Student Website Threat Model by Anton Chendea

Owner: Teacher
Reviewer: Anton Chendea
Contributors:
Date Generated: Fri Sep 13 2024

Executive Summary

High level system description

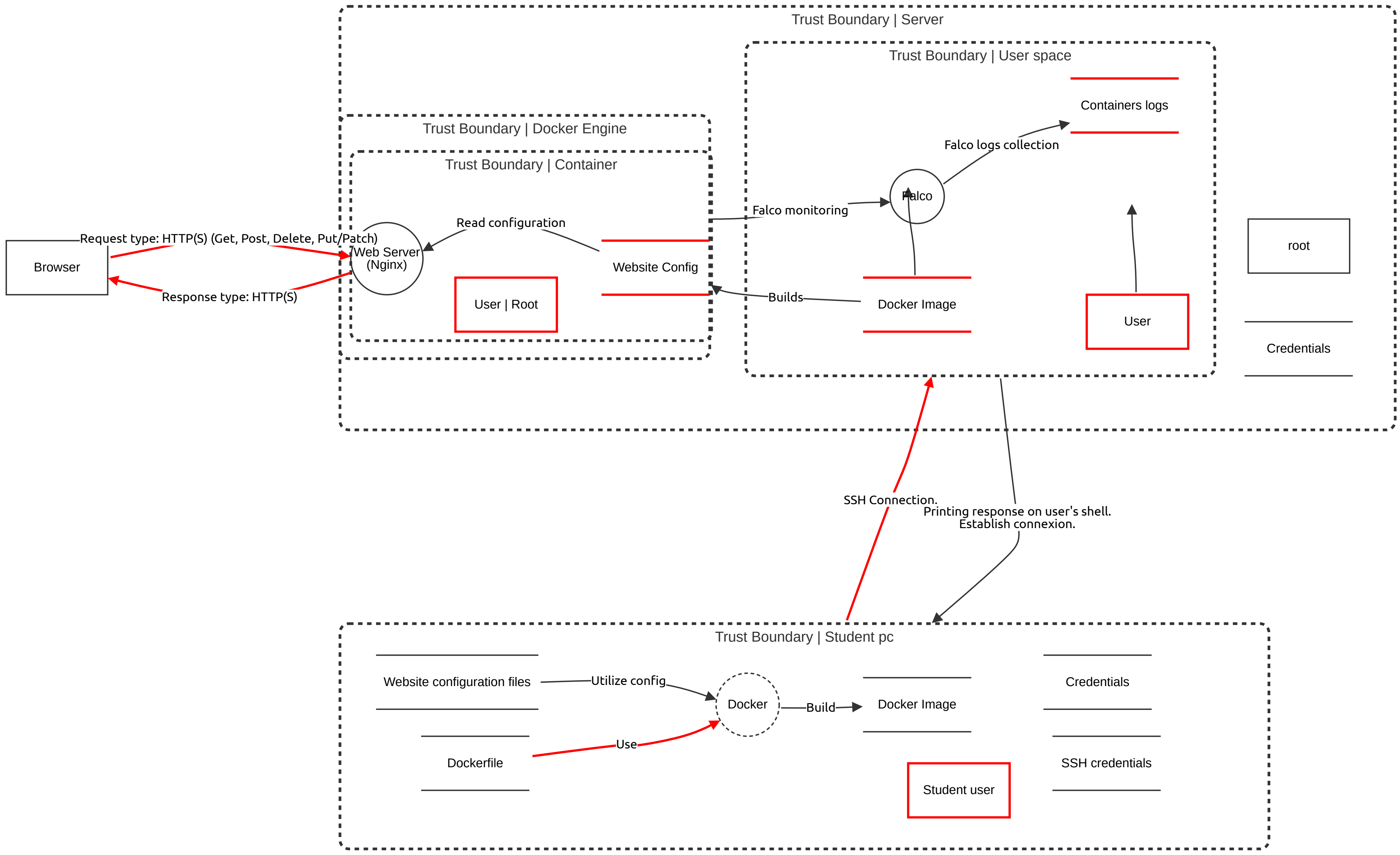
Whole system for a containerized website on cloud node.

Summary

Total Threats	11
Total Mitigated	0
Not Mitigated	11
Open / High Priority	0
Open / Medium Priority	11
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 Server (Nginx) (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
11	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Don't put important information on the website config (password, information on administrator...), encrypt configuration to prevent users access to its, never let link to DB or logs, limit access (to administrator for example), don't let the possibility to do modifications or SQL injections for avoid some breach exploit.

Read configuration (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Response type: HTTP(S) (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	STRIDE threat	Denial of service	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Request type: HTTP(S) (Get, Post, Delete, Put/Patch) (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

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
2	STRIDE threat	Denial of service	Medium	Open		Provide a description for this threat	Limit the number of authentification attempts for avoid some brute forces attacks, implement protection as Fail2ban wich can do some analysis on malicious behavior and take protection measures like ban an IP. Use TCP wrappers to filter access and blacklist some strange IP or networks.

Use (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Utilize config (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Printing response on user's shell. Establish connexion. (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

Docker Image (Store)

Ready made docker image

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Secure admission on it (don't let the possibility to user to access and modify), Use DCT to sign images, isolate information of the docker image for avoid all tampering try on it, check regulary for some strange changes.

Containers logs (Store)

Container monitoring via Falco

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	New STRIDE threat	Information disclosure	Medium	Open		Provide a description for this threat	Limit logs access with withlist, allow just administrators account access to the logs.

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
8	New STRIDE threat	Spoofing	Medium	Open		Provide a description for this threat	On site : don't store passwords in plain text, use secure hashing algorithm (with salt and peppering), do brute force protection by limiting attempts, have a strong password policy For users: use strong passwords, never share it

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Student user (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	New STRIDE threat	Spoofing	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A
6	New STRIDE threat	Repudiation	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

User | Root (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	New STRIDE threat	Spoofing	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A