Student Website Threat Model

Owner: Teacher
Reviewer: Tuomas Hänninen
Contributors:
Date Generated: Thu Sep 12 2024

Executive Summary

High level system description

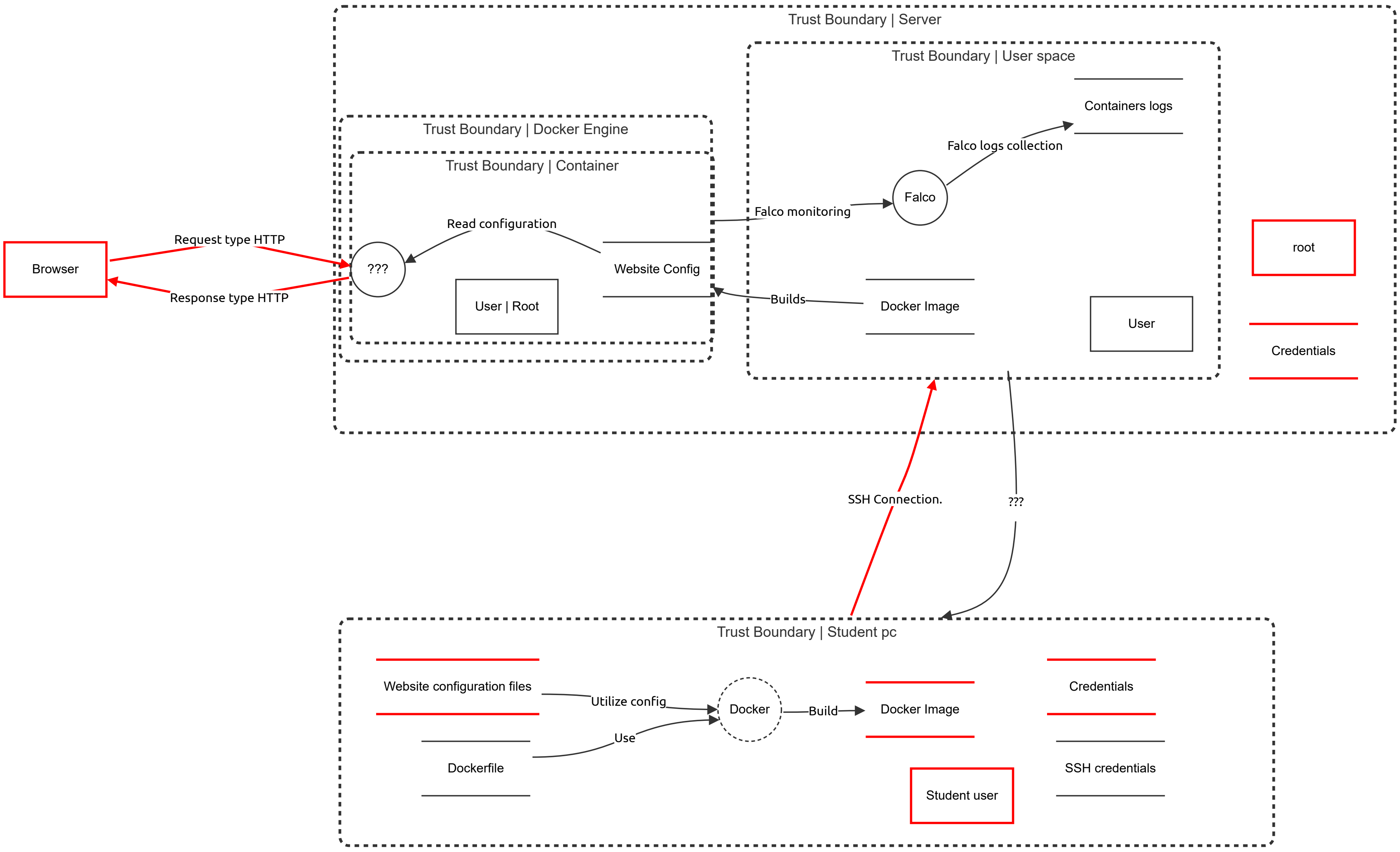
Whole system for a containerized website on cloud node.

Summary

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

System STRIDE

System includes: student's pc, cloud server and container.



System STRIDE

Browser (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Outdated browser STRIDE threat	Spoofing	Medium	Open		Outdated browser version.	Keep your browsers updated. Auto-updating is recommended.

??? (Process)

Engine

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Website Config (Store)

HTML and CSS for the website

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Read configuration (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response type HTTP (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Unsecure request type STRIDE threat	Tampering	Medium	Open		HTTP is not secure request type.	Use HTTPS for more secure request protocols

Request type HTTP (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Unsecure requests STRIDE threat	Tampering	Medium	Open		HTTP is not secure	Use HTTPS for more secure request protocols

Builds (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Falco monitoring (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Falco logs collection (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Build (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SSH Connection. (Data Flow)

Dev env to server, used to copy image and update image.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	Secure SSH STRIDE threat	Tampering	Medium	Open		Unsecure SSH Connection	Generate SSH key pairs securely, like using OpenSSH

Use (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Utilize config (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

???
(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Docker Image (Store)

Ready made docker image

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Containers logs (Store)

Container monitoring via Falco

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Falco (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Website configuration files (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Website configuration STRIDE threat	Tampering	Medium	Open		Using outdated tools eg. WordPress can lead to your website having exploitable vulnerabilities	Make sure to use up-to-date tools when configuring websites

Dockerfile (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Docker (Process) *- Out of Scope*

Builds docker image

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Docker Image (Store)

Includes website configuration files

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	New STRIDE threat	Tampering	Medium	Open		Docker Images can contain many vulnerabilities related to their content, especially if pulled from public registry.	Provide remediation for this threat or a reason if status is N/A

SSH credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Credentials STRIDE threat	Information disclosure	Medium	Open		Unencrypted credentials.	Credentials should be encrypted in a proper manner

root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Unsecured root STRIDE threat	Spoofing	Medium	Open		Unsecured root can lead to system takeover	Keep firewalls updated and credentials secure.

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Unsecure Credentials STRIDE threat	Tampering	Medium	Open		Unsecure credentials	Use password manager with complex passwords that are not easily crackable.

Student user (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
11	Outdated OS STRIDE threat	Spoofing	Medium	Open		Outdated Operating system with vulnerabilites	Keep OS Updated

User | Root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations