














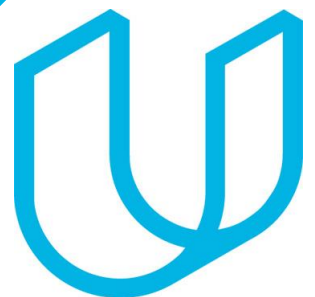


# TimeSheets: Threat Report

**YOUR NAME:** Amr Mohamed  
*DATE : 24/02/2025*



# Purpose of this Report:

This is a threat model report for **TimeSheets**. The report will describe the threats facing TimeSheets. The model will cover the following:

- Threat Assessment
  - Scoping out Asset Inventory
  - Architecture Audit
  - Threat Model Diagram
  - Threats to the Organization
  - Identifying Threat Actors
- Vulnerability Analysis
- Risk Analysis
- Mitigation Plan



# **Section 1**

## Initial Threat Assessment

# Completed Asset Inventory

## Components and Functions

- ***TimeSheets Web Server:*** The web server's primary role is to serve static content to a requesting client through the **http** protocol.
- ***TimeSheets Application Server:*** The application server handles **all** the business logic process and serves dynamic content.
- ***TimeSheetsDB:*** The database server stores employee data and will be queried from the application server.
- ***AuthDB:*** Stores user authentication data (credentials) and will be queried from the application server.

# Completed Asset Inventory

## Overview of Application Functionality

TimeSheets is used by employees to track their hours worked. Users will login to the TimeSheets application from their device.

## Data Flow

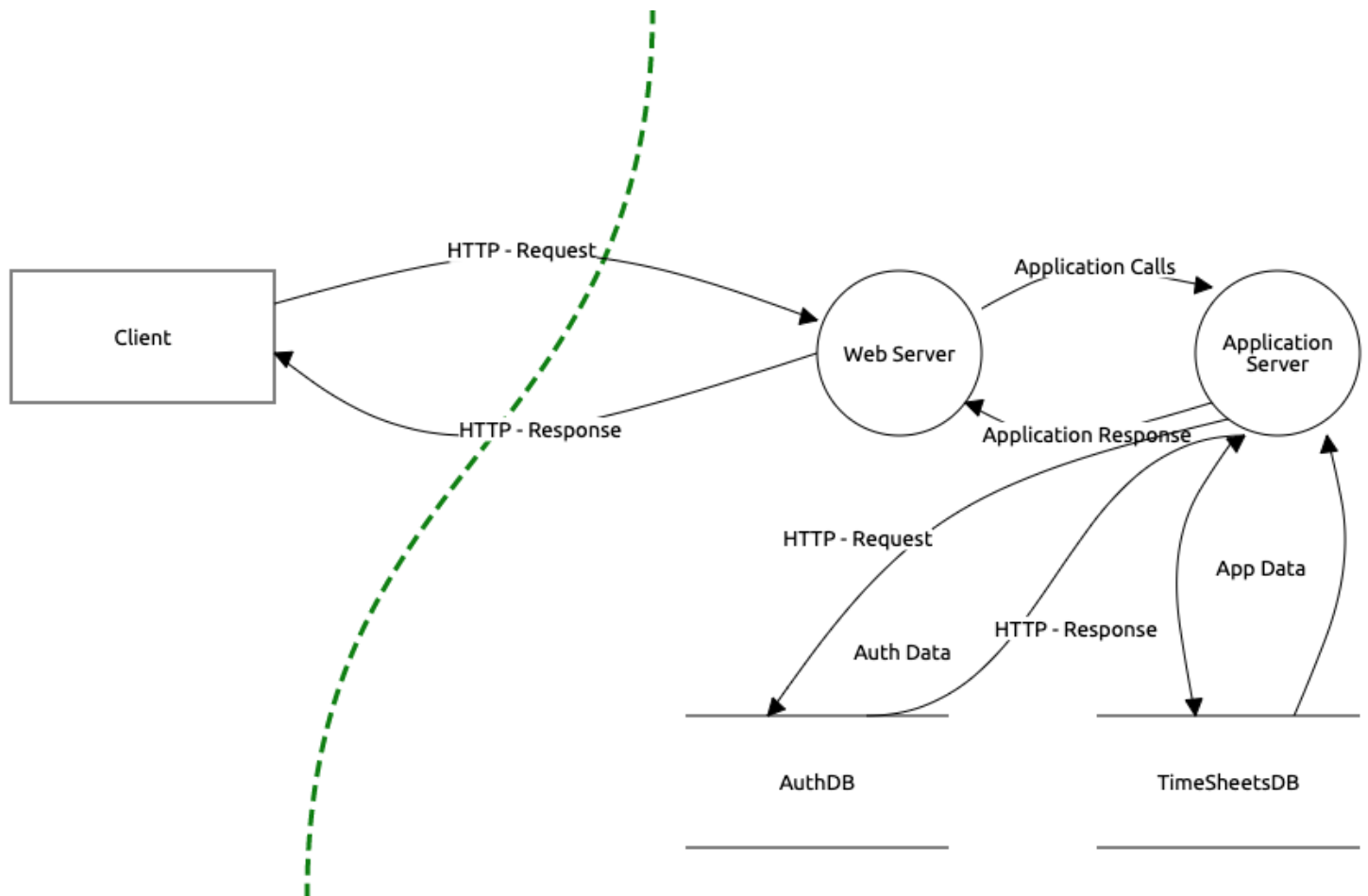
Request is generated from the client via the Internet. The request arrives at the TimeSheets web server which serves static content to the user (HTML, images, etc). Dynamic data is retrieved from the database and served to the client.

# Completed Architecture Audit

## Flaws

- *There is a lack of encryption at rest - database servers are storing data on unencrypted disks.*
- *There is lack of redundancy.*
- *There is no firewall that is filtering traffic coming from the Internet*

# Completed Threat Model



- Employee Data Unencrypted at Rest
- Authentication data is using reversible encryption
- Authentication requests are not encrypted in transit
- Sensitive data is encrypted using DES algorithm

# Completed Threat Analysis

## **What Type of Attack Caused the Login Alerts?**

Man in the Middle (MitM)

## **What Proves Your Theory?**

There is lack of encryption between the client and the application. A malicious actor is sniffing traffic and intercepting the requests with a valid username/password in the request. Additionally, the logs show successful login attempts from the expected IP, but also a different location at the same time.



# Completed Threat Actor Analysis

## Who is the Most Likely Threat Actor?

Internal User

## What Proves Your Theory?

The IP address of the unexpected login matches that of an internal user. Additionally, there was no data leaked from the company, and no data changed. Just data accessed that the legitimate user typically doesn't access.



## **Section 2**

# Vulnerability Analysis

## 2.1 Employee Data Unencrypted at Rest

### **Discovery:**

During threat modeling, the Site Reliability Engineering (SRE) team confirmed that the database is on a server that does not have encryption at rest.

### **Why is this an issue?**

*This can lead to a data leak easily and this also increase the risk of getting ransomware and maximizes attacking surface*

## 2.2 Authentication Data Stored Using Reversible Encryption

### **Discovery:**

During threat modeling, the Database Administrators (DBA) team confirmed that the database is storing authentication data (credentials) encrypted.

### **Why is this an issue?**

*This is not the best way to store credentials as the best way to store credentials is by salting them , hashing them and at last encrypt them.*

## 2.3 Authentication Requests are Unencrypted in Transit

### **Discovery:**

During threat modeling, the security team confirmed that authentication requests are being transmitted in plaintext.

### **Why is this an issue?**

*This is a big issue as the transfer of unencrypted authentication requests could ease the Man in the middle attack, which may result in the unauthorized access by the hacker to the users accounts or credentials. Authentication requests have to be encrypted in asymmetric encryption.*

## 2.4 DES Algorithm in Use

### **Discovery:**

While conducting threat modeling, the security team identified sensitive data being stored using the Data Encryption Standard (DES) algorithm.

### **Why is this an issue?**

*"DES" Algorithm is an insecure Algorithm as it can be brute forced and it has a short key length of (56 bits) while "3DES" has a key length of (168 bits) which is 3 (56 bit) keys, which also means its for sure more secure.*

# Optional Task:

**Examine the threat model diagram from Section 1 and answer:**

**What non-encryption issues can you identify?**

**What recommendation would you give to solve those issues?**

**Why do you recommend those solutions?**

- *[HTTP is used which is not secure and not secure and it is recommended to use HTTPS]*
- *[Every Server should have an IPS or IDS or at least a firewall system to protect it]*



# **Section 3**

## Risk Analysis



# 3.1 Scoring Risks

Risk	Score <i>(1 is most dangerous, 4 is least dangerous)</i>
Unencrypted at Rest	4
Reversible Encryption	3
Unencrypted in Transit	1
Outdated Algorithm	2

## 3.2 Risk Rationale

**Why did you choose that ranking? Make sure to include your risk ranking methodology. Your explanations must be based on the learnings from this course as well as observations from the initial report.** *(Did you use a tool or defined risk scoring system?)*

*According to the OWASP Risk Rating Methodology. Which is*  
*Risk = impact x likelihood*

*1- Unencrypted data : has a high impact and high likelihood due to the interference of the internet in this attack (MITM)*

*2-Outdated algorithm : has high impact but less likelihood causing it to become in the second more threatening risk.*

*3- Reversible encryption : Has a medium impact and low likelihood because the method is not the best but not easy to reverse.*

*4-Unencrypted at rest : is the medium impact but very low likelihood as the server is offline and can be mitigated quickly by encrypting the server's data.*



# **Section 4**

## Mitigation Plan

# 4.1 Employee Data unencrypted at Rest

## **What is Your Recommended Mitigation Plan?**

*The Recommended plan is to encrypt this data by AES-256 Algorithm ASAP to avoid insider attacks and minimize the surface attack*

## **Why Did you Recommend This Course of Action?**

*To minimize the surface attack and avoid the the insider attacks  
And ransomware or any possiable threat.*

## 4.2 Authentication Data Stored using Reversible Encryption

### **What is Your Recommended Mitigation Plan?**

*The Recommended plan is to take the input of the user and then salt his input after that we hash the result then we encrypt it and store it and when the user needs to sign in we decrypt the hash and compare it to the user's input hash.*

### **Why Did you Recommend This Course of Action?**

*This solution is one of the most globally used secure method to store users credentials as I do not want to know the data it self I want to confirm it the correct data and it also relifes the headache of the user's passwords leaks as they are already not stored at the companis servers which makes the company Not legally responsible.*

## 4.3 Authentication Requests are Not Encrypted in Transit

### **What is Your Recommended Mitigation Plan?**

*The recommended plan is to transfer the Authentication Requests using asymmetric encryption.*

### **Why Did you Recommend This Course of Action?**

*To Avoid the Man in the middle attacks and unauthorized access by external parties.*

## 4.4 DES Algorithm in Use

### **What is Your Recommended Mitigation Plan?**

*DES is an outdated encryption algorithm which means it can be brute forced meaning replacing it with 3DES is free of cost and more secure.*

### **Why Did you Recommend This Course of Action?**

*Because 3DES is a secure option for encrypting data at rest and it's cost free and ensures that even if the data was leaked to a malicious actor that this data will become useless to use.*

## 4.5 Security Audit

**The audit team has been made aware of the systemic issue and wants to ensure your recommendations are followed. What steps can the audit team take?**

*The security audit team should define their scopes then assess the present controles and check if they are functional as needed, after that the risk of these assets getting attacked is caluculated and priotarized m they can also check compliance with high regulation standards such as GDPR and HIPAA . After knowing all the possiable weakneses they can add corrective controles like patching systems or preventive systems like IPS or detective controls like CCTVs or IDSs.*