وزارة التربية والتعليم العالي
والبحث العلمي
الجامعة الإماراتية الدولية
كلية الهندسة وتكنولوجيا المعلومات

# تصميم نظام أمن للبلاغات الأمنية

## Designing a Secure Security Reporting System

## "DSSRS"

**إعداد:**

| | |
|---|---|
| أسامة أنور علي الشلالي | 2021030324 |
| أحمد عبد العليم عبدالحميد الاصبحي | 2021030802 |
| هيثم حسان علي الشامي | 2021030674 |
| آلاء علي حميد أحمد الوصابي | 2021030749 |
| ربى فهمي عبدالله الكميم | 2021030795 |

**المشرف:**

أ. م. د. جميل راشد

**المشرف المساعد:**

م. محمد العشملي

**تقرير مشروع التخرج المقدم لقسم أمن المعلومات كجزء من متطلبات الحصول على درجة البكالوريوس في أمن المعلومات.**

**1446-2025هـ**

## ملخص المشروع

نظام البلاغات متقدم يهدف إلى تعزيز القدرات الأمنية للأجهزة الأمنية وتسهيل عملها في القبض على المجرمين والهاربين من العدالة واستعادة الممتلكات والمسروقات. يعتمد النظام على تلقي بلاغات من المواطنين واستخدام التكنولوجيا الحديثة لتعميم هذه البلاغات وربط وزارة الداخلية بوزارة العدل، مما يساعد في تعزيز التعاون وسرعة التعميم للأوامر القهرية والأحكام التنفيذية ضد المجرمين والهاربين من العدالة.

يتم تلقي البلاغات عبر الرقم الوطني للبطاقة الشخصية والأرقام التسلسلية للأجهزة الإلكترونية والأسلحة ، وتعمم هذه البلاغات إلى الأجهزة الأمنية ونقاط التفتيش ونقاط البيع التجارية في انحاء الجمهورية. الاستعلام يتم عن طريق النظام لمعرفة إن كان المباع من المسروقات المبلغ عنها. يساعد هذا النهج في تسهيل عمليات القبض على المجرمين، يتيح هذا للتجار التحقق من صحة المسروقات والأجهزة قبل الشراء وتجنب شراء المسروقات والتبليغ عن حامل المسروق، مما يساهم في الحد من السرقة واستعادة المسروقات.

كذلك لوحة التحكم الأمنية بالنظام تمثل ميزة رئيسية تتيح للنظام التكامل مع نفسه والتحكم بكل خصائصه ومنح الصلاحيات وإدارة أنظمة الحماية المبرمجة ضمن النظام وذلك للتأكد من التكامل في الحماية من الهجمات السيبرانية، حيث تحتوي على أدوات أمنية متخصصة للحماية من الاختراق والهجمات السيبرانية. وتحليل سلوكيات النظام والتنبؤ بالمخاطر المحتملة، يتم استخدام تقنيات متقدمة لتأمين قواعد البيانات. كما يتضمن النظام خطة أمنية شاملة لمنع الوصول غير المصرح به وحماية البيانات الحساسة، مما يعزز من أمان النظام وفعاليته في التصدي للتهديدات.

# Project Summary

The reporting system is an advanced platform designed to enhance the security capabilities of law enforcement agencies and facilitate their efforts in apprehending criminals, fugitives from justice, and recovering stolen property. The system relies on receiving reports from citizens and utilizing modern technology to broadcast these reports and connect the Ministry of Interior with the Ministry of Justice, thereby promoting cooperation and enabling the rapid dissemination of enforcement orders and judicial rulings against criminals and fugitives.

Reports are submitted using the national ID number and the serial numbers of electronic devices and weapons. These reports are then circulated to security agencies, checkpoints, and commercial points of sale across the country. The system enables inquiries to verify whether an item being sold is among the reported stolen goods. This approach facilitates the arrest of criminals and allows merchants to verify the legitimacy of goods before purchase, helping them avoid buying stolen property and report anyone in possession of stolen items. This contributes to reducing theft and aiding in the recovery of stolen goods.

Additionally, the system's security control panel is a key feature that allows full integration and management of its functions, including access permissions and control over the built-in security systems. This ensures protection against cyberattacks through specialized security tools for intrusion prevention and behavior analysis to predict potential risks. Advanced technologies are used to secure databases, and the system includes a comprehensive security plan to prevent unauthorized access and protect sensitive data, thereby enhancing the system's safety and effectiveness in countering threats.

# تفويض

نفـــوض الجامعـــة الإماراتيـــة الدوليـــة كليـــة الهندســـة وتكنلوجيـــا المعلومـــات بتزويـــد نســـخ مشـــروع التخـــرج للمكتبـــات أو المنظمـــات أو الأفـــراد عنـــد الطلب من الكلية .كما يسمح باستخدامه في المسابقات الدولية والمحلية .

| أسم الطالب | التوقيع | التاريخ |
|---|---|---|
| أسامة أنور علي الشلالي | | |
| أحمد عبدالعليم الاصبحي | | |
| هيثم حسان الشامي | | |
| آلاء علي حميد الوصابي | | |
| ربى فهمي الكميم | | |

# 2

**:7**

﴿ قَالَ الَّذِي عِندَهُ عِلْمٌ مِّنَ الْكِتَابِ أَنَا آتِيكَ بِهِ قَبْلَ أَن يَرْتَدَّ إِلَيْكَ طَرْفُكَ ﴾

سورة النمل [الآية 40]

# الإهداء

**بكل فخر واعتزاز، أهدي هذا العمل المتواضع إلى من كان لهم الفضل الأكبر في صناعته. إلى والديّ اللذين كانا لي ملاذًا آمنًا ومصدر قوة وقدوة، شكرًا لكم على دعمكم اللامحدود وتضحياتكم التي لا تُقدَّر بثمن. إلى إخوتي الأعزاء، أصدقائي في الحياة، شكرًا لكم على وجودكم الدائم بجانبي وعلى تشجيعكم المستمر. وإلى أساتذتي الأفاضل، الذين أفنوا أعمارهم في نشر العلم والمعرفة، شكرًا لكم على كل ما قدمتموه لي من علمٍ وخبرة. لا يسعني إلا أن أتوجه بخالص الشكر والعرفان لكل من ساهم في إنجاز هذا المشروع، فأنتم جميعًا جزء لا يتجزأ من نجاحي.**

# الشكر والتقدير

**نتوجه بخالص الشكر لله سبحانه وتعالى، الذي منحنا القوة والتوجيه لإكمال هذا المشروع، نود أن نعرب عن خالص شكرنا وتقديرنا لمشرف مشروعنا د.جميل راشد و م.محمد العشملي على جهودهما المبذولة في سبيل إثراء معرفتنا بخبراتهم القيمة. إن مساهمتهما الفعالة في هذا المشروع قد تركت أثراً بالغاً في نفوسنا، وسوف نظل ممتنين لهما على الدعم والتشجيع المستمر؛ بفضل توجيهاتكم القيمة، تمكنا من تحقيق نتائج مبهرة في هذا المشروع. ولجميع الدكاترة والمدرسين الذين قدموا معرفتهم وخبرتهم لمساعدتنا في هذا العمل وعلى رأسهم د.خالد البريهي، فقد كان أساس ونقطة بداية المشروع. إننا مقتنعون بأن هذا المشروع لن يكون على ما هو عليه لولا دعمه المستمر ونصحه وتشجيعه الدائم.كذلك نتوجه بالشكر والتقدير للدكتور مالك الجبري، ود.هشام عقلان،و د.محمد الخولاني،و م.مجد عزالدين ،وأ.زيد الوشلي ،وأ.أحلام الهمداني، وأ.نجوى عامر، وأ.فتحي سلمان على توجيههم لنا ونصائحهم القيمة.كما نتوجه بجزيل الشكر والتقدير لأ. علياء العرسي على تعاونها الكريم وجهودها المشكورة التي كان لها أثر طيب في مسيرة إنجاز هذا المشروع.لقد كانت هذه التجربة مليئة بالتحديات والفرص للنمو، ولكن بفضل دعمكم وتوجيهكم، تمكنا من تجاوز التحديات وتحقيق النجاح. نشكركم جميعاً على المساهمة القيمة والمساعدة التي قدمتموها. ندعوا الله أن يجزيكم خير الجزاء ويبارك فيكم دائماً. شكراً لكم جميعاً على تعاونكم ودعمكم اللامحدود.**

# إقرار المشرف

نحن نشـهد بأن إعداد هذا المشـروع المعنون بـــــ **"نظام البلاغات الأمني"** المعد من قبل الطلاب أمن المعلومات:

أسامة أنور الشلالي - أحمد عبدالعليم الاصبحي - هيثم حسان الشامي - آلاء علي حميد أحمد الوصابي

– ربى فهمي الكميم ؛ تم تحت إشرافي كوثيقة مشروع تخرج مقدمة إلى قسم أمن المعلومات إستكمالاً لمتطلبات درجة البكالوريوس في 2024 – 2025.

**اسم المشرف:** أ. م. د. جميل راشد

**التوقيع :**

**التاريخ:**

**عنوان المشروع : تصميم نظام أمن للبلاغات الأمنية**

## المشرف

| م | أسم | | التوقيع |
|---|---|---|---|
| 1 | | | |

## لجنة المناقشين

| م | أسم | | التوقيع |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |

**رئيس القسم**

.....

# المحتويات

# فهرس الأشكال

## فهرس الجداول

# الفصل الأول:المقدمة

## 1.1 مقدمة

تُعدّ الجرائم والجنايات من أكبر التحديات التي تواجه المجتمعات في هذا العصر، حيث نعيش في مجتمع يتميز بسرعة التطور التكنولوجي وعالم مليء بالجرائم. مع زيادة الوعي، يتطلع الناس إلى أن يتم الاستجابة لمشاكلهم وشكواهم بشكل أسرع. لذلك، لابد من بناء نظام بلاغات قوي يتميز بالأمن ويساهم في تنظيم البلاغات ليتم اتخاذ الإجراءات والقبض على المجرمين.

الغرض من نظام البلاغات هو أن يكون وسيلة رادعة للمجرمين. فعندما يعلم المجرم أن هناك نظامًا فعالًا لتلقي البلاغات والتحقيق فيها، يتردد في القيام بأفعال إجرامية. فإذا كان يعلم أن أعماله ستتم ملاحقتها ومحاسبتها، فإن ذلك يقلل من ارتكاب المزيد من الجرائم ويحد من الإفلات من يد القانون والانتهاكات المحتمل حدوثها في المستقبل. يتم استقبال البلاغات وتعميمها إلى النقاط الأمنية ونقاط البيع التجارية. كذلك، يركز النظام على بلاغات الأجهزة المسروقة والأسلحة، حيث يساعد في استقبال بلاغات الأجهزة المسروقة (من خلال الرقم التسلسلي للجهاز) والأسلحة (من خلال الرقم التسلسلي)، ومشاركة هذه المعلومات مع المحلات التجارية؛ للحد من انتشار السرقات وتعزيز الأمن في المجتمع.

