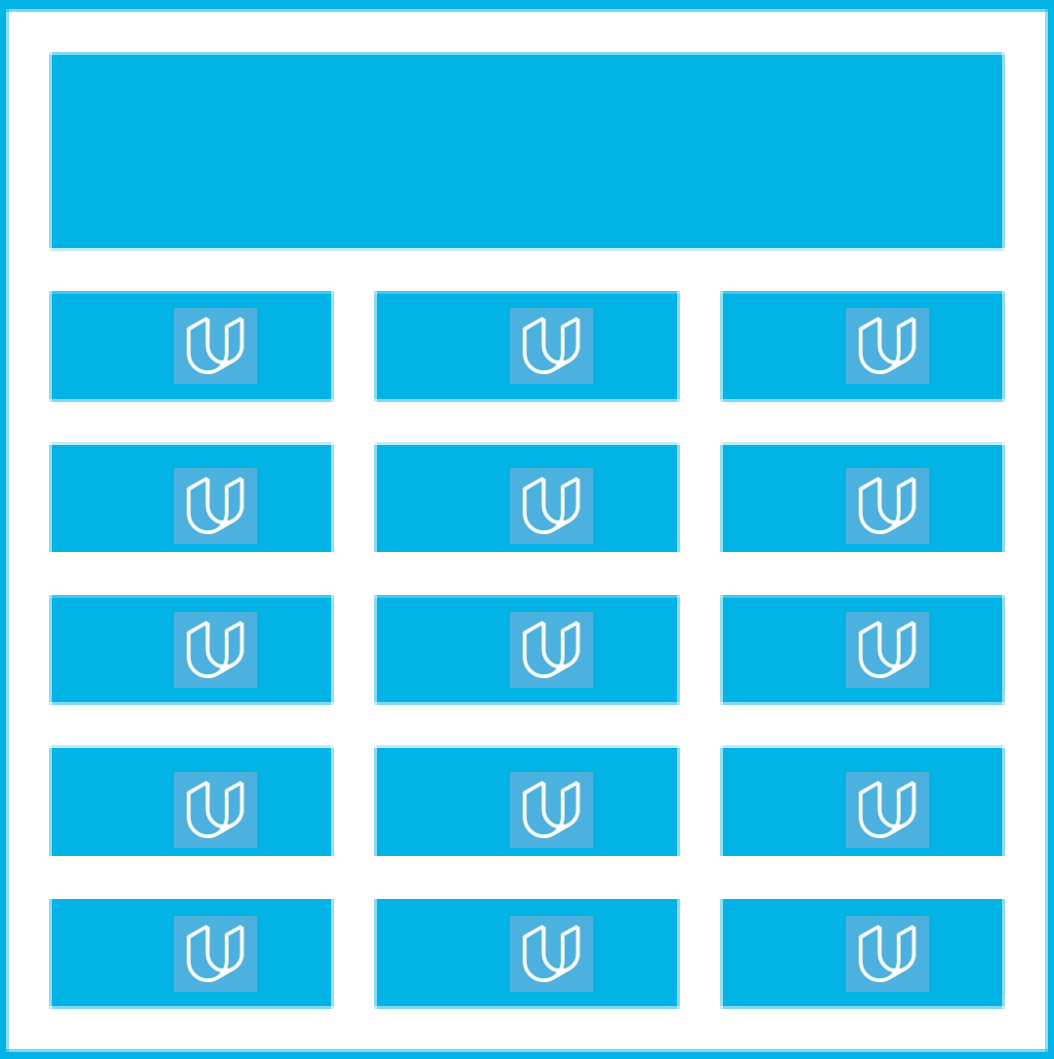
# TimeSheets :
# Threat Report



Omar Morsi

20/12/2022

# Section 1

## Initial Threat Assessment

# Completed Threat Analysis

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

The are a lot of attacks that may be caused by the login alert such as Phishing and man-in-the-middle attack

phishing: this is when a hacker sends as a trustworthy party sends you an email, hoping you will reveal your personal information voluntarily.

Man-in-the-middle (MitM): attacks are when a hacker sits in between two uncompromised systems or persons and deciphers the information they're sending to each other, including passwords.

**What Proves Your Theory?**

There is a deficiency in the encryption process, which made it easier for the hacker to phish and obtain information from both parties until he became in control of the data sent and received from both parties, and it became easy to catch information and passwords.

# Completed Threat Actor Analysis

**Who is the Most Likely Threat Actor?**

The internal user: because it is the main party that the phisher exploits to obtain information and passwords

**What Proves Your Theory?**

The phishing IP address matches that of an internal user

# 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?**

- This server may contain sensitive data (financial information, passwords) that the phisher may exploit in the attack process and exploit it to obtain customer and employee data and may access other servers connected to these employees.
- Unencrypted sensitive data leads to identity theft, phishing, and theft of financial resources from employees and clients

# 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 it is easy to break the reverse encryption by the hacker, so he can easily obtain this data, which may contain sensitive data, passwords, or financial transactions. Therefore, it is necessary to use hard-to-break encryption algorithms to protect that data.

