Web Server Threat Model

Owner:
Reviewer:
Contributors:
Date Generated: Mon Sep 30 2024

Executive Summary

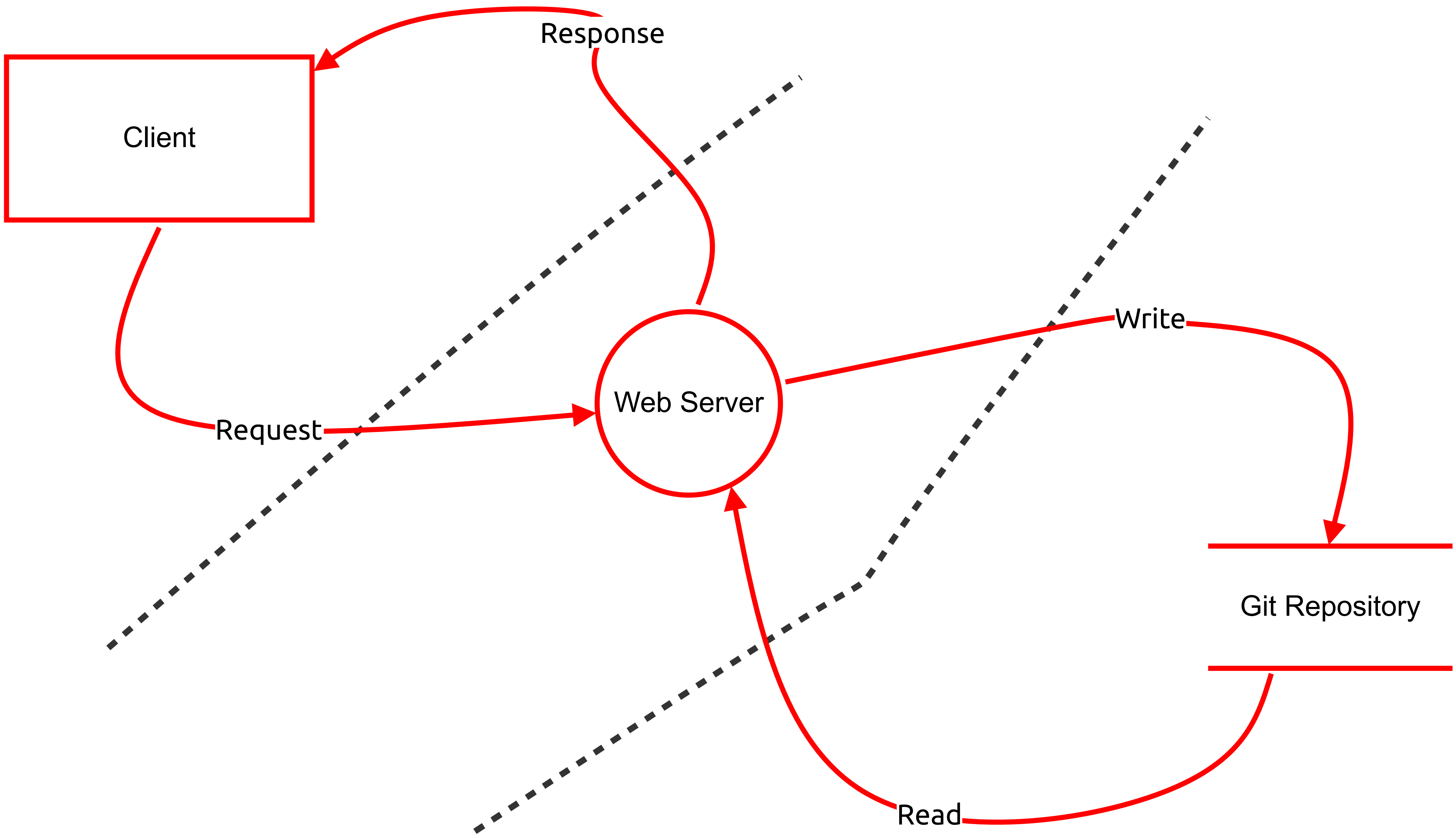
High level system description

This threat model represents an external user that interacts with a web server, which communicates with a backing Git repository (theoretically) for version control.

