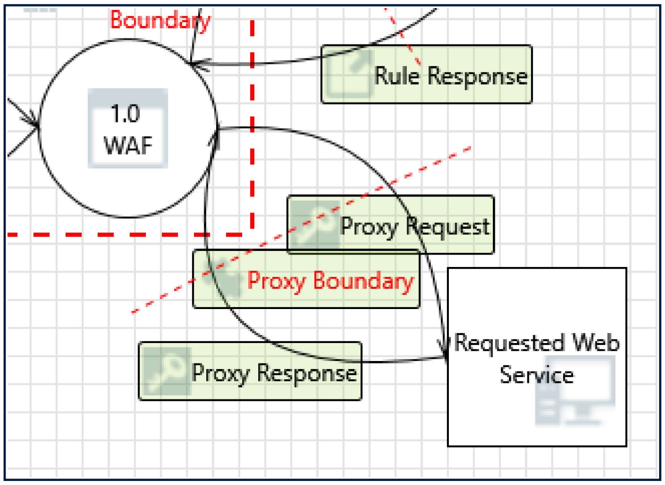
11. Spoofing of the Requested Web Service External Destination Entity [State: Not Started] [Priority: High]

Category: Spoofing

Description: Requested Web Service may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Requested Web Service. Consider using a standard authentication mechanism to identify the external entity.

Justification: <no mitigation provided>

Interaction: Proxy Response



12. Spoofing the Requested Web Service External Entity [State: Not Started] [Priority: High]

Category: Spoofing

Description: Requested Web Service may be spoofed by an attacker and this may lead to unauthorized access to 1.0 WAF. Consider using a standard authentication mechanism to identify the external entity.

Justification: <no mitigation provided>

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

Category: Elevation Of Privilege

Description: 1.0 WAF may be able to impersonate the context of Requested Web Service in order to gain additional privilege.

Justification: <no mitigation provided>

14. Elevation by Changing the Execution Flow in 1.0 WAF [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 WAF in order to change the flow of program execution within 1.0 WAF to the attacker's choosing.

Justification: <no mitigation provided>

15. 1.0 WAF May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Requested Web Service may be able to remotely execute code for 1.0 WAF.

Justification: <no mitigation provided>

16. Data Flow Proxy Response 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. Potential Process Crash or Stop for 1.0 WAF [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: 1.0 WAF crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: <no mitigation provided>

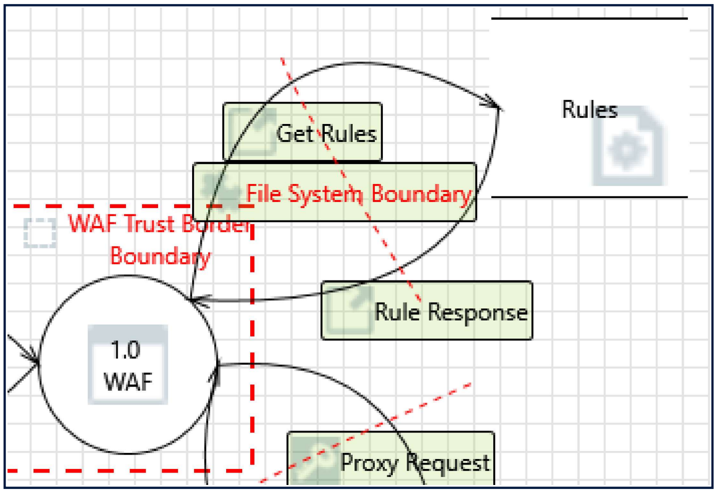
18. Potential Data Repudiation by 1.0 WAF [State: Not Started] [Priority: High]

Category: Repudiation

Description: 1.0 WAF 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>

Interaction: Rule Response



19. Spoofing of Source Data Store Rules [State: Not Started] [Priority: High]

Category: Spoofing

Description: Rules may be spoofed by an attacker and this may lead to incorrect data delivered to 1.0 WAF. Consider using a standard authentication mechanism to identify the source data store.