يساهم نظام البلاغات بشكل كبير في مساعدة وزارة الداخلية ووزارة العدل وإدارات الأمن وأقسام الشرطة من حيث تسجيل وتوثيق جميع التفاصيل المتعلقة بالبلاغات، مما يعمل على تحسين إدارة البيانات. يتم تسجيل تفاصيل الجريمة، مثل المكان والزمان والأشخاص المعنيين والشهود.

يساعد النظام على الاستجابة السريعة للبلاغات من قبل الجهات المعنية. عندما يتم تلقي بلاغ جديد، يمكن للأجهزة الأمنية تقييم الأولويات وتحديد الموارد المطلوبة للتعامل مع الحالة بشكل فوري وبصورة مستعجلة. يعمل نظام البلاغات على تسهيل التواصل والتنسيق الداخلي بين مختلف وحدات الأجهزة الأمنية. يُعدّ نظام البلاغات أداة قوية لتحسين أداء الأجهزة الأمنية.

## 1.2 الدوافع والمساهمة

إن الدافع وراء إختيار نظام البلاغات هو إيمانًا منا بأهمية خدمة المجتمع الذي يفتقر إلى نظام بلاغات فعال وذلك لتعزيز الأمن في المجتمع. حيث نسعى من خلاله إلى دعم الجهات المعنية في مكافحة الجريمة والحد من وقوع السرقات وإعادة الممتلكات لأصحابها ، وذلك بتسريع عملية القبض على المجرمين واستعادة الممتلكات المسروقة.

## 1.3 بيان المشكلة

عندما يعتمد نظام العمل في الجهات الأمنية على الطريقة التقليدية لتسجيل وتوثيق البلاغات وتعميمها، قد يواجه النظام عددًا من المشاكل:

1. التسجيل اليدوي للبلاغات.
2. بطئ الإجراءات وتعامل مع البلاغات.
3. صعوبة العودة للبلاغات السابقة .
4. صعوبة تبادل المعلومات بين الأقسام المختصة .
5. إحتمالية وجود أخطاء في التسجيل اليدوي .
6. صعوبة إستعادة المسروقات وتتبعها.

## 1.4 الأهداف والغايات

الهدف الرئيسي من تصميم النظام هو خدمة المجتمع والسعي لتحويل العلم إلى واقع ملموس للحد من الجريمة والسرقات وتسهيل عمل الجهات الأمنية ليتم الإبلاغ عن المشاكل والقضايا التي يشهدها المجتمع بسهولة والتعامل معها واتخاذ الإجراءات اللازمة. إضافة الى جعل النظام يتسم بالأمن والسرية و الخصوصية والعمل على سد الثغرات في النظام وجعله صعب الاختراق وقوي ضد الهجمات كما أن للنظام أهداف فرعية كما يلي:

1. توفير واجهة سهلة الاستخدام لمستخدمي النظام وأصحاب المحلات التجارية تسمح لهم بالبحث في قاعدة البيانات عن أجهزة مسروقة قبل شرائها، مما يساهم في تقليل تداول الأجهزة المسروقة في السوق.
2. سرعة التنفيذ والتعامل مع البلاغات.
3. إمكانية العودة للبلاغات السابقة ومتابعتها.
4. تسهيل الرجوع للبيانات في قاعدة البيانات الموحدة وتواصل بين الجهات المختصة.
5. الحفاظ على البيانات أمنة حيث يهدف النظام إلى تطبيق إجراءات أمنية موثوقة لحماية بيانات البلاغات والمعلومات الحساسة.
6. الحصول على تقنية تسهل ملاحقة ومتابعة المسروقات وإعادتها إلى أصحابها.

## 1.5 تعريف النظام

هو نظام "تطبيق ويب" لتسهيل وتنظيم عملية تلقي ومعالجة البلاغات والشكاوى وربط وزارة الداخلية بوزارة العدل حيث يتم إستخدام هذا النظام في مختلف المجالات مثل الأمن العام وتنفيذ الأحكام ضد المتهمين و يتضمن نظام البلاغات عادة مجموعة من الخصائص والمميزات مثل توثيق البلاغات، وتسجيل تفاصيل البلاغ وتعميمها لتحسين جودة الخدمات والسلامة العامة وأيضا يتسم النظام بالأمنية وتصديه لإستغلال الثغرات عن طريقة لوحة تحكم أمنية شاملة لمجموعة من الأدوات المدمجة مع النظام وخطته وتصميمه الذي تم بوضع إعتبار لكل ما يمكن أن يكون ثغرة في النظام.

## 1.6 معوقات النظام

**قلة الموارد والتمويل**

يمكن أن يعاني نظام البلاغات من قلة الموارد أو عدم استقرار الخوادم، مما يؤثر على قدرة المستخدمين على تقديم البلاغات ومتابعة المشكلات واتخاذ الإجراءات اللازمة

**عدم توفر أدوات لتحقق من مصداقية البلاغات**

يمكن أن يتعرض النظام لمشكلة تقديم بلاغات كاذبة أو مضللة، مما يؤدي إلى تضييع الجهود والموارد في التعامل مع هذه البلاغات غير الصحيحة.

**التكلفة في ربط النظام بالأقسام المختلفة** .

## 1.7 فرضيات النظام

- يفترض أن يكون نظام البلاغات سهل الإستخدام وبديهيًا، حتى يتمكن المستخدمون من تقديم البلاغات بسهولة ويسر.

- يفترض أن تتم معالجة البلاغات بشكل سريع وفعال من قبل الجهات المعنية؛ يجب توفير آليات فعالة لتوجيه البلاغات ومتابعة حالتها وإتخاذ الإجراءات اللازمة لحل المشكلة.

- يفترض أن يتم توفير البنية التحتية اللازمة لدعم نظام البلاغات، بما في ذلك الخوادم والشبكات والبرمجيات؛ يجب أن تكون هناك استثمارات في تحديث وتطوير البنية التحتية لضمان استقرار وفعالية النظام.

- يفترض تنفيذ سياسات صارمة للوصول والتحكم في نظام البلاغات. ينبغي تحديد الأذونات والصلاحيات بدقة وتقديم الوصول إلى المعلومات والوظائف المناسبة لكل مستخدم وفقًا لمسؤولياتهم. يجب أن يكون هناك أيضًا نظام لتتبع وتسجيل الأنشطة والتحقق من الدخول غير المصرح به.

- يفترض توفير التدريب المناسب للموظفين حول ممارسات الأمان والسلامة السيبرانية؛ يجب توعية المستخدمين بشأن التهديدات الأمنية المحتملة مثل هجمات الاحتيال الإلكتروني والتصيّد الاحتيالي وكيفية التعامل معها بشكل صحيح.

- يفترض حماية النظام وقواعد البيانات التي تحتوي على معلومات البلاغات بواسطة تشفير البيانات وتنفيذ آليات الوصول المحدودة. ينبغي تطبيق سياسات النسخ الاحتياطي المنتظمة للحفاظ على سلامة البيانات واستعادتها في حالة حدوث خرق أمني.

- يفترض رصد الأنشطة غير المشروعة عبر لوحة التحكم الأمنية المتواجدة في النظام؛ وينبغي تنفيذ أنظمة رصد الأمان والتحليل السلوكي للكشف عن أنشطة غير مشروعة أو مشبوهة. يجب استخدام تقنيات مثل تحليل السجلات ورصد الشبكة للكشف المبكر عن أي محاولة للاختراق أو استغلال الثغرات.

## 1.8 نطاق النظام

- وزارة العدل.
- وزارة الداخلية.
- إدارات الأمن.
- اقسام الشرطة.
- النقاط الامنية.
- المحلات والمعارض التجارية .

## 1.9 منهجية العمل

نظراً للمنهجيات المتعددة وبعد دراستنا للمنهجيات، تم اختيار منهجية(*Spiral*) ؛ تم إختيار هذه المنهجية لأن النظام واضح المتطلبات والأهداف من البداية، وكذلك لما تمتلكه المنهجية من مميزات. حيث تعتمد منهجية (*Spiral*) على التكرار والتحسين المستمر، وتسمح بالتعلم من الأخطاء والتكيف مع التغيرات. تعتبر هذه المميزات مهمة في تطوير البرمجيات.

تعتبر منهجية (*Spiral*) مرنة وتسمح بتعديل الخطط والمخرجات بناءً على الأخطاء المكتشفة خلال العملية. يتم تحليل الأخطاء وتحديد الأسباب الجذرية وإتخاذ إجراءات لتجنب تكرارها في المستقبل.

يتم إستخدام هذا النموذج في هندسة البرمجيات عندما يكون المشروع كبيرًا وعندما يكون تقييم المخاطر والتكاليف مهمًا.

## 1.10 الاعمال ذات صلة

**تكامل نظام البلاغات مع الأنظمة يعزز الكفاءة في تلقي ومعالجة البلاغات وتحقيق أهداف الجهات الأمنية بشكل أفضل وأوسع .**

- **<u>نظام الأحوال المدنية</u>**

يتيح ذلك توفير معلومات شخصية دقيقة ومحدثة للمستخدمين وتسهيل عملية التحقق من هويتهم وتحديد هوية المبلّغين والمشتبه بهم أيضاً.

- **<u>نظام التتبع الجنائي الرقمي</u>**

يتيح هذا النظام تكامل التحليل وربط البيانات المتعلقة بالبلاغات والتحقيقات الجنائية، وبالتالي تحسين قدرة الجهات الأمنية على معالجة البلاغات بشكل فعال وإتخاذ إجراءات تحقيقية.

- **<u>نظام مراقبة الكاميرات</u>**

يمكن أن يسهم تكامل نظام مراقبة الكاميرات مع نظام البلاغات في توفير مصادر إضافية للمعلومات والأدلة. يمكن استخدام مقاطع الفيديو المسجلة من كاميرات المراقبة في تحليل الحوادث وتحديد المشتبه بهم وتوثيق الأحداث.

- **نظام الاتصالات**

يعتبر التكامل مع نظام شركات الإتصالات المحلية أحد العوامل الحيوية لنجاح نظام البلاغات. يمكن إستخدام الهواتف النقالة وخدمه التتبع ومراقبة المواقع وإتصالات المشتبهين والبريد الإلكتروني والأنظمة الأخرى لتحقيق ذلك.

