














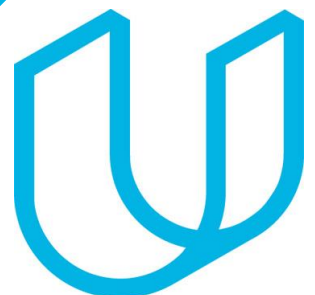


TimeSheets: Threat Report

Abdullah Al-Khammash
Date : 18/10/2022



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

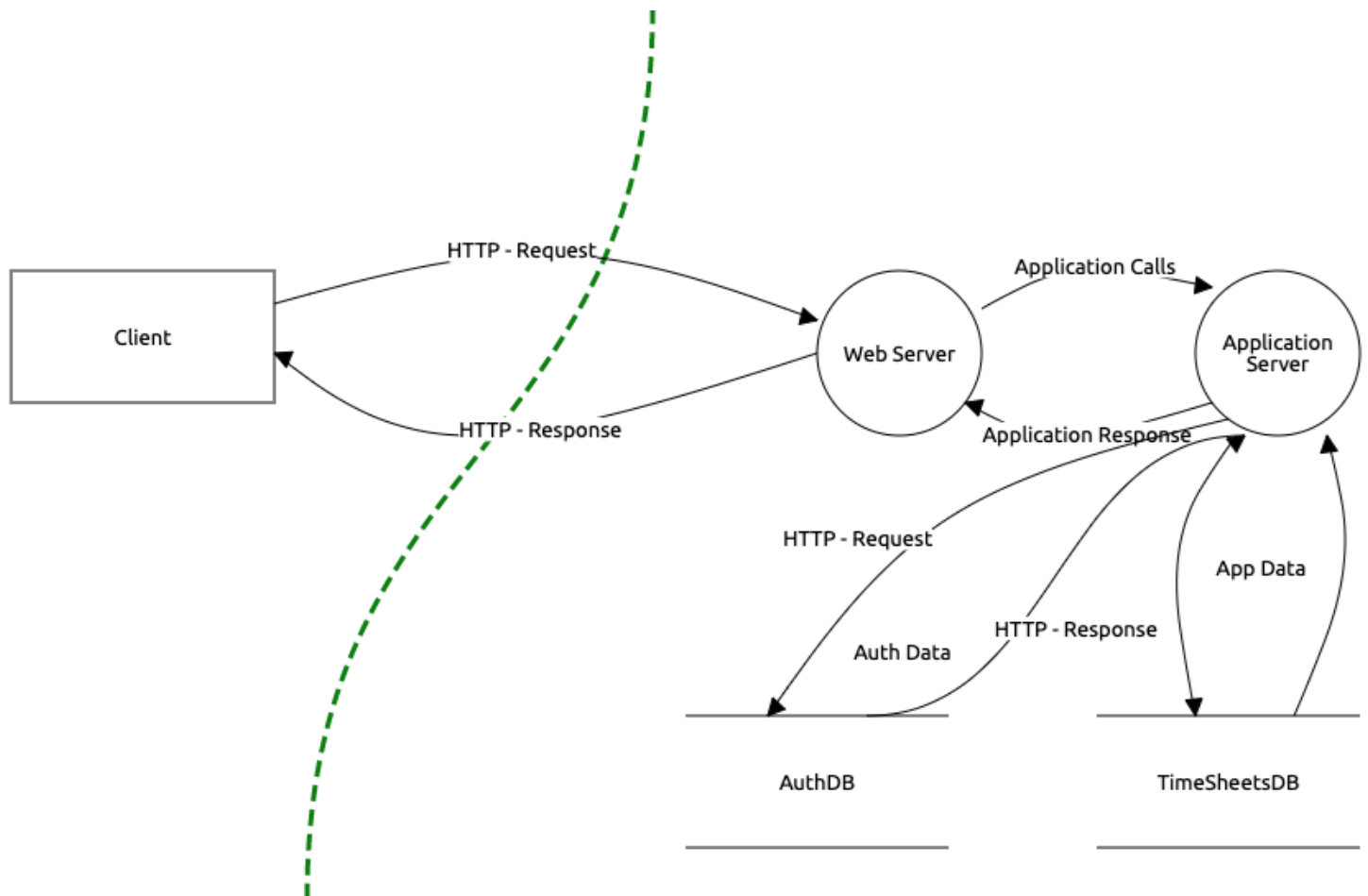
Request is generated from the client via the Internet. The request arrives at the TimeSheets web server which serves static content to the user (HTML, images, etc). Dynamic data is retrieved from the database and served to the client.

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 the threat model the SRE team confirmed that the database is on a server that does not have encryption at rest.

Why is this an issue?

[It's an issue because in any case an unauthorized access happened and the attacker getting access to these data , then he will gain these data .]

2.2 Authentication Data Stored Using Reversible Encryption

Discovery:

During the threat model the DBA team confirmed that the database is storing authentication data (credentials) encrypted.

Why is this an issue?

[Because when you encrypt your data in reversible way then you make your data at risk of compromise if the attacker obtain the secret key then he can decrypt the cipher text and get the plaintext .]

2.3 Authentication Requests are Unencrypted in Transit

Discovery:

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

Why is this an issue?

[Because these requests contain a credential data to authenticate so if these unencrypted requests have been intercepted by attacker, then you make these sensitive data at risk of losing it's confidentiality .]

2.DES Algorithm in Use

Discovery:

During the threat model the security team identified sensitive data being stored using the DES algorithm.

Why is this an issue?

[Using Data Encryption Standard (DES) algorithm could make these sensitive data at risk of being compromised using brute force mean break the encryption using all the possible keys and this kind of attack now become easy depending on the key length .]



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. *(Did you use a tool or defined risk scoring system?)*

I used the Risk Formula Methodology to Prioritizing the risks .

*Risk = Threat * Vulnerability * impact*

*Likelihood*impact*

Likelihood it's the threat times vulnerability

Risk	Likelihood	Impact	Priority	Justification
Unencrypted in Transit	High	High	High	This vulnerability is being active as the internal attacker can Man in the middle and read the original data that contain the authentication data in all communication between client and web server .
Outdated Algorithm	Medium	High	High	Using outdated encryption algorithm to encrypt sensitive data it's vulnerable method and it's make these data in risk of compromised , because recently can break these algorithms being easily with technology advance
Reversible Encryption	Low	High	Medium	Success this kind of exploitation is low because you need the secret key to attack and if the attack succussed the impact will be high as the data is sensitive .
Unencrypted at Rest	Low	Medium	Low	The chance of getting access to this data will be low as it's need to break all the defenses and it's impact is medium as the stored data it's not a sensitive data .



Section 4

Mitigation Plan

4.1 Employee Data Unencrypted at Rest

What is Your Recommended Mitigation Plan?

[The appropriate method to encrypt these data is using A symmetric encryption algorithm to encrypt the stored data in the database server and one of these symmetric algorithms is AES .]

Why Did you Recommend This Course of Action?

[Encryption that data at rest will make the access to the original data difficult and this will prevent losing the data confidentiality .And Because the symmetric encryption algorithm gives a fast and high secure method to protect data with less overhead and resources , so it's the appropriate method to encrypt . And for applying it can be done by encrypt the data using AES algorithm before it's stored in the database .]

4.2 Authentication Data Stored Using Reversible Encryption

What is Your Recommended Mitigation Plan?

[The appropriate method to store a sensitive data like the authentication data is using hashing algorithms such as SHA1 hash function . Before the data entered it will hash the authentication data as a hash values and store it in the Authentication Database .]

Why Did you Recommend This Course of Action?

[Hashing algorithm it's an irreversible encryption algorithm that mean it's a one way encryption so it can't be decrypted even if the hash values leaked still the attacker can't get the plaintext and since the stored data is a sensitive data then the the appropriate method is hashing .And we can hash the data using SHA1 hash function and store the hash values in the authentication database .]

4.3 Authentication Requests are Not Encrypted in Transit

What is Your Recommended Mitigation Plan?

[Encrypt the transmitted data must be considered to protect the data that transmit across the network from being intercept or sniffing from an attacker and we can replace the using of http protocol to the https protocol to transit data .]

Why Did you Recommend This Course of Action?

[Encryption the transmitted data will hide the plaintext from being compromised by the attacker and that can be achieved by using the https protocol and this protocol use a mathematical encryption algorithm to hide the original data that is being exchanged and this will protect data in transit .]

4.4 DES Algorithm in Use

What is Your Recommended Mitigation Plan?

[Encrypt a sensitive data with an outdated encryption algorithm makes these data vulnerable to compromised because the DES algorithm can be broken easily as a result of short key length and the appropriate encryption method by using AES encryption algorithm to encrypt these sensitive data .]

Why Did you Recommend This Course of Action?

[Encryption these sensitive data by Using the AES algorithm is a high secure method to protect data even against the brute force attack while the DES is vulnerable against these kind of attacks as a result of short key length , so using AES-128 to encrypt the data it's considered secure .]

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?

[

- Make sure that the A.10.1.1 Policy on the use of Cryptographic Controls from ISO27001 it's followed to apply a proper and effective use of cryptography to protect the confidentiality, integrity of information (1) .

-Work upon the NIST SP 800-175B Revision 1--Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms to stay in know about the best practices to protect data (2).

]

1- <https://www.isms.online/iso-27001/annex-a-10-cryptography/>

2- <https://csrc.nist.gov/publications/detail/sp/800-175b/rev-1/final>