# 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 is a serious problem because not encrypting the data during transmission enables an intruder to capture it and see what is inside it, and this data may contain financial information, passwords, or sensitive information, and this causes damage. This must encrypt the data during transmission, and there are two ways to encrypt the data, symmetric encryption, and asymmetric encryption.*

*Symmetric encryption: use one key that is the same key is used for both encryption and decryption*

*Asymmetric encryption: use two keys one for encryption and a different one for decryption.*

# 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?**

Because it has a 56-bit key so it is possible to brute-force is a big problem and works slowly AES may be best because the key size can be 128 bits so brute-force is hard.

# 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?**

- Not encrypting data is a serious problem because the data will become readable, so any third party can read this data, and this data may contain highly sensitive information, customer information, or financial data. It is necessary to encrypt the data if it is to be transmitted over the Internet, but if this data does not contain important information, or it was to be transmitted internally, it may not be encrypted
- I highly recommend encrypting data if it is sent over the Internet or if it contains sensitive data, customer data, or passwords.
- So that a phisher does not seize this data

# Section 3

Risk Analysis

# 3.1 Scoring Risks

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

# 3.2 Risk Rationale

**Why Did You Choose That Ranking? Make sure to include your risk ranking methodology.**

- Unencrypted at Rest: The data may be transmitted internally and may not contain highly sensitive data or contain important information.

Risk = Threat x Vulnerability x Impact = low * medium * low = low

Reversible Encryption :Reverse encryption is easy to break encryption by a phisher and obtain information that may carry highly sensitive data. Therefore, you must stop using reverse encryption, especially in the case of transmission over the Internet, or if the data contains highly sensitive information.
Risk = Threat x Vulnerability x Impact = high * high * high = high

- Unencrypted in Transit :Not encrypting data during transmission is a serious problem because it carries the risk of phishing by the hacker and makes it easier for him to obtain that unencrypted information, which may contain financial data, passwords, or customer data. Therefore, data must be encrypted during transfers by strong algorithms to make it difficult for the hacker to crack the code.

Risk = Threat x Vulnerability x Impact = high * high * high = high

- *Outdated Algorithm :It is very important not to use old algorithms because they make it easier for the hacker to break their encryption, because with technological progress, tools appear that make it easier to break those old algorithms, and therefore strong new algorithms must always be followed up and used in encryption, especially the very important data.*
  *Risk = Threat x Vulnerability x Impact = high * high * medium = medium*

# Section 4

## Mitigation Plan

# 4.1 Employee Data Unencrypted at Rest

**What is Your Recommended Mitigation Plan?**

It's important to make sure you're using the strong encryption strategy!

So I recommended to encrypted sensitive data using
symmetric : Symmetric encryption uses a single key to encrypt and decrypt
or asymmetric encryption : use two key one for encryption and different one for decryption
or any robust algorithm such as 128 or 256-bit AES keys which is difficult to undecrypt it.

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

To save sensitive data from any threat or phishing or attack from any hackers (man in the middle),without non-encryption, anyone can access the data and manipulate it, Because the cipher is the procedure one must follow in order to convert the data from plaintext to ciphertext.

# 4.2 Authentication Data Stored Using Reversible Encryption

### What is Your Recommended Mitigation Plan?

I recommend stopping the using Reversible Encryption in authentication because encryption is reversible and using hashing because encryption is a two-way reversible process, but Hashing is one-way or irreversible there are a lot of hashing algorithms such as MD5 that generate an almost unique 128-bit hash value or using SHA-256 that generate an almost-unique 256-bit

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

Using Reversible Encryption to store authentication data is not secure because any attacker can decrypt because it is a two-way reversible process but hashing is one-way or irreversible so it is difficult to decrypt it.

# 4.3 Authentication Requests are Not Encrypted in Transit

**What is Your Recommended Mitigation Plan?**

*I recommend encrypting data in transitusing hashing because Hashing is one-way or irreversible there are a lot of hashing algorithms if the data is very sensitive must use strong algorithms such as MD5 or 256 SHA as MD5 that generates an almost unique 128-bit hash value or using SHA-256 that generates an almost-unique 256-bit or using SSL, LTS*

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

*because the unencrypted data allows the third party to access it, such that the man in the middle can phish these unencrypted data which may contain sensitive data, passwords, or financial information, it is very important to encrypt the data, especially which contains sensitive information or using SSL, LTS that is widely used protocol for establishing encryption communication between system.*

# 4.4 DES Algorithm in Use

**What is Your Recommended Mitigation Plan?**

I recommend using hashing Algorithm or using encryption, hashing, signing, certificates but encryption is a two-way reversible process, so it is easy to decrypt it, but Hashing is one-way or irreversible so it is difficult to decrypt it, there are a lot of hashing algorithms such as SHA-256 that generate an almost-unique 256-bit.

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

I recommend using AES because it uses a 128-bit key size so it is difficult to brute-force this key or using hashing algorithm such as SHA-256 that generate an almost-unique 256-bit

But the DES algorithm uses a 56-bit key so is too short. it is easy to brute-force this key.

# 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 audit will take action from them preventive control, detective control, and corrective control
- Policies : it is a high-level document that States what can and cannot be done. The document may provide for forcing users to use passwords that must be committed to the requirements of complexity with its change every period and that period is specified in that document.
- preventive control: a security measure to prevent an event from occurring
- detective control: are measure to alert on an event or incident
- corrective control: any measure taken to repair damage and to correct errors that have been detected.