## 1.11 تنظيم المشروع

- **الفصل الأول، المقدمة:** مقدمة عامة عن نظام البلاغات، وبيان المشكلة، ولماذا تعتبر أسئلتنا جديرة بالاهتمام، وماذا سيكون غلاف النتائج.

- **الفصل الثاني، الخلفية النظرية والدراسات السابقة :** قسم موجز يقدم المعلومات الأساسية الضرورية حول مجال بحثنا ودراستنا؛ وخاصة ما تم القيام به من قبل من دراسات في نظام البلاغات.

- **الفصل الثالث، دراسة الجدوى والتحليل:** يقدم العمل التجريبي التفصيلي، والمتطلبات وجمع البيانات وتصميم النظام، وتنفيذ تصميم في نظام البلاغات.

- **الفصل الرابع، التصميم**: يتناول هذا الفصل تصميم واجهات النظام ومكوناتها، مع توضيح كيفية تفاعل المستخدم مع النظام.

- **الفصل الخامس، التنفيذ والإختبار:** يستعرض هذا الفصل آلية تنفيذ النظام وفقًا للتصميم المعتمد، ويشمل الأدوات واللغات المستخدمة في البرمجة. كما يتناول خطوات اختبار النظام للتحقق من صحة الوظائف، واكتشاف الأخطاء وتصحيحها، بما يضمن عمل النظام بكفاءة وموثوقية.

- **الفصل السادس، الخاتمة:** يعرض ما تعلمناه، هل حققنا أهادفنا، ما هي المقترحات حول مجال البحث، ما الذي لم نتطرق إليه في مجال البحث؟

# الفصل الثاني : الخلفية النظرية والدراسات السابقة

## 2.1 نبذة تاريخية

نظم البلاغات هي أنظمة تهدف إلى تلقي ومعالجة البلاغات من قبل خدمة الجمهور وتوجيهها إلى الجهات المعنية لاتخاذ الإجراءات اللازمة. تطورت هذه الأنظمة على مر الزمن وشهدت تحسينات تقنية وتطويرات لتلبية احتياجات المجتمع وتحسين التواصل بين الجمهور والسلطات المعنية.

في السابق، كانت أنظمة البلاغات تعتمد بشكل رئيسي على الوسائل التقليدية للتواصل مثل الهواتف والبريد الورقي.

كانت البلاغات تُقدم عن طريق الاتصالات بمراكز الطوارئ أو مكاتب الشرطة المحلية. وتتطلب هذه العملية وقتًا طويلا وجهودًا يدوية لتوجيه البلاغات الصحيحة إلى الجهات المعنية .مع التطور التكنولوجي، ظهرت أنظمة البلاغات الإلكترونية.

بدأت الحكومات والجهات الأمنية في تطوير أنظمة إلكترونية تسمح للجمهور بتقديم البلاغات والشكاوى. تمكنت هذه الأنظمة الجديدة من تسريع عملية التوجيه وتحسين الكفاءة في معالجة البلاغات .مع استمرار التقدم التكنولوجي، بدأت أنظمة البلاغات في استخدام تقنيات أكثر تطورا مثل تطبيقات الهواتف الذكية.

## 2.2 أنواع أنظمة البلاغات تاريخياً

### 2.2.1 الأنظمة التقليدية للبلاغات

**هي الأساليب التي تم استخدامها في الماضي قبل تطور التكنولوجيا الحديثة. كانت تعتمد على الاتصال الهاتفي أو الحضور الشخصي لتقديم البلاغات. فيما يلي شرح للأنظمة التقليدية ومثال عن بعض الدول التي استخدمتها:**

**1- البلاغات عبر الاتصال الهاتفي**

كانت هذه إحدى الأنظمة التقليدية الأولى للبلاغات. يمكن للأفراد الاتصال بمراكز الطوارئ أو مراكز الشرطة المحلية عبر الهاتف لتقديم البلاغات. يتم استقبال المكالمة من قبل موظف في المركز الذي يستمع للبلاغ ويسجل المعلومات الأساسية مثل نوع الحادث أو الجريمة ومكانها. يتم توجيه البلاغ إلى الجهات المختصة لاتخاذ الإجراءات اللازمة. تعتمد هذه الأنظمة على قدرة الأفراد على الاتصال وشرح الحادث بشكل صحيح.

مثال: كانت الولايات المتحدة الأمريكية تستخدم البلاغات عبر الاتصال الهاتفي في العديد من المدن قبل التطور التكنولوجي، حيث يمكن للمواطنين الاتصال برقم الطوارئ 911 لتبليغ عن الحوادث والطوارئ.

**2- البلاغات الشفهية أو الكتابية في المراكز المحلية**

في هذه الحالة، يمكن للأفراد زيارة مراكز الشرطة المحلية أو المركز المخصص لتقديم البلاغ. يتحدث مقدم البلاغ شفهياً مع ضابط الشرطة الموجود في المركز ويقدم معلومات البلاغ. يتم تسجيل المعلومات في نموذج أو استمارة ويتم توجيهها يدويًا إلى الجهة المعنية.

مثال: في المملكة المتحدة، يمكن للأفراد زيارة مراكز الشرطة المحلية لتقديم البلاغات بشكل شفهي أو كتابي، حيث يتم استقبال المبلغين من قبل ضباط الشرطة وتسجيل المعلومات في النماذج المخصصة.

**3- البلاغات عبر البريد الورقي**

كانت هذه الأنظمة تعتمد على إرسال البلاغات عن طريق البريد الورقي إلى الجهة المعنية. يقوم مقدم البلاغ بكتابة البلاغ وإرساله عبر البريد إلى مركز الشرطة أو الجهات المختصة. يتم توجيه البلاغات المستلمة يدويًا إلى الجهات المختصة لاتخاذ الإجراءات اللازمة.

في العديد من البلدان، كانت هناك خدمات البريد الورقي المخصصة لتلقي البلاغات. على سبيل المثال، في الهند، يمكن للأفراد إرسال بلاغاتهم عبر البريد الورقي إلى مركز الشرطة المحلي.

تلك هي بعض الأمثلة عن الأنظمة التقليدية للبلاغات. تتشابه هذه الأنظمة في أسلوبها العام، حيث يتم تقديم المعلومات بشكل شفهي أو كتابي أو عبر الهاتف، ومن ثم يتم توجيه البلاغات إلى الجهات المختصة للتعامل معها. ومع ذلك، يجب التأكيد على أن هذه الأنظمة التقليدية للبلاغات قد تطورت بشكل كبير خلال السنوات الأخيرة مع استخدام تكنولوجيا الاتصالات المتقدمة وتطبيقات الهواتف الذكية والإنترنت لتحسين عملية تلقي ومعالجة البلاغات.

### 2.2.2 الأنظمة الإلكترونية للبلاغات

**هي الانظمة تعتمد على استخدام التكنولوجيا الحديثة والإنترنت لتلقي ومعالجة البلاغات. تعمل هذه الأنظمة على تسهيل وتسريع عملية تقديم البلاغات وتوجيهها إلى الجهات المعنية. فيما يلي شرح للأنظمة الإلكترونية وبعض الأمثلة عن الدول التي تستخدمها:**

**1- البلاغات عبر تطبيقات الهواتف الذكية**

تعتمد هذه الأنظمة على تطبيقات الهواتف الذكية التي يمكن تنزيلها على الهواتف المحمولة. يمكن للمستخدمين استخدام هذه التطبيقات لتقديم البلاغات عن طريق ملء نماذج إلكترونية تحتوي على المعلومات المطلوبة مثل نوع الحادث وموقعه ووصف مفصل للحادث. يتم إرسال البلاغات المقدمة عبر التطبيقات مباشرة إلى المراكز المخصصة لمعالجة البلاغات، حيث يتم توجيهها والتعامل معها وفقًا للأولوية.

**مثال**: في المملكة المتحدة، يستخدم تطبيق "999" لتقديم البلاغات عبر الهواتف الذكية، حيث يمكن للمستخدمين تحميل التطبيق وتعبئة النموذج الإلكتروني لتقديم البلاغات.

**2- البلاغات عبر الإنترنت**

تعتمد هذه الأنظمة على استخدام مواقع الويب المخصصة لتلقي البلاغات. يمكن للأفراد زيارة الموقع الإلكتروني للجهة المعنية وملء النماذج الإلكترونية لتقديم البلاغات. يتم توجيه البلاغات المقدمة عبر الإنترنت إلى الجهة المعنية لمعالجتها واتخاذ الإجراءات اللازمة.

**مثال**: في أستراليا، يمكن للأفراد تقديم البلاغات عبر موقع الشرطة الفيدرالية الأسترالية الرسمي على الإنترنت.

**3- البلاغات عبر وسائل التواصل الاجتماعي**

بعض الدول تسمح بتقديم البلاغات عبر وسائل التواصل الاجتماعي مثل تويتر أو فيسبوك. يمكن للمستخدمين إرسال البلاغات عن طريق التعليقات أو الرسائل المباشرة عبر هذه المنصات، والتي يتم رصدها وتوجيهها إلى الجهات المعنية للتعامل معها . استخدام الأنظمة الإلكترونية للبلاغات بدأ بشكل واسع في العقد الأخير، وذلك بسبب التطور التكنولوجي وانتشار استخدام الإنترنت والهواتف الذكية. تم تبني هذه الأنظمة في مختلف الدول حول العالم بغية تحسين مستوى الخدمات العامة وتعزيز التواصل بين المواطنين والجهات المعنية.

**الآلية عمل الأنظمة الإلكترونية للبلاغات العامة تتضمن الخطوات التالية:**

- **تقديم البلاغ**

يقدم المواطنون أو الأفراد البلاغات المختلفة عبر إحدى من وسائل التواصل الإلكترونية المذكورة أعلاه، مثل تطبيق الهاتف الذكي أو الموقع الإلكتروني أو وسائل التواصل الاجتماعي.

- **جمع المعلومات**

يتم جمع المعلومات المقدمة في البلاغ، مثل نوع الحادث أو المشكلة وموقعها وأي تفاصيل إضافية ذات صلة.

- **توجيه البلاغ**

يتم توجيه البلاغ إلى الجهات المعنية لمعالجة البلاغات المقدمة. قد يتم تحويل البلاغات إلى الجهة المناسبة حسب نوع الحادث أو المشكلة، مثل الشرطة، أو الإطفاء، أو الإسعاف، أو البلدية.

- **معالجة البلاغ**

تقوم الجهات المعنية بتقييم البلاغ واتخاذ الإجراءات اللازمة لحل المشكلة أو التعامل مع الحادث. يمكن أن تشمل الإجراءات إرسال فرق ميدانية، أو التواصل مع مقدم البلاغ للحصول على مزيد من المعلومات، أو توجيه البلاغ للجهات الأخرى في حالة الاختصاص.

- **متابعة البلاغ**

يمكن للمواطنين متابعة حالة البلاغ الذي قاموا بتقديمه ومعرفة التقدم المحرز في حل المشكلة عبر الأنظمة الإلكترونية. قد توفر بعض الأنظمة رقم تتبع للبلاغ يمكن استخدامه لمتابعة حالته.

## 2.3 الدراسات السابقة

**جدول (2.1) الدراسات السابقة**

| عنوان البحث | تاريخ التصميم | الشركة المصممة | مميزات | العيوب |
|---|---|---|---|---|
| **نظام بلاغات الشرطة الإلكترونية ElectroniPolice Reporting System** | **2011** | **Tenable Security** | **يتيح للمواطنين إرسال بلاغاتهم إلى الشرطة بشكل إلكتروني دون الحاجة للذهاب إلى المراكز الشرطة بشكل مباشر. يتضمن نظام إدارة الملفات والتوثيق الرقمي للبلاغات.** | **قد يكون هناك تحديات في تأمين البيانات الشخصية وضمان سرية المعلومات المرسلة عبر النظام.** |

| | | | | |
|---|---|---|---|---|
| نظام بلاغات الجرائم المتكامل Integrated Crime Reporting System | 2012 | Akinetic, Inc | يسمح بتجميع وتحليل البيانات المرتبطة بالجرائم من مصادر متعددة، بما في ذلك التقارير مراكز الشرطة. يمكن استخدامه في رصد النماذج الجغرافية للجريمة وتحديد الاتجاهات وتوجيه استراتيجيات الشرطة. | قد تواجه التحديات في جمع البيانات بشكل موحد وتوحيدها في قواعد بيانات مركزية، وقد يكون هناك صعوبات في تبادل المعلومات بين أنظمة الشرطة المختلفة. |
| نظام إدارة الحوادث والتحقيق<br><br>Incident and Investigation Management System | 2012 | Ideated | يتيح لرجال الشرطة إدارة الحوادث والتحقيقات بشكل مركزي، بدءًا من تسجيل التقارير وجمع الأدلة ومتابعة التحقيقات وتوثيق النتائج .<br>يمكن أن يسهم في تحسين كفاءة وسرعة استجابة الشرطة وتحسين جودة البيانات والتوثيق. | قد تواجه بعض التحديات في التكامل مع أنظمة أخرى المستخدمة في مراكز الشرطة وتوحيدها مع قواعد بيانات المحكمة وأجهزة الشرطة الأخرى. |
| نظام بلاغات الطوارئ المركزية Centralized Emergency Reporting System | 2014 | Security Apsana | 1- يسمح للمواطنين بالإبلاغ عن الحوادث والحالات الطارئة مثل الجرائم والحرائق والحوادث عبر وسائل التواصل المتاحة مثل الهاتف والإنترنت والتطبيقات المحمولة.<br><br>2- يتضمن نظام التحقق وتحليل البيانات لتحديد وتوجيه استجابة الشرطة وفرق الطوارئ المناسبة. | قد تحتاج إلى إدارة كبيرة للبيانات وتحقيق في سرعة الاستجابة وتوجيه الفرق والتواصل الفعال مع المواطنين في حالات الطوارئ المتعددة. |
| نظام إدارة البلاغات المتكامل Integrated Incident Management System | 2015 | Outswinger Lt | يتم استخدامه لتسجيل وإدارة البلاغات المتعلقة بالجرائم والحوادث والمخالفات المرورية والشكاوى العامة. يوفر واجهة مركزية لإدارة البلاغات وتوزيعها للفرق المعنية وتتبع تقدم التحقيقات والتنسيق مع الجهات الأخرى. | قد تحتاج إلى تدريب مستخدمين متخصصين على النظام وتكامله مع أنظمة أخرى مستخدمة في مراكز الشرطة. |
| نظام بلاغات الشرطة المحمول Mobile Police Reporting System | 2019 | Orc, security | 1- يسمح لرجال الشرطة باستخدام الأجهزة المحمولة مثل الهواتف الذكية أو الأجهزة اللوحية لتلقي وتسجيل البلاغات وإرسال التقارير الميدانية مباشرةً إلى النظام المركزي.<br>2- يمكن استخدامه في جمع الأدلة والصور وتحديد الموقع الجغرافي للبلاغات. | قد تواجه بعض التحديات فيما يتعلق بالتوافر الشبكي والتكامل مع أنظمة أخرى في مراكز الشرطة. |

## 2.4 الدراسة الحالية

الأنظمة السابقة للبلاغات تختلف من دولة إلى أخرى وتعتمد على التطور التكنولوجي والتنظيمات المحلية ومع ذلك، يمكن تحديد بعض الاتجاهات العامة في تطور أنظمة البلاغات.

في الماضي، كانت البلاغات تُقدم بشكل رئيسي عن طريق الاتصال الهاتفي بمراكز الطوارئ أو مكاتب الشرطة المحلية. كان مقدموا البلاغ يتواصلون شفهيًا أو كتابيًا لتقديم البلاغات، وكانت هناك جهود يدوية لتوجيه البلاغات الصحيحة إلى الجهات المعنية.

مع تطور التكنولوجيا، بدأ استخدام نماذج البلاغات الورقية المحددة لتسهيل عملية تقديم البلاغات. تتمثل هذه النماذج في استمارات يملأها المبلغون ويقومون بإرسالها عبر البريد الإلكتروني أو البريد الورقي. تقوم الجهات المعنية بتوجيه البلاغات المستلمة يدويًا.

مع تزايد استخدام الإنترنت والتقنيات الرقمية، ظهرت أنظمة البلاغات الإلكترونية. تم تطوير منصات إلكترونية خاصة لتلقي وتوجيه البلاغات. يستخدم مقدموا البلاغ النماذج الإلكترونية المتاحة لتقديم البلاغات، وتحتوي هذه الأنظمة على آليات لتحليل وتصنيف البلاغات وتوجيهها إلى الجهات المختصة بشكل أكثر فعالية.

مع تطور التكنولوجيا المحمولة، بدأت بعض الأنظمة في استخدام تقنيات الموقع الجغرافي والتطبيقات الذكية لتحسين عملية البلاغات. يمكن لمقدمي البلاغات استخدام تطبيقات الهواتف الذكية لتقديم البلاغات وتوثيقها بالصور أو مقاطع الفيديو. تستخدم هذه التقنيات المعلومات الجغرافية لتحديد موقع البلاغ وتوجيهه بشكل دقيق إلى الجهات المختصة.

من المهم أيضًا أن نشير إلى أن تطور أنظمة البلاغات يتطلب أيضًا اهتمامًا بالقضايا المتعلقة بالخصوصية والأمان. يجب ضمان أن تكون هذه الأنظمة آمنة ومحمية بما يكفي لحماية معلومات مقدم البلاغ والحفاظ على سرية البلاغات.

علاوة على ذلك، يمكن أن يتم تحسين أنظمة البلاغات عن طريق تعزيز التعاون والتنسيق بين الجهات المعنية. يمكن للتكنولوجيا أن تسهم في تبادل البيانات والمعلومات بين الجهات المختلفة لتحقيق استجابة أفضل وتعاون أكثر فاعلية في التعامل مع البلاغات.
في النهاية، يجب أن يكون التركيز دائمًا على تحسين أنظمة البلاغات لضمان أن يتم تلقي ومعالجة البلاغات بسرعة وفعالية ودقة. يمكن أن تلعب التكنولوجيا والابتكار دورًا هامًا في تحقيق ذلك من خلال تسهيل عملية البلاغات وتحسين التوجيه وتحليل البيانات والتعاون بين الجهات المعنية.

# الفصل الثالث :دراسة الجدوى والتحليل

## 3.1 السيناريو

أولا على مستوى قسم الشرطة تتم إضافة البلاغات من قبل ضباط البلاغات، حيث يتم تسجيل جميع تفاصيل البلاغ بما في ذلك بيانات مقدم البلاغ.

بعد إضافة البلاغ، يتم إحالته إلى إدارة البلاغات التي تتألف من مشرف البلاغات ورئيس قسم الشرطة للموافقة عليه وإذا كان البلاغ يحتاج الي موافقة الجهات العليا في إدارة الامن او وزارة الداخلية يتم رفع البلاغات حسب الأهمية ومدى التعميم وعند الاحتياج للأوامر من النيابة يتم رفع البلاغ إلى إدارة الامن لتقوم بتبليغ النيابة المختصة في المنطقة عبر مسؤول النظام في النيابة للحصول على الموافقة .

عند استلام الموافقة، يتم تعميم البلاغ إلى الأجهزة الأمنية في قسم الشرطة للأمساك بالجاني ورفع تقرير البلاغ إلى إلى إدارة الأمن عند الاحتياج لتعميمه بشكل أوسع ويمكن أيضا تعميمه على مستوى وزارة الداخلية ليعمم في انحاء الجمهورية، مما يتيح لضباط النقاط الأمنية في منطقة التعميم البحث بواسطة الرقم الوطني للأشخاص ومعرفة سجلهم.

بالإضافة إلى ذلك، يتم تعميم بلاغات المسروقات على المحلات والمعارض التجارية باستخدام الرقم التسلسلي لوقف بيع المسروقات.

حيث أيضا هناك مشرف للمحلات والمعارض التجارية في كل قسم شرطة ضمن منطقته الذي يعمل على الاشراف وتلقي التقارير من المحلات والمعارض التجارية ومصادرة المسروقات والتحفظ عليها ليتم تسليميها إلى مسؤول المسروقات في النيابة .

وفي حال كان البلاغ كاذب او هناك حاجه لتعديله أو حذفه يتم ذلك من الجهة الإدارية وفق الوقت المحدد لتعديل مالم فيتم بطلب تفويض.

## 3.2 دراسة الجدوى

**قمنا بدراسة الجدوى لمعرفة ما إذا كان النظام مجدي من جميع النواحي التي قد تؤثر على النظام و تقييم مدى جدوى هذا المشروع وقدرته على النجاح وتحقيق الأهداف المرجوة ؛ الجوانب الذي قمنا بدراستها:**

### 3.2.1 الجدوى التقنية

1. **تجهيزات الهارد وير:**
   - **3 أجهزة حاسوب ؛ بالمواصفات التالية :**
     1. CPU: Core i7.
     2. RAM: 8 GB.

**2. تجهيزات السوفت وير :**

- نظام تشغيل Windows10 /11.
- Laravel Framework .
- برنامج Microsoft Visual Studio Code لإنشاء وتصميم الواجهات.
- Xampp لرفع الموقع على سيرفر محلي على جهاز الكمبيوتر(Localhost) .
- برنامج Edraw Max لرسم مخططات ER ، UML وغيرها.

### 3.2.2 الجدوى الزمنية

**الجدول التالي يبين الجدوى الزمنية للمشروع :**

**جدول (3.1) الجدوى الزمنية**

| المرحلة | الفترة الزمنية / بالشهور | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| التحديد والاختيار | | | | | | | | | | | | |
| تجميع البيانات | | | | | | | | | | | | |
| التخطيط والبدء بالمشروع | | | | | | | | | | | | |
| التحليل | | | | | | | | | | | | |
| التصميم | | | | | | | | | | | | |
| التنفيذ والاختبار | | | | | | | | | | | | |
| التوثيق | | | | | | | | | | | | |

### 3.2.3 الجدوى الإقتصادية

**جدول (3.2) الجدوى الاقتصادية المادية**

| متطلبات مادية | العدد | التكلفة |
|---|---|---|
| اجهزة كمبيوتر مكتبية | 3 | $300 |
| Access point. | 1 | $20 |
| Server | 1 | $600 |
| Switch | 1 | $300 |
| Cable Cat 6 | | $15 |
| الاجمالي : | $ 1235 | |

**جدول (3.3) الجدوى الاقتصادية البرمجية**

| متطلبات البرمجية | العدد | التكلفة |
|---|---|---|
| Windows 11 | 1 | $20 |
| Laravel Framework | 1 | $0 |
| Edraw Max | 1 | $5 |
| Visual Studio code | 1 | $10 |
| Xammp | 1 | $0 |
| الاجمالي : | $35 | |

**جدول (3.4) الجدوى الاقتصادية بشكل عام**

| الفائدة | الوضع قبل النظام | الوضع بعد تطبيق النظام | التأثير الاقتصادي / الاستثماري |
|---|---|---|---|
| وجود أدوات أمنية مدمجة بالنظام | يعتمد على أنظمة مشتتة وأجهزة متفرقة | أدوات أمنية موحدة ومتكاملة ضمن النظام | تقليل تكلفة شراء وصيانة الأنظمة المنفصلة، وتحسين كفاءة العمليات |
| تقليل الاعتماد على الموارد البشرية | حاجة لموظفين كُثر لاستقبال البلاغات يدويًا عبر الهاتف أو المراكز | النظام يستقبل البلاغات آليًا ويقلل عدد الموظفين اللازمين | توفير في الرواتب والتدريب بنسبة قد تصل إلى30–50% |
| تسريع وصول البلاغات للجهات الأمنية | تأخير بسبب الإجراءات اليدوية أو الوسائل التقليدية | وصول فوري للبلاغات مع تحديد الموقع والبيانات تلقائيًا | تقليل زمن الاستجابة بنسبة–50 70%، مما يقلل من الخسائر الناجمة عن التأخير |
| شعور أكبر بالأمان وتحسين ثقة المجتمع بالأجهزة الأمنية | شكاوى مجتمعية بسبب بطء الاستجابة وضعف التفاعل | زيادة التفاعل المجتمعي والرضا العام عن الجهات الأمنية | دعم الاستقرار المجتمعي، ما ينعكس على تقليل التكاليف الاجتماعية والأمنية على المدى الطويل |
| استجابة أسرع تسهم في تقليل الحوادث والجرائم | تأخر في التدخل يؤدي إلى تفاقم الحوادث وزيادة الخسائر | سرعة استجابة تقلل من آثار الحوادث وتحد من تطورها | انخفاض معدلات الحوادث والجرائم يقلل من الإنفاق الأمني الطارئ ويزيد من كفاءة الأداء |

## 3.2.4 الجدوى التشغيلية

- **الاداء "performance"**

التأكد من ان النظام يعمل بسرعه بحيث يقوم بأجراء أكبر قدر من العمليات بأقل وقت ممكن .

- **معلومات "information"**

يجب ان يقوم بإدخال بيانات صحيحه اللازمة لإتمام العمليات بنجاح والتأكد من مرونة النظام بحيث لا يتوقف النظام في حال تم ادخال بيانات خاطئة كما يجب ان يقوم النظام بتخزين البيانات بالشكل والصيغة الصحيحة بحيث يمنع أي تعارض في قاعدة البيانات وبالتالي يقوم باسترجاع المعلومات المطلوبة منه بالشكل الصحيح .

- **الاقتصادية "Economic"**

تم توضيحه في الجدوى الاقتصادية.

- **خدمات"Services"**

تتمثل خدمات النظام في اعطائه نتائج صحيحه، دقيقة، متناسقة لتحقق الهدف المرغوب كما ان النظام قادر على التوافق مع الانظمة الاخرى.

## 3.3 جمع المتطلبات

نتطرق هنا إلى الجهة التحليلية للنظام من حيث عملية جمع البيانات وتحديد كلا من مدخلات ومخرجات النظام حيث أنه بعد تجميع الآراء والحقائق يجب أن نقوم بتنظيمها بصورة تسمح باستخلاص بعض النتائج ذات الفائدة، والتي سوف تساهم في إكمال الصورة عن احتياجات مستخدمي النظام وخدمتهم .وهناك عدة طرق لجمع المتطلبات وقد قمنا باستخدام بعضها بما يتوافق مع مشروعنا لإكمال جمع المتطلبات ومنها:

### 3.3.1 المقابلة الشخصية

**(مرفق في الملحق أسئلة المقابلة)**

تم إجراء مقابلة مع بعض المواطنين المتواجدين في أقسام الشرطة لتقديم بلاغاتهم وشكاويهم. أشار المواطنون إلى عدة تحديات تواجههم في النظام الحالي، بما في ذلك عدم توفر الاستجابة السريعة وصعوبة في الإجراءات المتبعة. كما أبدوا استياءهم من صعوبة تحديد هوية المجرمين المشتبه بهم وسهولة التلاعب من قبل بعض المنتسبين للمراكز الشرطة بسبب عدم وجود رقابة ومتابعة فعالة للبلاغات.

تم تقديم مقترحات من قبل المواطنين بشأن نظام البلاغات، وتحديد الاحتياجات التي يرون أنها تحتاج إلى تلبية الخدمات الأمنية وتوصيل مركز الشرطة بالوزارة والسلطات العليا للمتابعة. يجب أن يكون هناك نظام يتيح الاستجابة السريعة والفعالة للبلاغات، بالإضافة إلى وسيلة سهلة وكفؤة لتعميم المعلومات والقبض على المجرمين.

تم أيضًا إجراء مقابلات مع أصحاب المحلات التجارية وتجار الجملة في مجال الأجهزة الإلكترونية لمعرفة كيفية شراء الأجهزة من المواطنين وكيفية التحقق من تعرضها للسرقة. وتمت مقابلات مع موظفي الأقسام والمسؤولين أيضًا لفهم الإجراءات المتبعة واحتياجات النظام الحالي.

بناءً على المقابلات التي تم إجراؤها، يتضح أن هناك حاجة لتحسين نظام البلاغات فيما يتعلق بالاستجابة السريعة، وتسهيل الإجراءات، وتعزيز الرقابة والمتابعة، وتحسين وسائل التواصل والتعميم، وتعزيز قدرة الشرطة على القبض على المجرمين وحماية المواطنين من الجرائم وأيضاً تعزيز الحماية والخصوصية في النظام.

### 3.3.2 الاستبيان

**(مرفق في الملحق الاستبيان)**

تم إجراء استبيان خاص بنظام البلاغات في أقسام الشرطة لغرض تقييم النظام الحالي وتقييم النظام الجديد بعد تعريف المشاركين بتفاصيله. كما تم منح المشاركين الفرصة لتقديم مقترحاتهم وآرائهم بشأن النظام الجديد.

تهدف هذه المبادرة إلى فهم آراء وتقييمات المستخدمين المشاركين في النظام حاليًا والمواطنين، والحصول على اقتراحاتهم لتحسين النظام الجديد. من خلال تحليل النتائج والاستنتاجات المستخلصة من الاستبيان، وفقا للاستبيانات والمقابلات الفردية والجماعية سوف يتم اتخاذ التدابير اللازمة للتحسين وتلبية احتياجات المواطنين بشكل أفضل.

**ومن أبرز الأفكار التي تم استنتاجها (بعد المقابلة والاستبيان)**

1- **المواطنين**

كانت النتيجة كالتالي

50% اشروا إلى ضرورة تحسين سرعة وفعالية استجابة الأقسام الشرطية للبلاغات المقدمة.

30% طلبوا التوسيع لوسائل التواصل المتاحة للمواطنين للإبلاغ عن الجرائم، مثل الهواتف المحمولة والتطبيقات الذكية.

بقية الاستبيانات كانت حول توفير تحديثات دورية للمبلغين وتزويدهم بمعلومات حول تطورات التحقيق ونتائجه.

2- **الموظفين**

70% أشاروا ضرورة توفير التدريب المستمر لأفراد الشرطة حول كيفية التعامل مع البلاغات وتقنيات التحقيق الحديثة، بالإضافة إلى زيادة الوعي بحقوق المواطنين وواجبات الشرطة.

20% أبدوا أن لديهم الرغبة في تعزيز مستوى الشفافية والثقة في نظام البلاغات، من خلال توفير معلومات واضحة حول إجراءات التحقيق وتوفير تحديثات مستمرة للمبلغين.

بقية الإستبيانات كانت مع ضرورة تحسين سرعة وفعالية إستجابة أقسام الشرطية للبلاغات المقدمة.

3- **أصحاب المحلات التجارية**

80%يعتقد بعض المشاركين أن وجود نظام لتنظيم عملية شراء الأجهزة والمسروقات والتحقق من سرقتها يمكن أن يعزز المصداقية والثقة بين المحلات والزبائن. يمكن لهذا النظام المساعدة في تحسين عملية فحص الأجهزة المعروضة للبيع والتأكد من أنها ليست مسروقة، مما يوفر حماية أكبر للمشترين ويقلل من تعرضهم للمشتريات غير الشرعية. وبالتالي، يمكن أن يؤدي هذا النظام إلى تعزيز الثقة والرضا لدى الزبائن وتحسين المصداقية والسمعة العامة للمحلات التجارية.