Justification: <no mitigation provided>

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

Category: Information Disclosure

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

Justification: <no mitigation provided>

21. Elevation by Changing the Execution Flow in 1.0 WAF [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 WAF in order to change the flow of program execution within 1.0 WAF to the attacker's choosing.

Justification: <no mitigation provided>

22. 1.0 WAF May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Rules may be able to remotely execute code for 1.0 WAF.

Justification: <no mitigation provided>

23. 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>

24. Data Flow Rule Response 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>

25. Potential Process Crash or Stop for 1.0 WAF [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: 1.0 WAF crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: <no mitigation provided>

26. Potential Data Repudiation by 1.0 WAF [State: Not Started] [Priority: High]

Category: Repudiation

Description: 1.0 WAF 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>

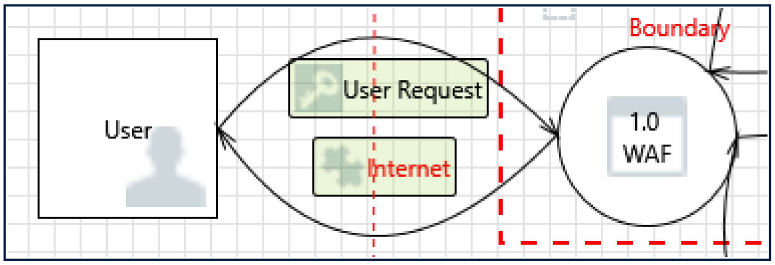
27. Spoofing the 1.0 WAF Process [State: Not Started] [Priority: High]

Category: Spoofing

Description: 1.0 WAF may be spoofed by an attacker and this may lead to information disclosure by Rules. Consider using a standard authentication mechanism to identify the destination process.

Justification: <no mitigation provided>

Interaction: User Request



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

Category: Spoofing

Description: User may be spoofed by an attacker and this may lead to unauthorized access to 1.0 WAF. Consider using a standard authentication mechanism to identify the external entity.

Justification: <no mitigation provided>

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

Category: Elevation Of Privilege

Description: 1.0 WAF may be able to impersonate the context of User in order to gain additional privilege.

Justification: <no mitigation provided>

30. Potential Data Repudiation by 1.0 WAF [State: Not Started] [Priority: High]

Category: Repudiation

Description: 1.0 WAF 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. Potential Process Crash or Stop for 1.0 WAF [State: Not Started] [Priority: High]

Category: Denial Of Service

Description: 1.0 WAF crashes, halts, stops or runs slowly; in all cases violating an availability metric.

Justification: <no mitigation provided>

32. Data Flow User Request 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>

33. 1.0 WAF May be Subject to Elevation of Privilege Using Remote Code Execution [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: User may be able to remotely execute code for 1.0 WAF.

Justification: <no mitigation provided>

34. Elevation by Changing the Execution Flow in 1.0 WAF [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: An attacker may pass data into 1.0 WAF in order to change the flow of program execution within 1.0 WAF to the attacker's choosing.

Justification: <no mitigation provided>

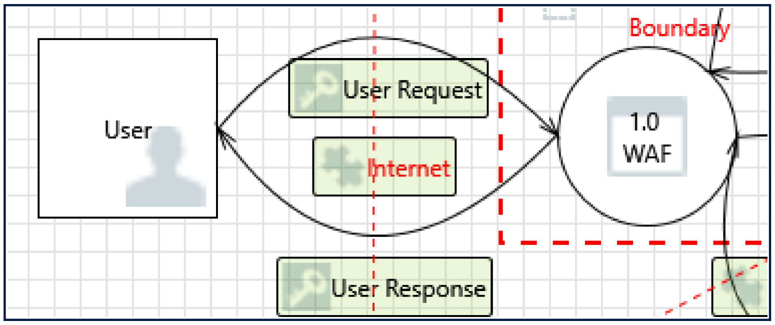
35. Cross Site Request Forgery [State: Not Started] [Priority: High]

Category: Elevation Of Privilege

Description: Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.

Justification: <no mitigation provided>

Interaction: User Response



36. Spoofing of the User External Destination Entity [State: Not Started] [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>

37. External Entity User Potentially Denies Receiving Data [State: Not Started] [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>

38. Data Flow User Response 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>