## Threat model report for Student Website Threat Model

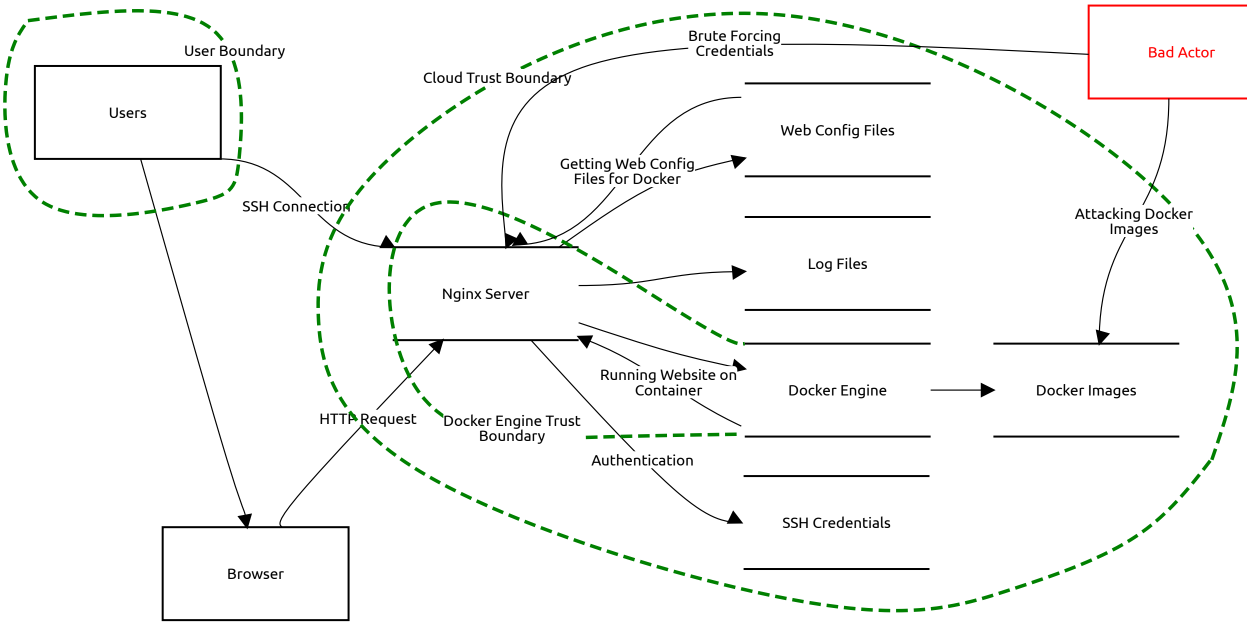
**Owner:**
Teacher
**Reviewer:**
Abdurrehman Syed
**Contributors:**

## High level system description

Whole system for a containerized website on cloud node.

Report printing failed

## System STRIDE



### Users (External Actor)

**Description:**

*No threats listed.*

### Browser (External Actor)

**Description:**

*No threats listed.*

### Nginx Server (Data Store)

**Description:**
Hosts Website

*No threats listed.*

Report printing failed

### Web Config Files (Data Store)

**Description:**

*No threats listed.*

### Log Files (Data Store)

**Description:**

*No threats listed.*

### Docker Images (Data Store)

**Description:**

*No threats listed.*

### Docker Engine (Data Store)

**Description:**

*No threats listed.*

### SSH Credentials (Data Store)

**Description:**

*No threats listed.*

### (Data Flow)

**Description:**

*No threats listed.*

### (Data Flow)

**Description:**

*No threats listed.*

Report printing failed

### (Data Flow)

**Description:**

*No threats listed.*

### Authentication (Data Flow)

**Description:**

*No threats listed.*

### HTTP Request (Data Flow)

**Description:**

*No threats listed.*

### (Data Flow)

**Description:**

*No threats listed.*

### SSH Connection (Data Flow)

**Description:**

*No threats listed.*

### (Data Flow)

**Description:**

*No threats listed.*

### Running Website on Container (Data Flow)

**Description:**

*No threats listed.*

Report printing failed

### Getting Web Config Files for Docker (Data Flow)

**Description:**

*No threats listed.*

Report printing failed

## Bad Actor (External Actor)

**Description:**

### SSH Auth Bypass

*Spoofing, Mitigated, Medium Severity*

**Description:**
Actor can impersonate other users by brute forcing their way and trying out credentials.

**Mitigation:**
SSH Key-Based Authentication, Enable Multi-factor Authentication (MFA)

### Tampering With Docker

*Tampering, Mitigated, Low Severity*

**Description:**
Attacker with access to docker repo could alter the image used to deploy on website.

**Mitigation:**
Image signing and trusted image sources.

### Lack of Logging

*Repudiation, Mitigated, Medium Severity*

**Description:**
If SSH access and server logins are not logged, attackers can do whatever they want without ability to trace them.

**Mitigation:**
Implement detailed logging, logging server.

### DoS Attacks

*Denial of service, Mitigated, High Severity*

**Description:**
Large number of http requests on the server to slowdown or crash.

**Mitigation:**
Use a software to limit the number of connections SSH attempts allowed and then block IP

Report printing failed

### Sensitive Info in Log Files

*Information disclosure, Mitigated, Low Severity*

**Description:**
Attacker could gain insight by reading logs of the server or docker.

**Mitigation:**
Sensitive logs should be masked and have proper permissions.

### Docker Admin Privilege

*Elevation of privilege, Mitigated, Medium Severity*

**Description:**
If docker is being ran as the root user, a hacker can do anything with that access.

**Mitigation:**
Run docker containers with non-root user permissions.

### DNS Spoofing

*Spoofing, Open, Medium Severity*

**Description:**
Attacker can redirect the users to a malicious version of the website by DNS spoofing responses

**Mitigation:**

### Code Injection in SSH Session

*Tampering, Open, Medium Severity*

**Description:**
Injecting malicious commands into the SSH session.

**Mitigation:**

### Insecure API Endpoints

*Information disclosure, Open, Medium Severity*

**Description:**
Bad security can lead to retrival of sensitive data.

**Mitigation:**

Report printing failed

### File Upload Abuse

*Denial of service, Mitigated, Low Severity*

**Description:**
If there is no limit to the files, attacker can upload large amounts of files and empty out the server storage.

**Mitigation:**
Have a limit.

### Brute Forcing Credentials (Data Flow)

**Description:**

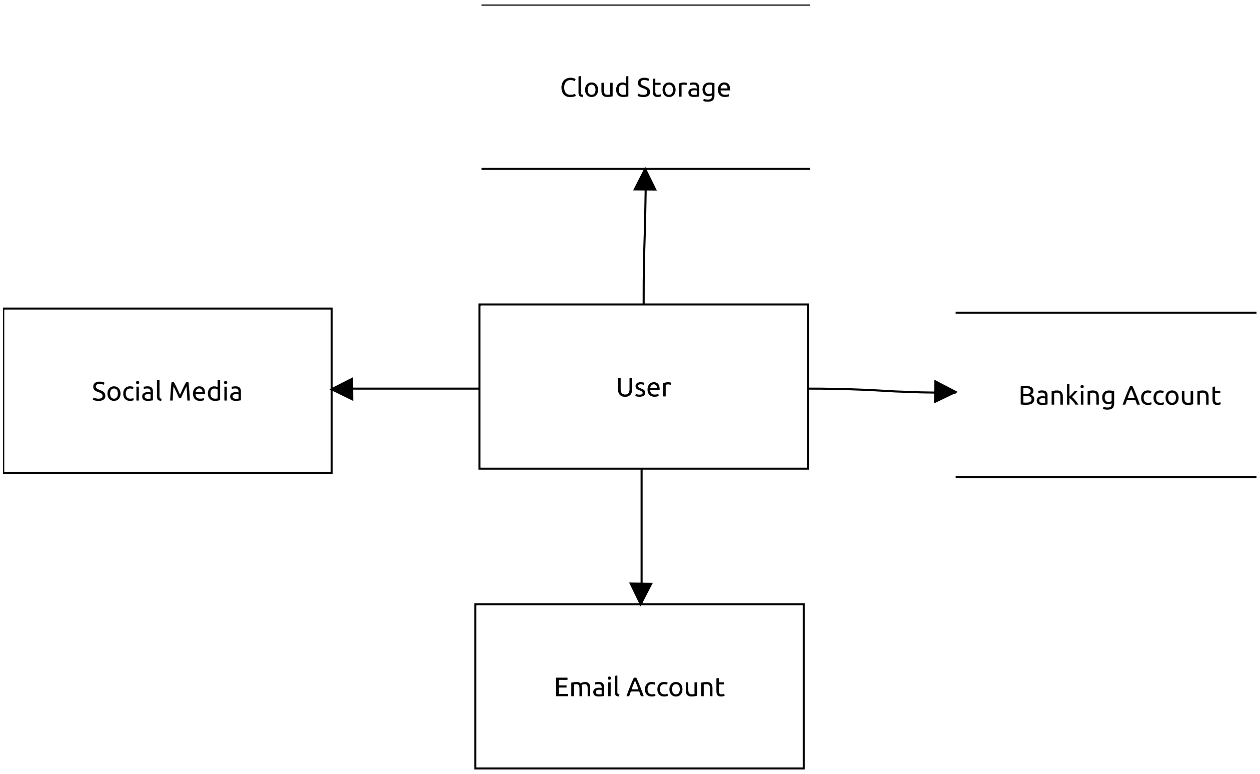
*No threats listed.*

### Attacking Docker Images (Data Flow)

**Description:**

*No threats listed.*

## Task 3.2 - Login Flow



### User (External Actor)

**Description:**

*No threats listed.*

### Email Account (External Actor)

**Description:**

#### Phishing Attack

*Spoofing, Mitigated, Medium Severity*

**Description:**
Attacker creates a fake impersonation

**Mitigation:**
MFA, strong password

Report printing failed

### Social Media (External Actor)

**Description:**

#### Password Breach

*Elevation of privilege, Mitigated, Medium Severity*

**Description:**
weak or reused passwords can lead to unauthorized email, social media, or banking access.

**Mitigation:**

### Banking Account (Data Store)

**Description:**

*No threats listed.*

### Cloud Storage (Data Store)

**Description:**

*No threats listed.*

### (Data Flow)

**Description:**

*No threats listed.*

### (Data Flow)

**Description:**

*No threats listed.*

### (Data Flow)

**Description:**

*No threats listed.*

Report printing failed

(Data Flow)

**Description:**

*No threats listed.*