20% يعارض هذا الإجراء بسبب الروتين الطويل والمعقد الذي يشوب عملية الشراء. يرون أن تنفيذ إجراءات تحقق الجهاز والتأكد من عدم سرقته يزيد من التعقيد والوقت اللازم لإتمام الصفقة، مما يجعل عملية الشراء أكثر صعوبة وتعقيدًا للمواطن. قد يؤدي هذا الإجراء إلى إبطاء عملية الشراء وتأخير حصول العملاء على المنتجات التي يحتاجونها.

### 3.3.3 الملاحظة و المشاهدة

**بناءً على الاستبيانات والمقابلات السابقة واحتياجات المواطنين والموظفين، يمكن اقتراح التعديلات التالية لتحسين نظام البلاغات وإستجابة الأقسام الشرطة:**

**1. تحسين سرعة وفعالية الاستجابة:**

- زيادة عدد رجال الشرطة وموظفي الإدارة المستخدمين للنظام المعني بالبلاغات لتحقيق استجابة أسرع وأكثر فعالية.

- تطوير نظام آلي لتوزيع البلاغات وتعيين الموظفين المناسبين للتعامل مع كل بلاغ بناءً على المنطقة والطبيعة الجغرافية والمهارات المطلوبة.

**2. توسيع وسائل التواصل المتاحة للمواطنين:**

- تطوير تطبيقات ذكية ومنصات إلكترونية تسمح للمواطنين بتقديم البلاغات والتواصل مع الشرطة والاستعلامات عبر الهواتف المحمولة.

**3. تحسين الشفافية وتوفير المعلومات:**

- تطوير نظام إلكتروني يتيح للمبلغين تتبع تطورات التحقيق والحصول على تحديثات دورية عند توفرها.

- نشر تقارير دورية توضح معدلات الاستجابة والتحقيق والنتائج المحققة، مع توفير تفسيرات واضحة للإجراءات المتبعة والتحديثات المستمرة.

**4. تعزيز التدريب والوعي:**

- توفير برامج تدريبية مستمرة لأفراد الشرطة حول كيفية التعامل مع البلاغات وتقنيات التحقيق الحديثة، بالإضافة إلى زيادة الوعي بحقوق المواطنين وواجبات الشرطة.

- تنظيم حملات توعية للمواطنين بطرق التواصل مع الشرطة وكيفية تقديم البلاغات بشكل صحيح وفعال.

## 3.4 متطلبات المستخدم

1. ان تكون الواجهات سهلة ليتم التعامل معها دون وجود عوائق.
2. ان تكون قاعدة البيانات مصممة بلغة SQL .
3. القدرة على إجراء نسخة احتياطية للبيانات وتحديثها دورياً .
4. سرعة وكفاءة استجابة النظام.
5. أن يتسم بالأمنية والسرية والخصوصية العالية.
6. سد الثغرات والوقاية من الهجمات.

## 3.5 المتطلبات الوظيفية (Functional Requirements)

نظام البلاغات الخاص بأقسام الشرطة يهدف إلى توفير الميزات والوظائف الأساسية التي يجب أن يقدمها النظام لتلبية إحتياجات أقسام الشرطة وتسهيل إدارة ومعالجة البلاغات وتسجيل البلاغات وتعميم البلاغات و توليد تقارير وإحصائيات والتكامل مع الأنظمة أخرى حيث يمكن أن يتطلب نظام البلاغات التكامل مع أنظمة أخرى داخل أقسام الشرطة وخارج اقسام الشرطة، ويتيح التكامل مع هذه الأنظمة لتبادل المعلومات والتعاون بين الأنظمة المختلفة.

- **تقديم البلاغ**

يتيح النظام للمواطنين تقديم البلاغات بسهولة ويسر حيث يتضمن النظام استمارة تعبئة البيانات التي تحتوي على معلومات مقدم البلاغ والمبلغ علية مثل الاسم الكامل ورقم الوطني ومعلومات الاتصال والشهود ووصف واضح للحادثة أو الجريمة. تحديد طبيعة البلاغ، مثل البلاغات المتعلقة بأجهزة أو البلاغات الجنائية مثل السرقة أو الاعتداء ويساعد هذا التحديد في توجيه البلاغات الصحيحة إلى الجهات ذات الصلة في المركز الشرطة.

- **متابعة التحقيق**

يتيح النظام للموظفين المختصين تتبع ومتابعة التحقيقات المرتبطة بالبلاغات ويوفر النظام واجهة لإدخال تحديثات التحقيق والمعلومات الجديدة المكتشفة.

- **تعميم البلاغ**

يتيح النظام تعميم البلاغات ذات الصلة على النقاط الأمنية الأخرى لتعزيز التعاون والتنسيق بين الجهات المختلفة كما يتيح النظام إرسال تنبيهات أو إشعارات لأصحاب المحلات التجارية أو الجهات المعنية ببلاغات الأجهزة عبر تطبيقات أو وسائل الاتصال الأخرى.

- **توليد التقارير**

يوفر النظام إمكانية توليد تقارير شاملة تتضمن إحصائيات البلاغات المستلمة، ومعدلات الاستجابة، ونتائج التحقيقات. وهذا التقارير قابلة للتخصيص والتصدير لمساعدة الإدارة في اتخاذ القرارات الاستراتيجية وتحسين أداء النظام.

- **الأمان**

أن يكون النظام ذو حس أمني عالي جدًا للحفاظ على سلامة المعلومات والبيانات المتعلقة بالبلاغات.بحيث يكون لنظام طبقات أمان متعددة تشمل التحقق من الهوية، وحماية البيانات، وصلاحيات الوصول، وتدقيق السجلات بالتالي مستويات الحماية في النظام هي : في قواعد البيانات و الاكواد البرمجية والشبكات وغيرها.

## 3.6 المتطلبات غير الوظيفية (Non-Functional Requirements)

يعتبر نظام البلاغات أداة حيوية لإدارة ومعالجة البلاغات والتعامل مع الجرائم والحوادث. وبالإضافة إلى المتطلبات الوظيفية التي تركز على الميزات والوظائف الأساسية للنظام، هناك مجموعة من المتطلبات الغير وظيفية التي تهدف إلى تعزيز كفاءة، وفعالية النظام وتحسين النظام وتأمينه.

- **قابلية الاستخدام**

- أن يكون النظام سهل الاستخدام للمستخدمين المختلفين، بما في ذلك والموظفين وضباط النقاط الأمنية وأصحاب المحلات التجارية.
- أن تكون واجهة المستخدم بسيطة وبديهية، ويجب أن يتم توفير تعليمات وتوجيهات واضحة للمستخدمين.

- **الثقة**

أن يكون النظام قابلًا للثقة وموثوقًا به في تنفيذ المهام المطلوبة ويتم اختبار وتحليل النظام بدقة للتأكد من أنه يلبي المعايير والمتطلبات المحددة وفقا لما يتناسب معا المستخدمين ويلبي احتياجات المواطنين في الوقت المحدد.

- **الأداء**

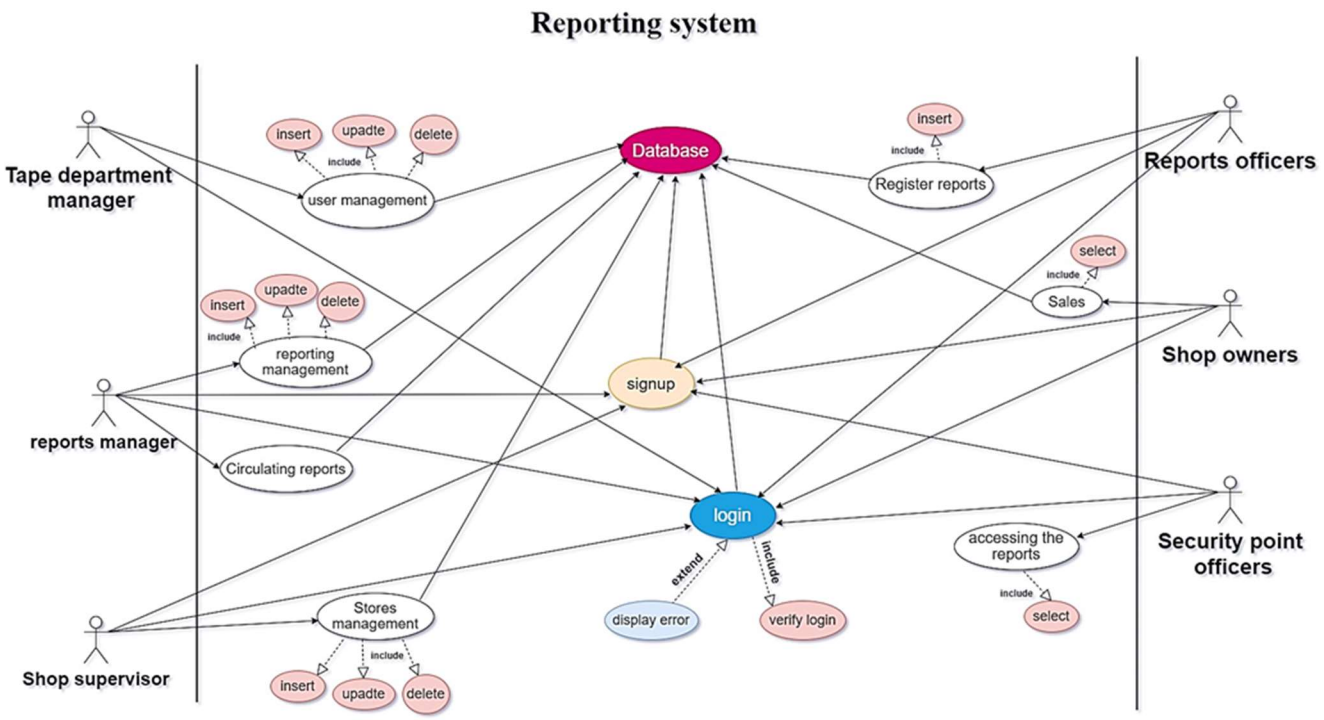
- أن يكون النظام قادر على التعامل مع حجم كبير من البلاغات والمعلومات بكفاءة وسرعة.
- يتم تحسين أداء النظام من خلال استخدام تقنيات مثل التخزين المؤقت والتحسينات على مستوى قاعدة البيانات.

- **التنقيح**

- توفير آليات لتنقيح النظام بناءً على ردود فعل المستخدمين والتحسينات المستمرة.
- آلية لتحديث النظام وإصلاح الأخطاء وتطويره لتلبية احتياجات المستخدمين وتغيرات البيئة.

## 3.7 مخططات النظام

### Use case 3.7.1




**شكل (3.1) Use Case diagram**

**جدول (3.5) جدول عملية signup**

| | |
|---|---|
| **User Case Id** | **1** |
| **User CaseName** | **Signup** |
| **Description** | **User signup your information to the application.** |
| **Actors** | **All users except police manager.** |
| **Flow of event** | **1. User enters user name , password and email.**<br>**2. User submits user name , password and email.** |
| **Precondition** | **Enter new username , password and email.** |
| **Postcondition** | **You can go to log in.** |
| **Exception** | **Enter user name ,password , email.** |

**جدول (3.6) جدول عملية login**

| | |
|---|---|
| **User Case Id** | **2** |
| **User Case Name** | **Login** |
| **Description** | **User login to the application** |
| **Actors** | **All users** |
| **Flow of event** | **User valid enters user name and password.** |
| **Precondition** | **You must be signed up in the system. .** |
| **Postcondition** | **You can go to your Authorized operations.** |
| **Exception** | **Error password and username entered .** |

**جدول (3.7) جدول عملية User management**

| | |
|---|---|
| **User Case Id** | **3** |
| **User Case Name** | **User management .** |
| **Description** | **Manage users and police station.** |
| **Actors** | **Police manager.** |
| **Flow of event** | **Add ,update, delete (limited)** |
| **Precondition** | **You must be logined in the system. .** |
| **Postcondition** | **You can go to your Authorized operations.** |
| **Exception** | **…** |

**جدول (3.8) جدول عملية Reporting management**

| | |
|---|---|
| User Case Id | 4 |
| User Case Name | Reporting management |
| Description | Manage reports |
| Actors | Reporting manager |
| Flow of event | Add ,update, delete (limited) |
| Precondition | You must be logined in the system. . |
| Postcondition | You can go to your Authorized operations. |
| Exception | … |

**جدول (3. 9) جدول عملية Circulating reports**

| | |
|---|---|
| **User Case Id** | **5** |
| **User Case Name** | **Circulating reports** |
| **Description** | **.stations and security points Circulating reports to police** |
| **Actors** | **Reporting manager** |
| **Flow of event** | **Sending notification of a report** |
| **Precondition** | **You must be added the report in the system. .** |
| **Postcondition** | **You can go to your Authorized operations.** |
| **Exception** | **…** |

**جدول (3.10) جدول عمليةStores management**

| | |
|---|---|
| **User Case Id** | **6** |
| **User Case Name** | **Stores management** |
| **Description** | **Managr stores** |
| **Actors** | **Stores manager** |
| **Flow of event** | **Add ,update, delete (limited)** |
| **Precondition** | **You must be logined in the system. .** |
| **Postcondition** | **You can go to your Authorized operations.** |
| **Exception** | **…** |

**جدول (3.11) جدول عملية Register reports**

| | |
|---|---|
| **User Case Id** | **7** |
| **User Case Name** | **Register reports** |
| **Description** | **Enter the report to the system** |
| **Actors** | **Reports officers** |
| **Flow of event** | **Insert the reports** |
| **Precondition** | **You must be logined in the system. .** |
| **Postcondition** | **You can go to your Authorized operations.** |

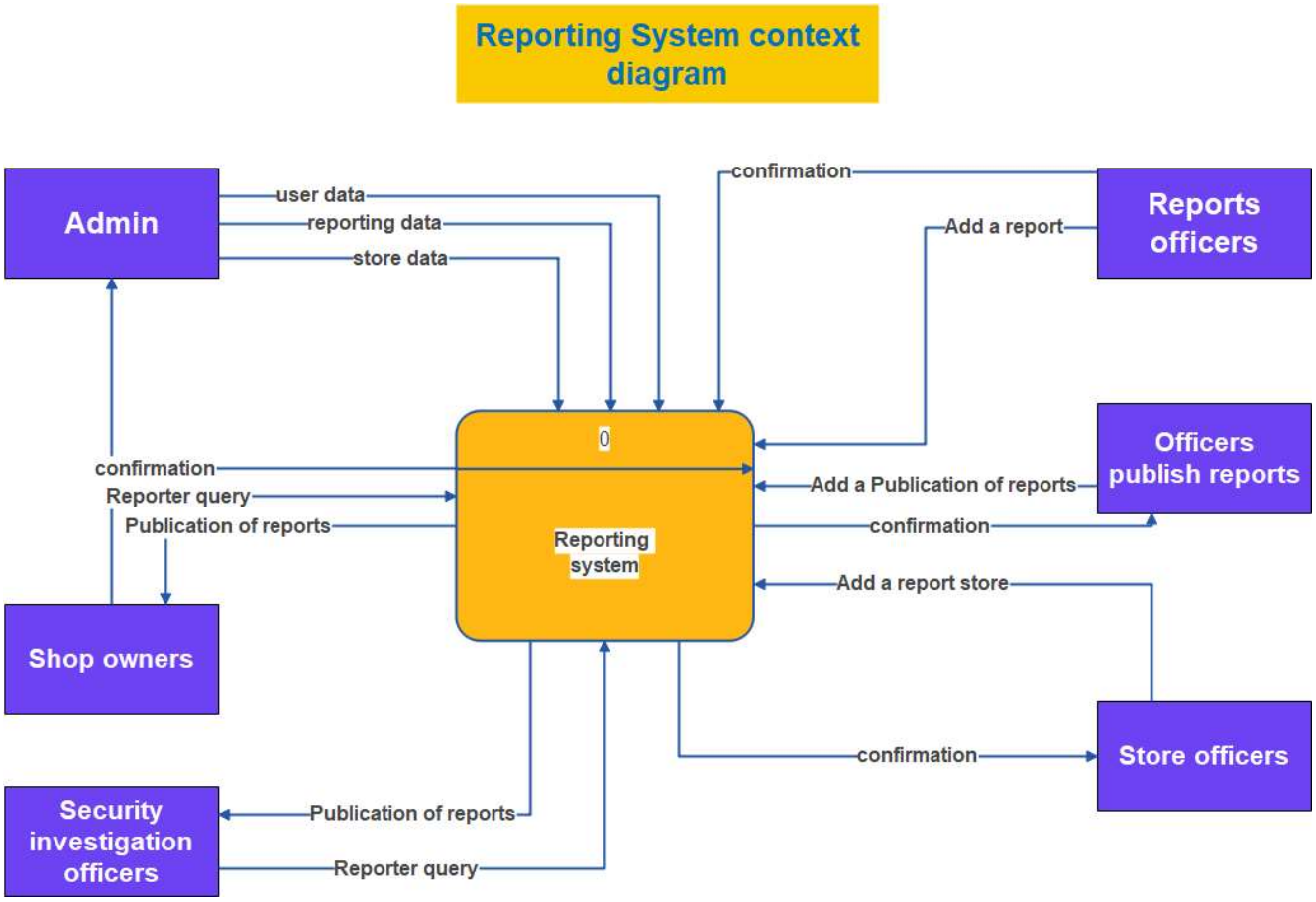
**جدول (3.12) جدول عملية Sales**

| | |
|---|---|
| **User Case Id** | **8** |
| **User Case Name** | **Sales** |
| **Description** | **Check out the sales** |
| **Actors** | **Stores owner** |
| **Flow of event** | **Select and manage the sales** |
| **Precondition** | **You must be logined in the system. .** |
| **Postcondition** | **You can go to your Authorized operations.** |
| **Exception** | **…** |

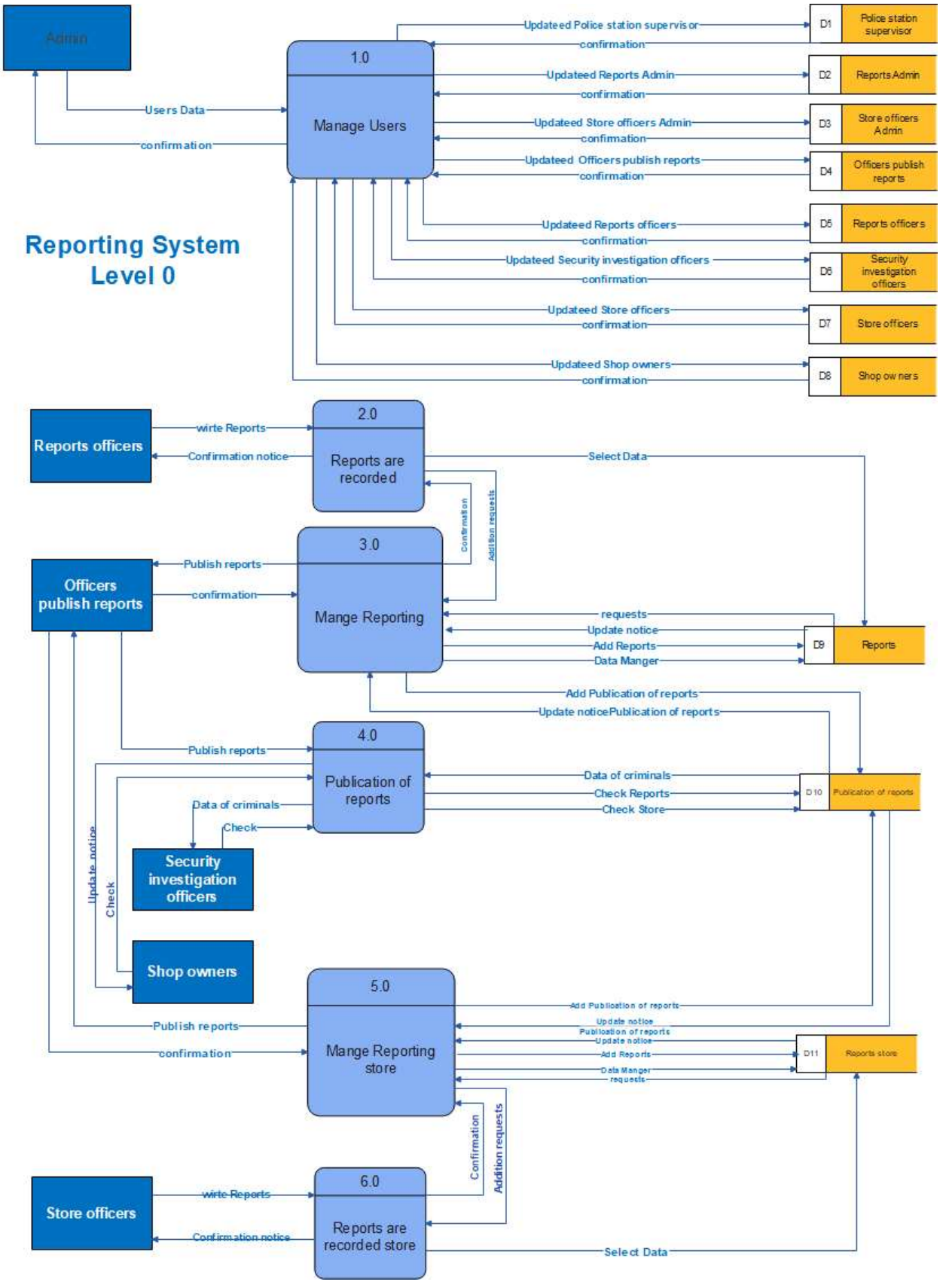
**جدول (3.13) جدول عملية accessing the reports**

| | |
|---|---|
| **User Case Id** | **9** |
| **User Case Name** | **accessing the reports** |
| **Description** | **Check out the reports** |
| **Actors** | **security points officers** |
| **Flow of event** | **Select the reports** |
| **Precondition** | **You must have sent a notification of reports.** |
| **Postcondition** | **You can go to your Authorized operations.** |
| **Exception** | **…** |

