Mini Zanzibar

Owner:
Reviewer:
Contributors:
Date Generated: Sun Jun 23 2024

Executive Summary

High level system description

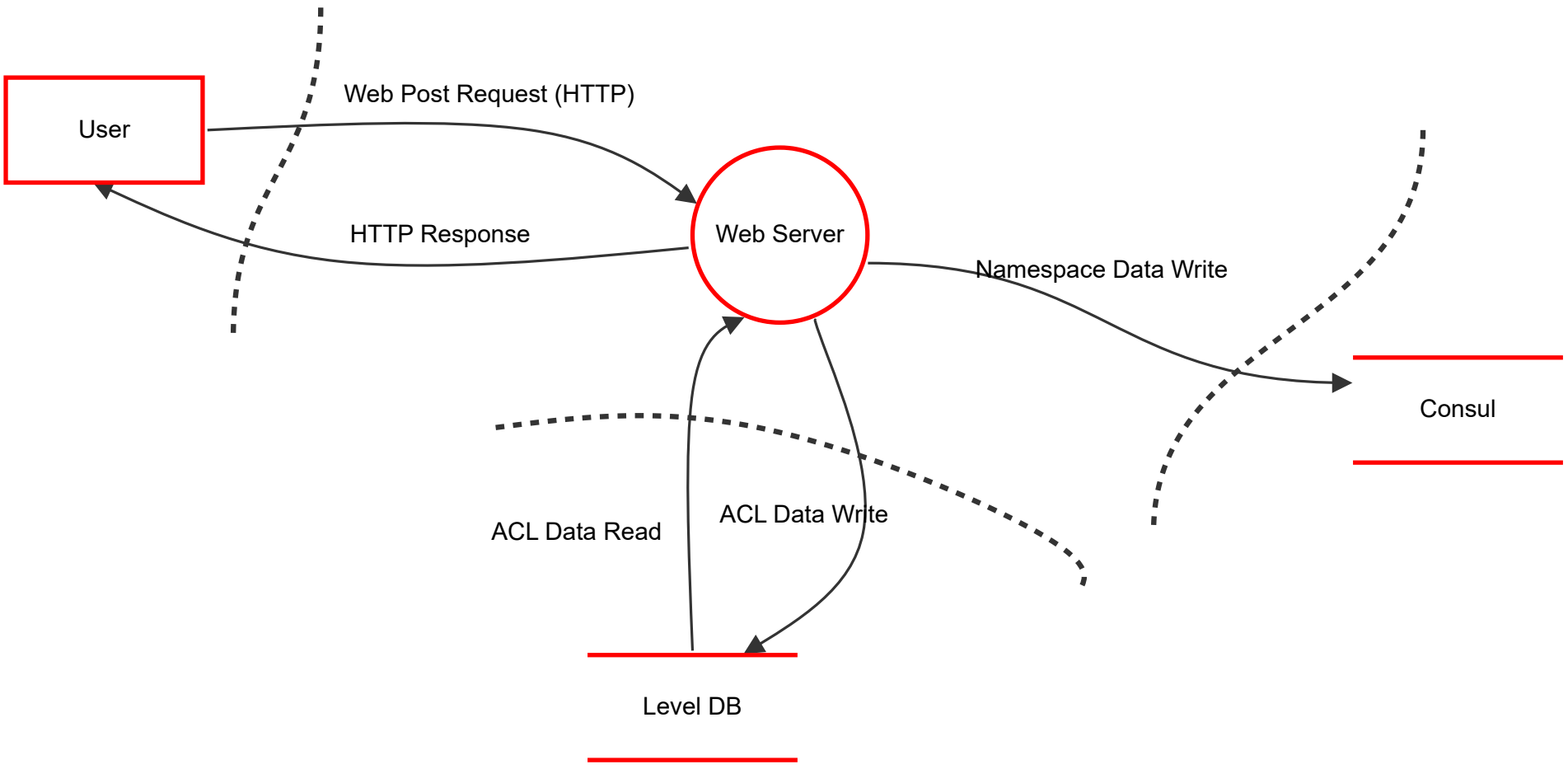
Not provided

Summary

Total Threats	10
Total Mitigated	0
Not Mitigated	10
Open / High Priority	1
Open / Medium Priority	9
Open / Low Priority	0
Open / Unknown Priority	0

Mini Zanzibar Stride

Threat Model for Mini Zanzibar



Mini Zanzibar Stride

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User (Actor)

Frontend

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	Malicious request	Spoofing	High	Open		An attacker can impersonate a User and send malicious requests.	Implement strong user authentication and access control to reduce opportunities for impersonation and privilege escalation. Implement detailed logging and auditing to enable monitoring and verification of user actions.

