

# Threat Modeling Report

Created on 11/18/2025 1:36:55 PM

Threat Model Name:

Owner:

Reviewer:

Contributors:

Description:

Assumptions:

External Dependencies:

## Threat Model Summary:

Not Started	18
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	18
Total Migrated	0

---

## Diagram: Diagram 1

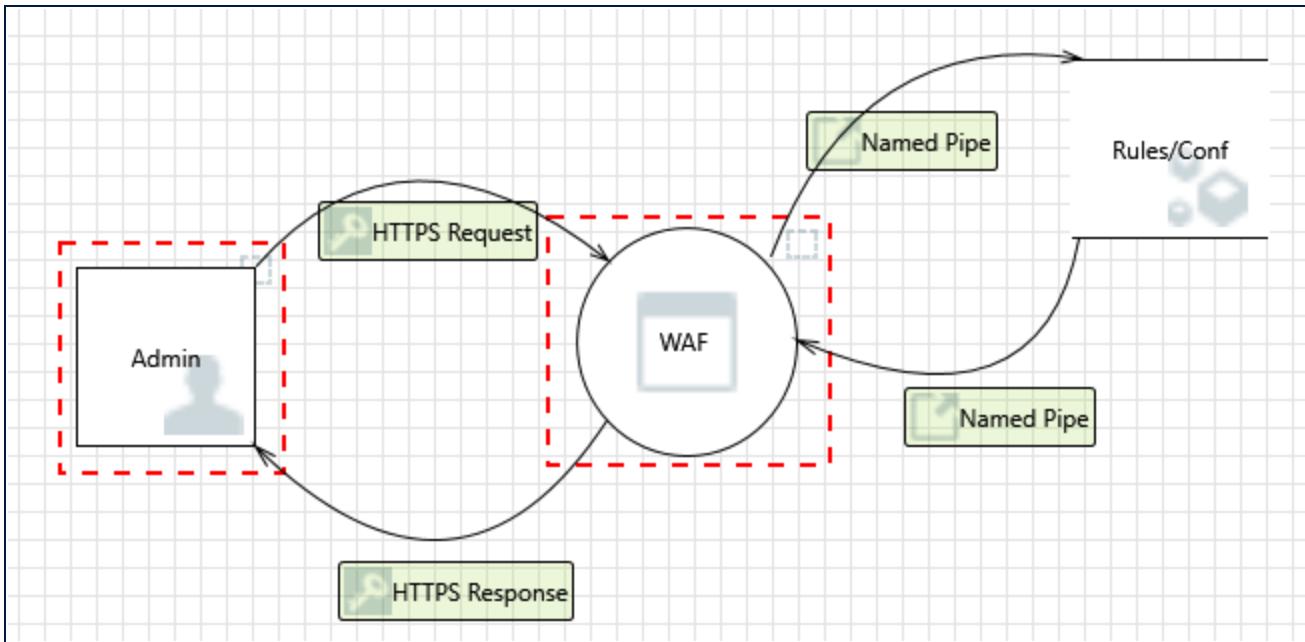
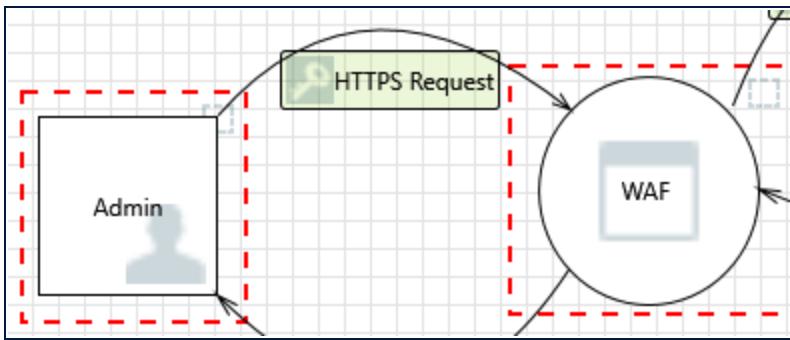


Diagram 1 Diagram Summary:

Not Started	18
Not Applicable	0
Needs Investigation	0
Mitigation Implemented	0
Total	18
Total Migrated	0

### Interaction: HTTPS Request



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

**Category:** Elevation Of Privilege

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

**Justification:** <no mitigation provided>

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

**Category:** Repudiation

**Description:** 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>

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

**Category:** Denial Of Service

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

**Justification:** <no mitigation provided>

### 4. Data Flow HTTPS 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>

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

**Category:** Elevation Of Privilege

**Description:** Admin may be able to remotely execute code for WAF .

**Justification:** <no mitigation provided>

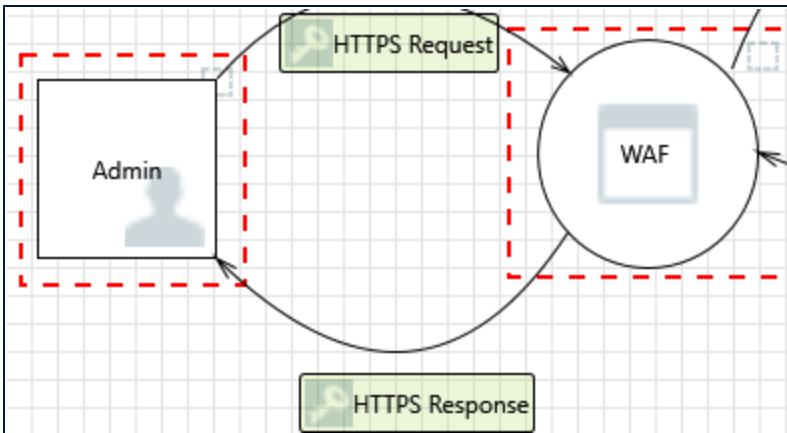
### 6. Elevation by Changing the Execution Flow in WAF [State: Not Started] [Priority: High]

**Category:** Elevation Of Privilege

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

**Justification:** <no mitigation provided>

**Interaction:** HTTPS Response



## 7. Spoofing of the Admin External Destination Entity [State: Not Started] [Priority: High]

**Category:** Spoofing

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

**Justification:** <no mitigation provided>

## 8. External Entity Admin Potentially Denies Receiving Data [State: Not Started] [Priority: High]

**Category:** Repudiation

**Description:** Admin 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>

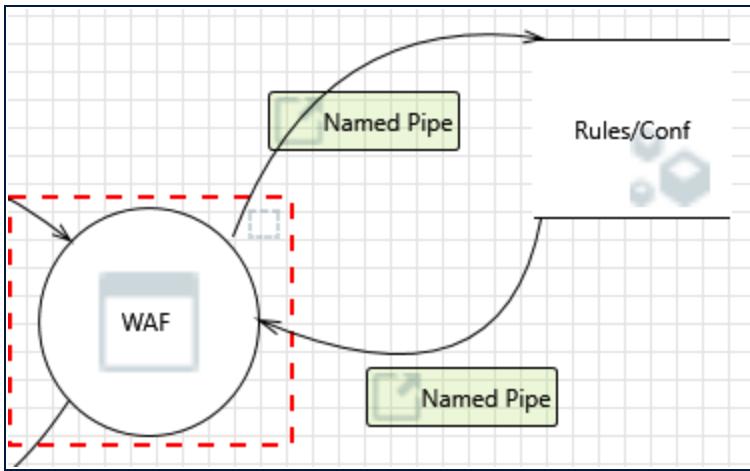
## 9. Data Flow HTTPS Response Is Potentially Interrupted [State: Not Started] [Priority: High]

**Category:** Denial Of Service

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

**Justification:** <no mitigation provided>

**Interaction:** Named Pipe



10. Spoofing of Source Data Store Rules/Conf [State: Not Started] [Priority: High]

**Category:** Spoofing

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

**Justification:** <no mitigation provided>

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

**Category:** Information Disclosure

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

**Justification:** <no mitigation provided>

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

**Category:** Spoofing

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

**Justification:** <no mitigation provided>

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

**Category:** Repudiation

**Description:** 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>

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

**Category:** Denial Of Service

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

**Justification:** <no mitigation provided>

#### 15. Data Flow Named Pipe 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>

#### 16. 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>

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

**Category:** Elevation Of Privilege

**Description:** Rules/Conf may be able to remotely execute code for WAF .

**Justification:** <no mitigation provided>

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

**Category:** Elevation Of Privilege

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

**Justification:** <no mitigation provided>