Summary

Total Threats	24
Total Mitigated	0
Not Mitigated	24
Open / High Priority	0
Open / Medium Priority	24
Open / Low Priority	0
Open / Unknown Priority	0

Web Server Threat Model



Web Server Threat Model

Client (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	Client Spoofing Attack	Spoofing	Medium	Open		An attack may impersonate a legitimate process in a/the system to execute malicious code.	Strong Authentication, Certificates, PKI
13	Client Repudiation	Repudiation	Medium	Open		The process could deny executing specific actions, especially if logs are tampered with or detailed insufficiently.	Logging, non-repudiation mechanisms (signatures), secure log storage

Web Server (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Web Server Spoofing Attack	Spoofing	Medium	Open		An attack may impersonate a legitimate process in a/the system to execute malicious code.	Strong Authentication, Certificates, PKI
5	Web Server Tampering Attack	Tampering	Medium	Open		An attacker could modify the execution of the process to alter its behavior, such as injecting malicious code.	Integrity checks, encryption, digital signatures
	Web Server Repudiation	Repudiation	Medium	Open		The process could deny executing specific actions, especially if logs are tampered with or detailed insufficiently.	Logging, non-repudiation mechanisms (signatures), secure log storage
7	Web Server Information Disclosure	Information disclosure	Medium	Open		This is sensitive information proceeded by the process could be exposed to adversarial processes.	Encryption, Access Control, TLS, data masking
8	Web Server Denial of Service Attack	Denial of service	Medium	Open		The process might be overwhelmed by excessive requests, which in turn, prevents it from functioning properly.	Rate Limiting, load balancing, WAF, DDoS Protection
9	Web Server Elevation of Privilege	Elevation of privilege	Medium	Open		A user could exploit the process to gain unauthorized administrative privileges.	Least Privilege Principle, RBAC, patch management, monitoring

Write (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
22	Write Tampering Attack	Tampering	Medium	Open		An attacker could modify the execution of the process to alter its behavior, such as injecting malicious code.	Integrity checks, encryption, digital signatures
23	Write Information Disclosure	Information disclosure	Medium	Open		This is sensitive information proceeded by the data flow that could be exposed to adversarial processes.	Encryption, Access Control, TLS, data masking
24	Write Denial of Service Attack	Denial of service	Medium	Open		The data flow might be overwhelmed by excessive requests, which in turn, prevents it from functioning properly.	Rate Limiting, load balancing, WAF, DDoS Protection

Read (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
28	Read Tampering Attack	Tampering	Medium	Open		An attacker could modify the execution of the data flow to alter its behavior, such as injecting malicious code.	Integrity checks, encryption, digital signatures
29	Read Information Disclosure	Information disclosure	Medium	Open		This is sensitive information proceeded by the data flow could be exposed to adversarial processes.	Encryption, Access Control, TLS, data masking
30	Read Denial of Service	Denial of service	Medium	Open		The data flow might be overwhelmed by excessive requests, which in turn, prevents it from functioning properly.	Rate limiting, load balancing, WAF, DDoS Protection

Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
31	Request Tampering Attack	Tampering	Medium	Open		An attacker could modify the execution of the data flow to alter its behavior, such as injecting malicious code	Integrity checks, encryption, digital signatures
32	Request Information Disclosure	Information disclosure	Medium	Open		This is sensitive information proceeded by the process data flow could be exposed to adversarial processes.	Encryption, Access Control, TLS, data masking
33	Request Denial of Service	Denial of service	Medium	Open		The data flow might be overwhelmed by excessive requests, which in turn, prevents it from functioning properly.	Rate limiting, load balancing, WAF, DDoS Protection

Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	Response Tampering Attack	Tampering	Medium	Open		An attacker could modify the execution of the process to alter its behavior, such as injecting malicious code	Integrity checks, encryption, digital signatures
35	Response Information Disclosure	Information disclosure	Medium	Open		This is sensitive information proceeded by the process could be exposed to adversarial processes.	Encryption, Access Control, TLS, data masking
36	Response Denial of Service	Denial of service	Medium	Open		The data flow might be overwhelmed by excessive requests, which in turn, prevents it from functioning properly.	Rate Limiting, load balancing, WAF, DDoS Protection

Git Repository (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
14	Git Repo Tampering	Tampering	Medium	Open		An attacker could modify the execution of the process to alter its behavior, such as injecting malicious code.	Integrity checks, encryption, digital signatures
16	Git Repo Repudiation	Repudiation	Medium	Open		The Git Repo could deny executing specific actions, especially if logs are tampered with or detailed insufficiently.	Logging, non-repudiation mechanisms (signatures), secure log storage
17	Git Repo Information Disclosure	Information disclosure	Medium	Open		This is sensitive information proceeded by the process could be exposed to adversarial processes.	Encryption, Access Control, TLS, data masking
18	Git Repo Denial of Service	Denial of service	Medium	Open		The Git Repo might be overwhelmed by excessive requests, which in turn, prevents it from functioning properly.	Rate Limiting, load balancing, WAF, DDoS Protection