Web Server (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	Transit data attack threat	Tampering	Medium	Open		(Web Post Request (HTTP), HTTP Response) between the user and the web server can be modified if it is not encrypted. An attacker can intercept and modify data in transit.	Ensure that all data in transit is encrypted using TLS.
14	Inadequate Logging and Auditing	Repudiation	Medium	Open		The Web Server should have appropriate logging and auditing to prevent denial of actions by users or attackers. The lack of these mechanisms allows users or attackers to deny their activities.	Implement detailed logging and auditing to enable monitoring and verification of user actions.
15	Unencrypted Data Transmission	Information disclosure	Medium	Open		Data Flow can reveal sensitive information if communication is not encrypted. Attackers can eavesdrop on traffic between users and web servers.	Ensure that all data in transit is encrypted using TLS.
17	Denial of Service (DoS) Attack	Tampering	Medium	Open		Web Server can be the target of a DoS attack, where attackers can flood the server with requests, thereby denying legitimate access to users.	Traffic Management: Use load balancers and rate limiters to manage incoming traffic and mitigate the impact of volumetric attacks. Network Security: Deploy firewalls and intrusion detection/prevention systems (IDPS) to filter out malicious traffic. Resource Scaling: Scale infrastructure resources (such as servers and bandwidth) to handle sudden spikes in traffic. DDoS Protection Services: Consider using specialized DDoS protection services that can detect and mitigate attacks in real-time.
19	Privilege Escalation Attack on Web Server	Spoofing	Medium	Open		Attackers target the Web Server with the goal of escalating their privileges, gaining access to resources and capabilities beyond their authorized permissions.	Assign minimal privileges necessary for users and processes to perform their functions, reducing the impact of potential privilege escalation. Keep software and applications on the Web Server up to date with security patches to mitigate known vulnerabilities. Monitor server activities, log access attempts, and set up alerts for suspicious activities or unauthorized privilege escalations.

Level DB (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
16	Data Disclosure	Information disclosure	Medium	Open		Data can be exposed if it is not adequately protected.	Implement robust access controls and authentication mechanisms to restrict access to sensitive data. Encrypt sensitive information both at rest (stored data) and in transit (data being transmitted). Regularly audit and monitor access to sensitive data to detect unauthorized access or anomalies. Train employees and users on data protection best practices and awareness.
18	Resource Exhaustion Attack on LevelDB	Tampering	Medium	Open		Level DB can be the target of attacks that can exhaust database resources, thus slowing down or preventing access to data.	Implement controls to limit the rate of requests or queries to LevelDB, preventing overload from excessive traffic. Set up monitoring systems to detect unusual spikes in database activity or resource consumption, triggering alerts for timely intervention. Optimize LevelDB configurations and performance parameters to handle peak loads more efficiently and resist resource exhaustion attempts.

Consul (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Security Risks to Consul	Tampering	Medium	Open		Attackers may attempt to modify or tamper with data stored in Consul, such as service configurations or key-value pairs, leading to operational disruptions or unauthorized access.	Configure strict access controls and authentication mechanisms for Consul APIs and user interfaces to prevent unauthorized access. Encrypt data stored in Consul to protect it from unauthorized disclosure or tampering.
21	Security Risks to Consul [Information disclosure]	Information disclosure	Medium	Open		Vulnerabilities in Consul could potentially expose sensitive information, such as credentials or configuration details, to unauthorized parties.	Conduct regular security audits and vulnerability assessments of Consul configurations and deployments. Encrypt data stored in Consul to protect it from unauthorized disclosure or tampering.