Student Website Threat Model

Owner: Teacher
Reviewer: Kalle Haapalainen
Contributors:
Date Generated: Thu Sep 12 2024

Executive Summary

High level system description

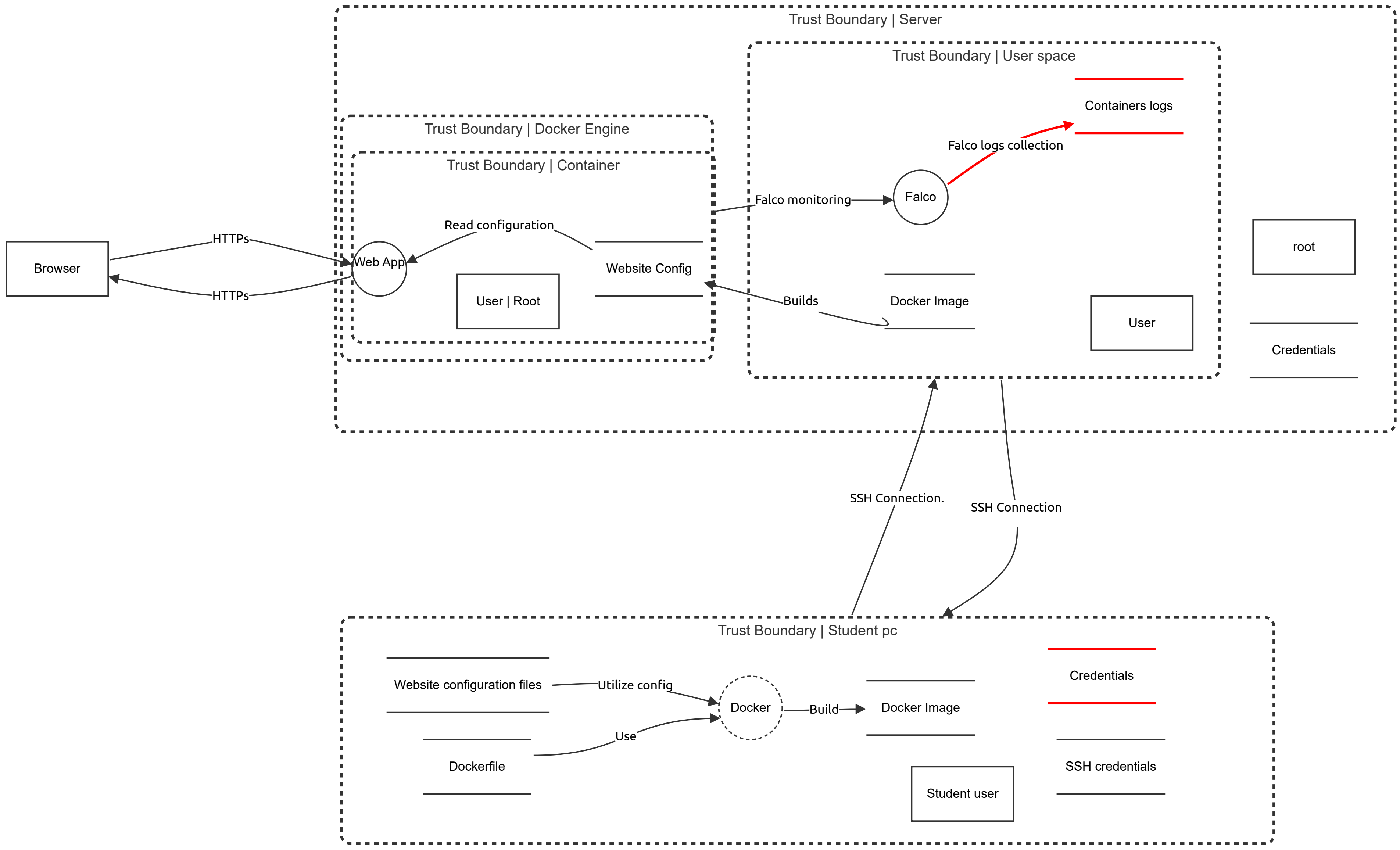
Whole system for a containerized website on cloud node.

Summary

Total Threats	9
Total Mitigated	6
Not Mitigated	3
Open / High Priority	0
Open / Medium Priority	3
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

Web App (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
16	New STRIDE threat	Information disclosure	Medium	Mitigated		Website config should be encrypted	Changed to encrypted

Read configuration (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

HTTPs (Data Flow)

Secure connection from an outside browser

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	New STRIDE threat	Tampering	Medium	Mitigated		Should be encrypted	Change to encrypted

HTTPs (Data Flow)

Secure connection to an outside browser

Number	Title	Type	Priority	Status	Score	Description	Mitigations
17	New STRIDE threat	Tampering	Medium	Mitigated		Should be encrypted	Change to encrypted

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
0	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

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

Use (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Utilize config (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SSH Connection (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Builds
(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
13	New STRIDE threat	Tampering	Medium	Open		Not marked as a log?	Mark as a log
14	New STRIDE threat	Information disclosure	High	Mitigated		Encrypt logs for security	Provide remediation for this threat or a reason if status is N/A
15	New STRIDE threat	Tampering	Medium	Mitigated		Logs might store sensitive information and good to have signed in	Change to signed

Falco (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Website configuration files (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

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

SSH credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	New STRIDE threat	Information disclosure	Medium	Mitigated		Credentials are not encrypted	Add encryption to stored credentials
0	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Student user (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User | Root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations