Student Website Threat Model

Owner: Teacher
Reviewer: Henri Meriläinen
Contributors:
Date Generated: Mon Sep 09 2024

Executive Summary

High level system description

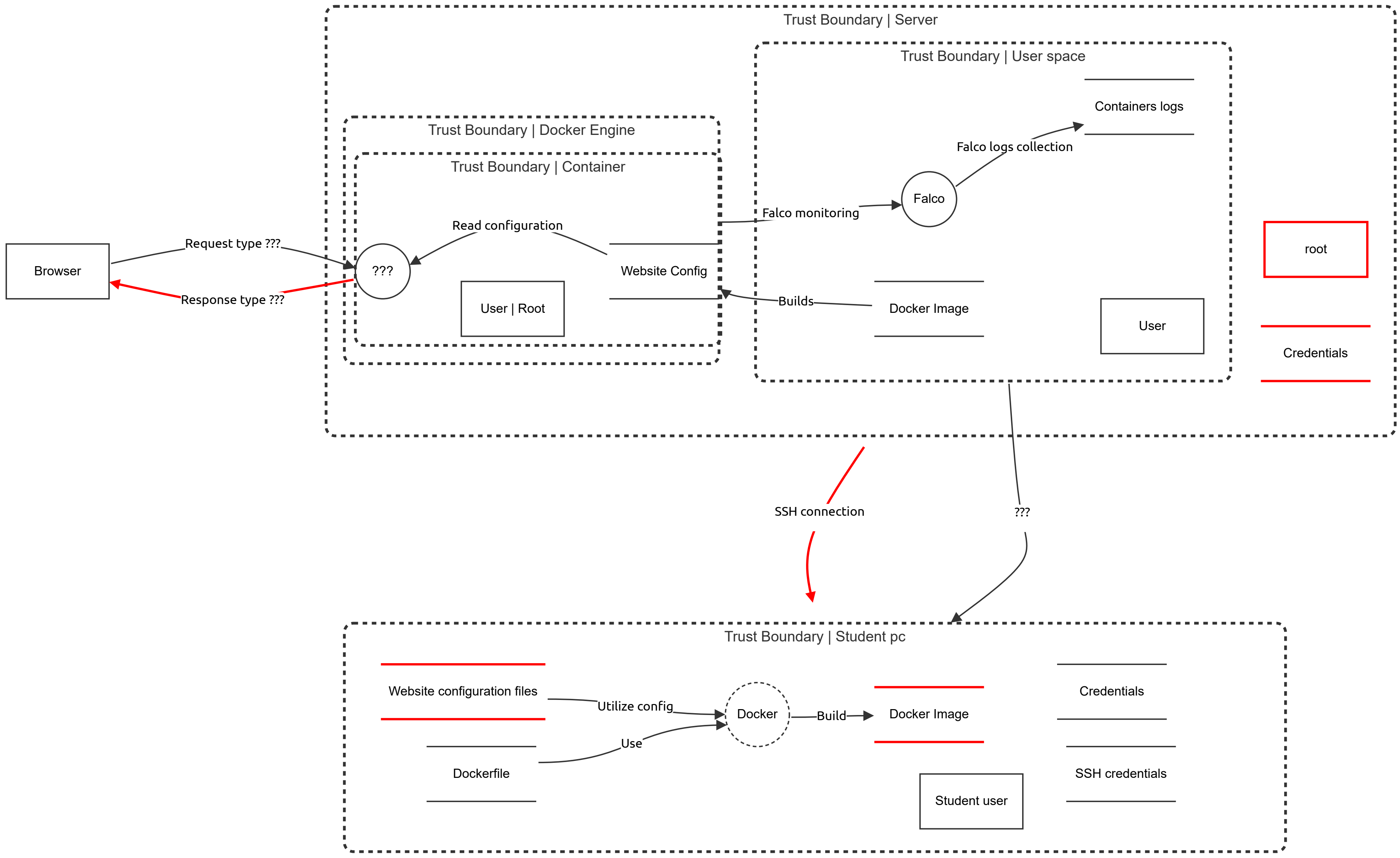
Whole system for a containerized website on cloud node.

Summary

Total Threats	10
Total Mitigated	5
Not Mitigated	5
Open / High Priority	0
Open / Medium Priority	5
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

??? (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 ??? (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Tampering	Medium	Open		If the the communication between the browser and the container for some reason is not secure. Threats like man in the middle attacks are a possibility.	Provide remediation for this threat or a reason if status is N/A

Request type ??? (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

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

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

SSH connection
(Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Tampering	Medium	Mitigated		there are many SSH connection threats, like Unapproved SSH servers, Unpatched SSH software, Vulnerable SSH configuration etc.	make sure to use approved servers, patch all softwares and make sure the SSH configuration is configurated correctly

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
0	New STRIDE threat	Spoofing	Medium	Mitigated		If Falco is somehow not for example updated or configured, threats and vulnerabilities can appear that Falco doesn't detect.	ensure that Falco is updated and configured correctly

Website configuration files (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Tampering	Medium	Open		the website configuration files can possibly be malicious.	Provide remediation for this threat or a reason if status is N/A

Dockerfile (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Information disclosure	Medium	Mitigated		the dockerfile itself can contain malicious packages, code and vulnerabilities.	Go through the file and make sure there is no malicious code. Use approved packages. Also make sure to understand the file.

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
0	New STRIDE threat	Tampering	Medium	Open		the docker image can be vulnerable or malicious.	Provide remediation for this threat or a reason if status is N/A

SSH credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Tampering	Medium	Mitigated		if the SSH credentials are not strong then brute force attacks are a threat.	make sure the SSH credentials are strong and use multi factor authentication if possible.

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Tampering	Medium	Open		if an attacker gains access to server's credentials, He can get to the servers contents and possibly tamper them.	Provide remediation for this threat or a reason if status is N/A

root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Spoofing	Medium	Open		if an attacker gets root priviliges. He can escalate priviliges and control the server	Provide remediation for this threat or a reason if status is N/A

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Tampering	Medium	Mitigated		if the credentials are not strong for the students pc, it is a threat	Make sure the credentials are strong enough and use multi factor authentication if possible

Student user (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User | Root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations