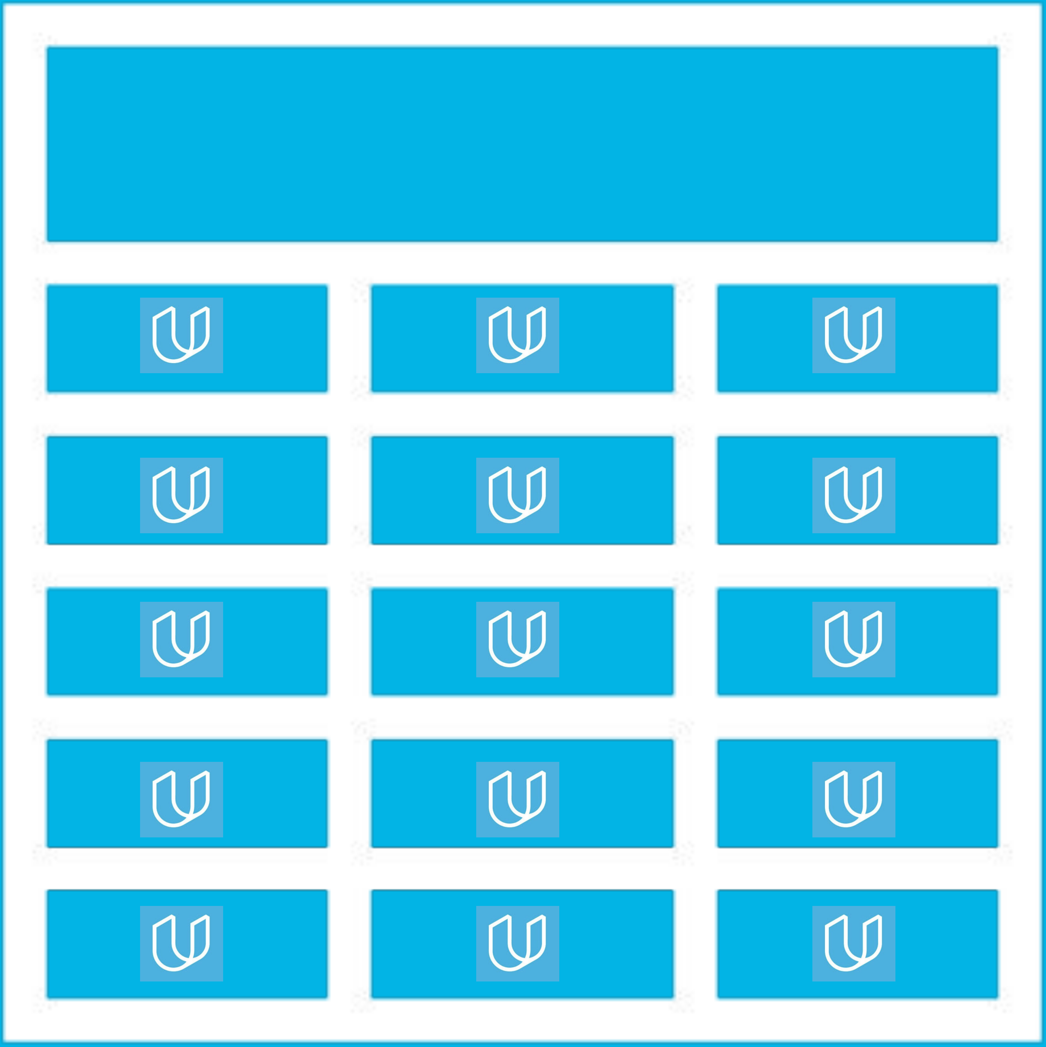
TimeSheets: Threat Report



Islam Alsaeed:

25/08/2022

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

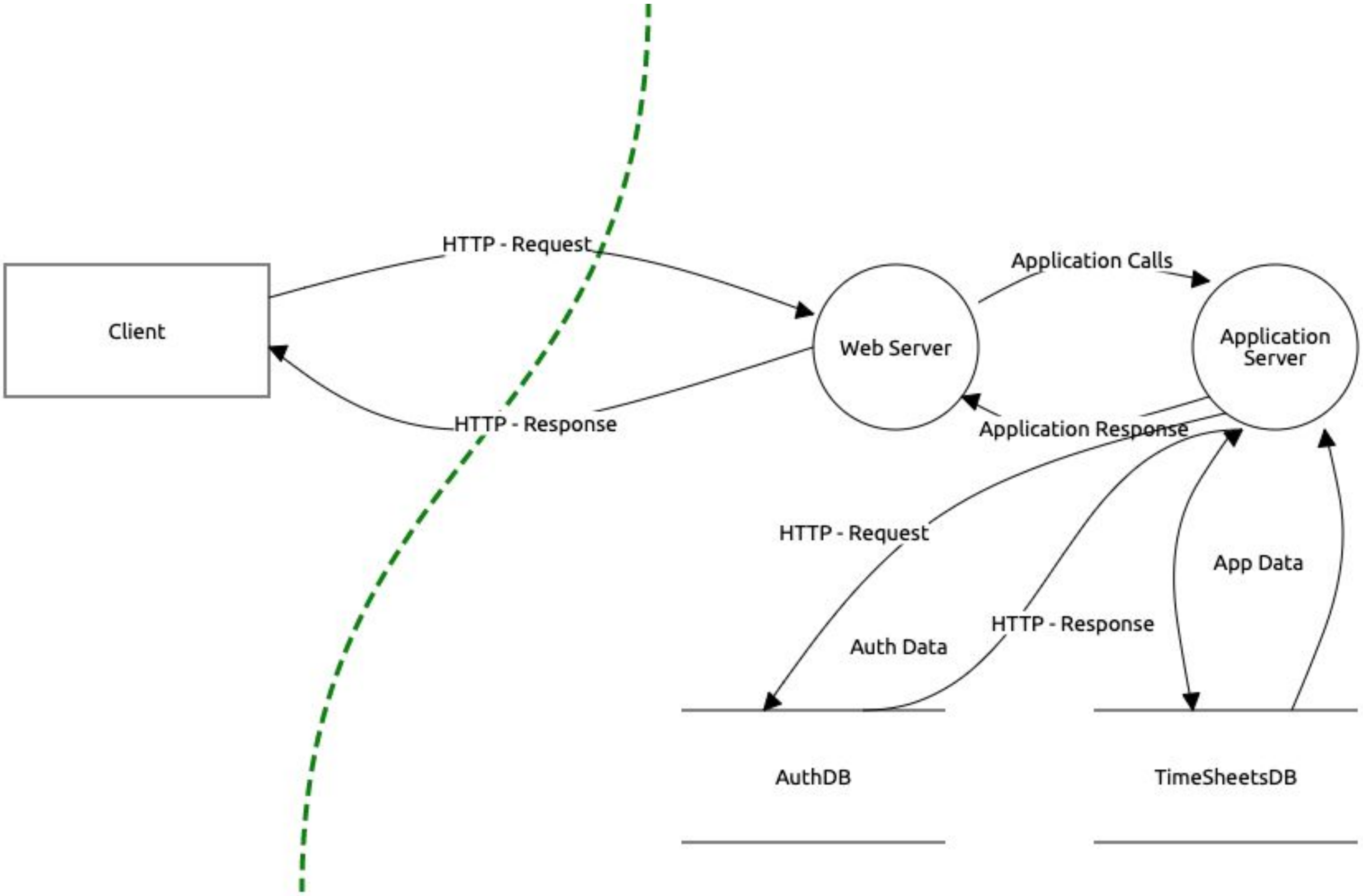
Request is generated from the client via the Internet. The request arrives at the TimeSheets web server which serves static content to the user (HTML, images, etc). Dynamic data is retrieved from the database and served to the client.

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?

Data must be encrypted to be protected from unauthorized access or viewed to a users whom should not see it

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?

It leaves these data under many threats one of them is brute force attack once the attacker finds the key he/she will have the ability to view all these encrypted data and can use them in the future to gain access.

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?

This will leaves them under threat of man in the middle attack either by only sniffing and spoofing or by forwarding the request and alter the information.

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?

DES is no longer a secure enough to be used for such data and these data are stored with this encryption will be under brute force attack threat.

Optional Task:

Examine the threat model diagram from Section 1 and answer:

What non-encryption issues can you identify?

- Filters and access controls

What recommendation would you give to solve those issues?

- **Implemtent filters and access controls**

Why do you recommend those solutions?

- *To ba able to controls the access*

- *Managing who can access what*

Section 3

Risk Analysis

3.1 Scoring Risks

Risk	**Score** ***(1 is most dangerous, 4 is least dangerous)***
Unencrypted at Rest	3
Reversible Encryption	4
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?)*

Risk= likelihood x impact

Vulnerability 1 : high impact and moderate likelihood thus ranked as 3
Vulnerability 2 : low impact and moderate likelihood thus ranked as 4
Vulnerability 3 : very high impact and high likelihood thus ranked as 1
Vulnerability 4 : high impact and high likelihood thus ranked as 2

Section 4

Mitigation Plan

4.1 Employee Data Unencrypted at Rest

What is Your Recommended Mitigation Plan?

- *Use a secure algorithms like AES*
- *Secure data in transit*

Why Did you Recommend This Course of Action?

To be able to protect data at rest because outdated algorithms like DES are vulnerable to brute force attack .

4.2 Authentication Data Stored Using Reversible Encryption

What is Your Recommended Mitigation Plan?

- *Use non reversible encryption algorithms Like:*
  hash and the way it works is each entry or data have a unique instant

Why Did you Recommend This Course of Action?

To make the data more secure under threats the exploit reversibility vulnerability.

4.3 Authentication Requests are Not Encrypted in Transit

What is Your Recommended Mitigation Plan?

- *Use an https request and response*
- *Encrypt the data before transit by a secure algorithm*

Why Did you Recommend This Course of Action?

For making the data more secure while transiting and be less vulnerable to attacks the exploits it.

4.4 DES Algorithm in Use

What is Your Recommended Mitigation Plan?

- *Use a more secure algorithm like AES*

Why Did you Recommend This Course of Action?

Using a secure algorithm and non outdated algorithms will make the data more protected and secured.

4.5 Security Audit

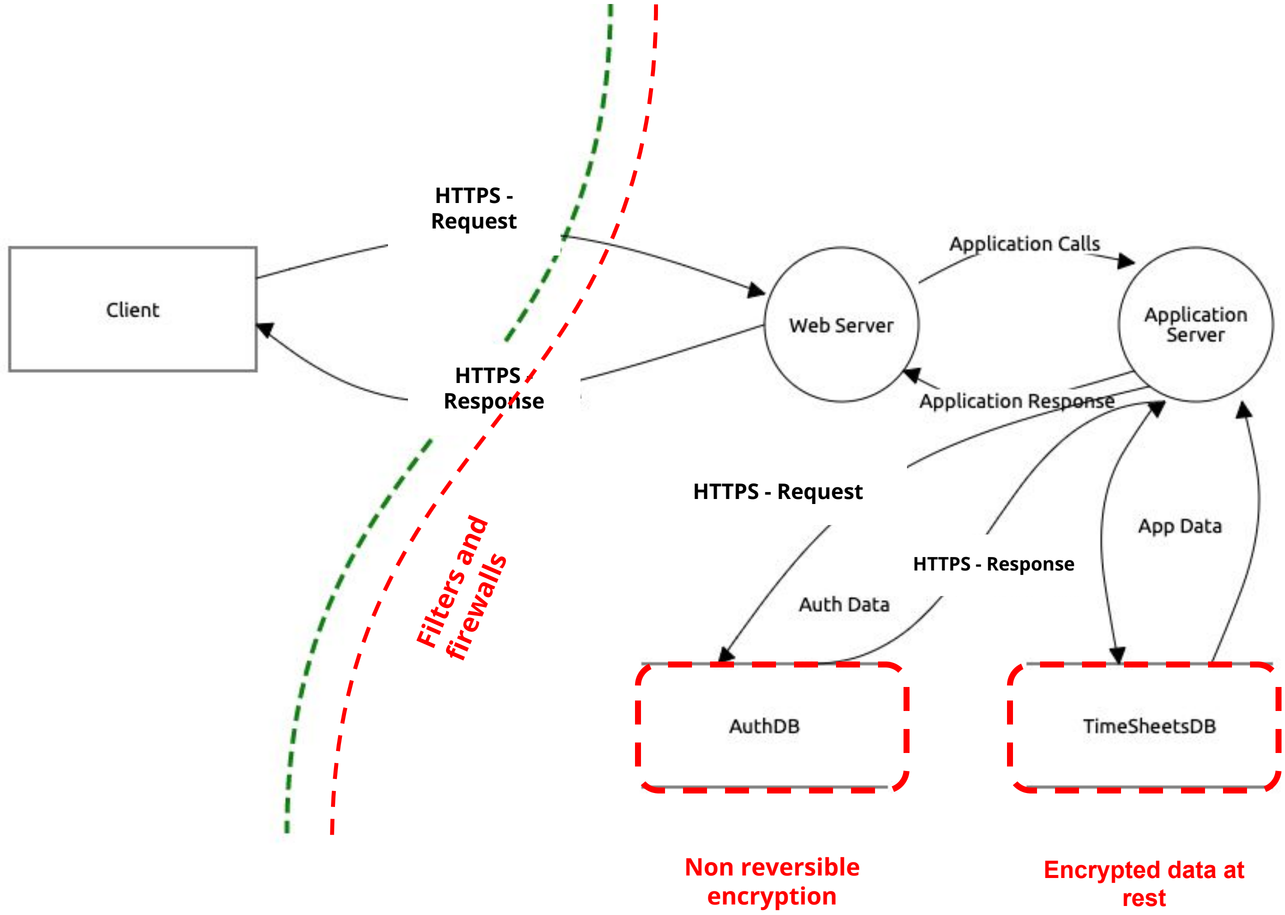
The audit team has been made aware of the systemic issue and wants to ensure your recommendations are followed. What steps can the audit team take?

- *sniff the data and implement man in the middle attack.*
- *penetrate the data at the database.*
- *Use brute force attack to detect if the outdated algorithms is still used.*
- *Policies forcing and creation*
- *Keys creation ,protection and sharing*

Optional Task:

Create an architecture diagram of a secure system.

Image of your secure architecture:



Optional Task *(Continued)*:

Additional Steps Would You Recommend to Prevent the Attack as well as Future Issues:

- Add a firewall
- Add filters