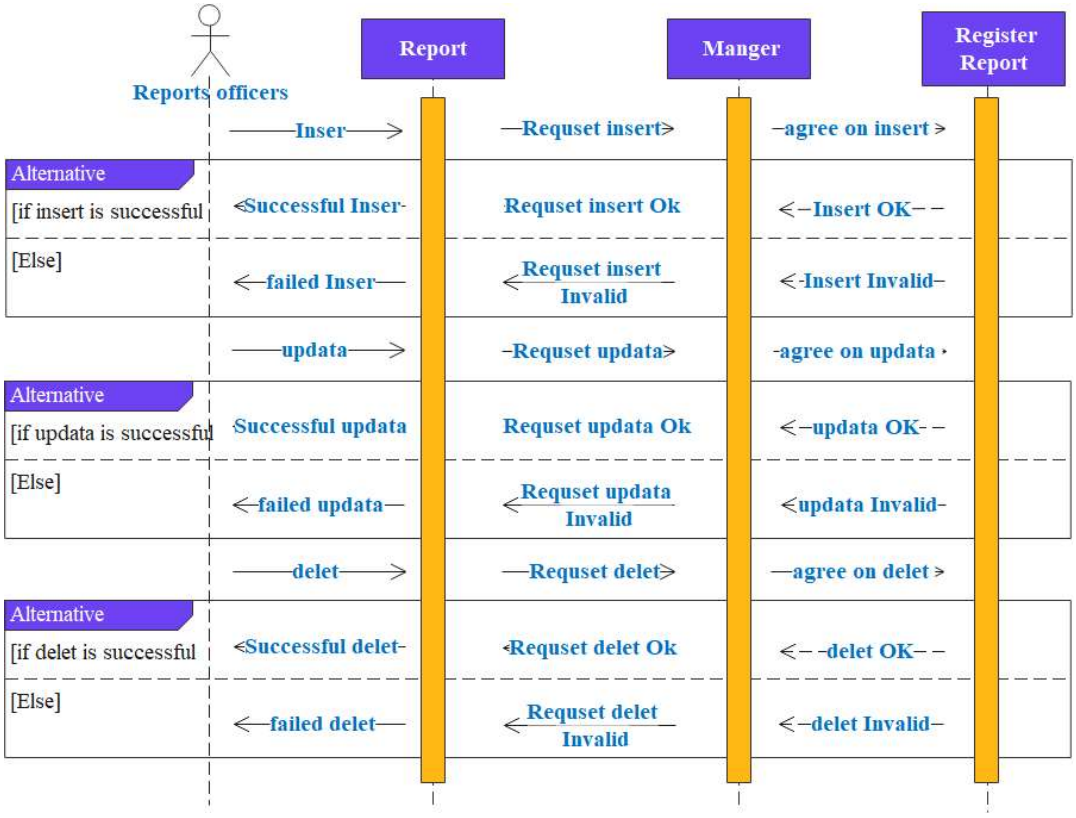
DFD context 3.7.1



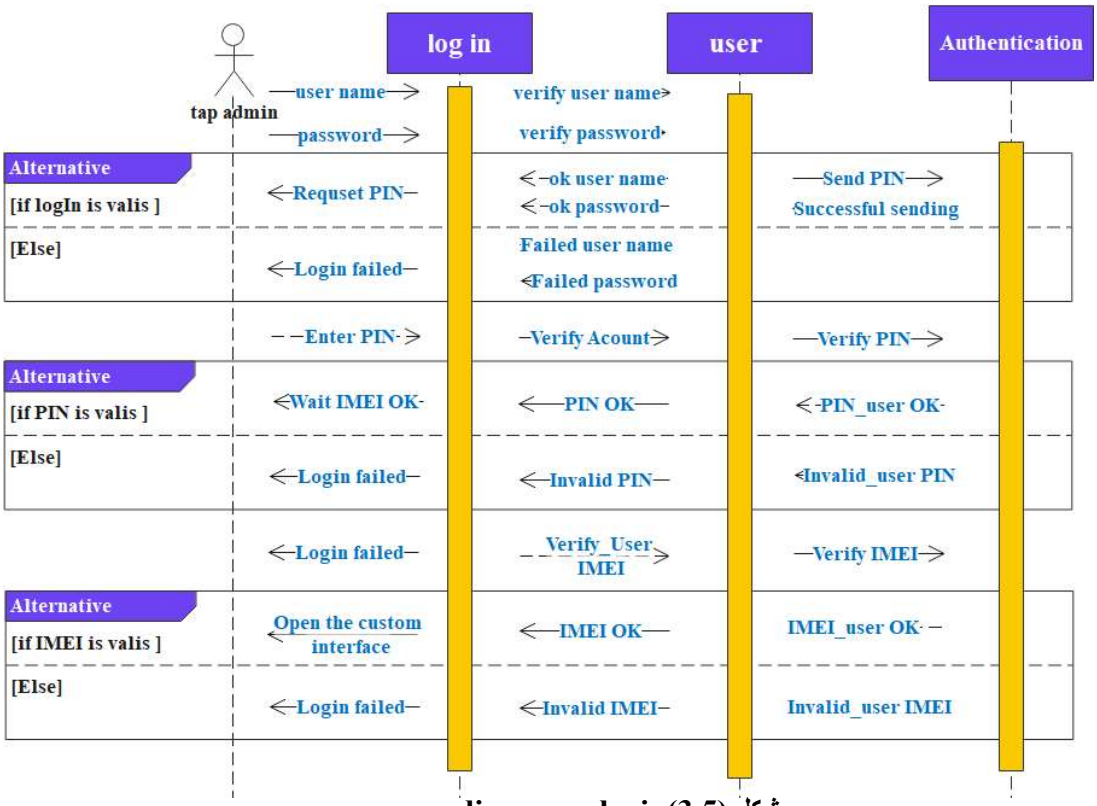

**DFD context(3.2) شكل**




**DFD Level 0 (3.3) شكل**

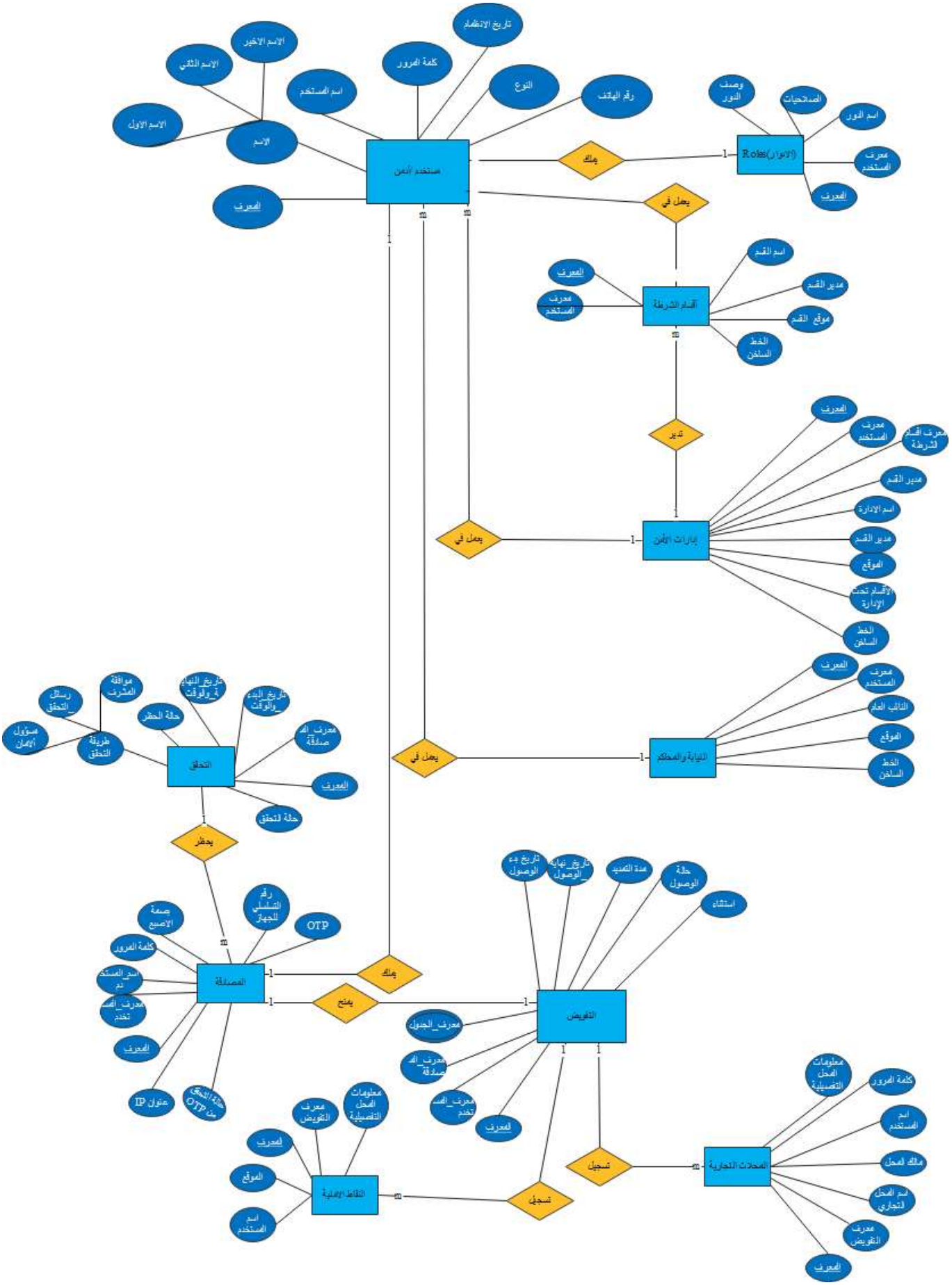


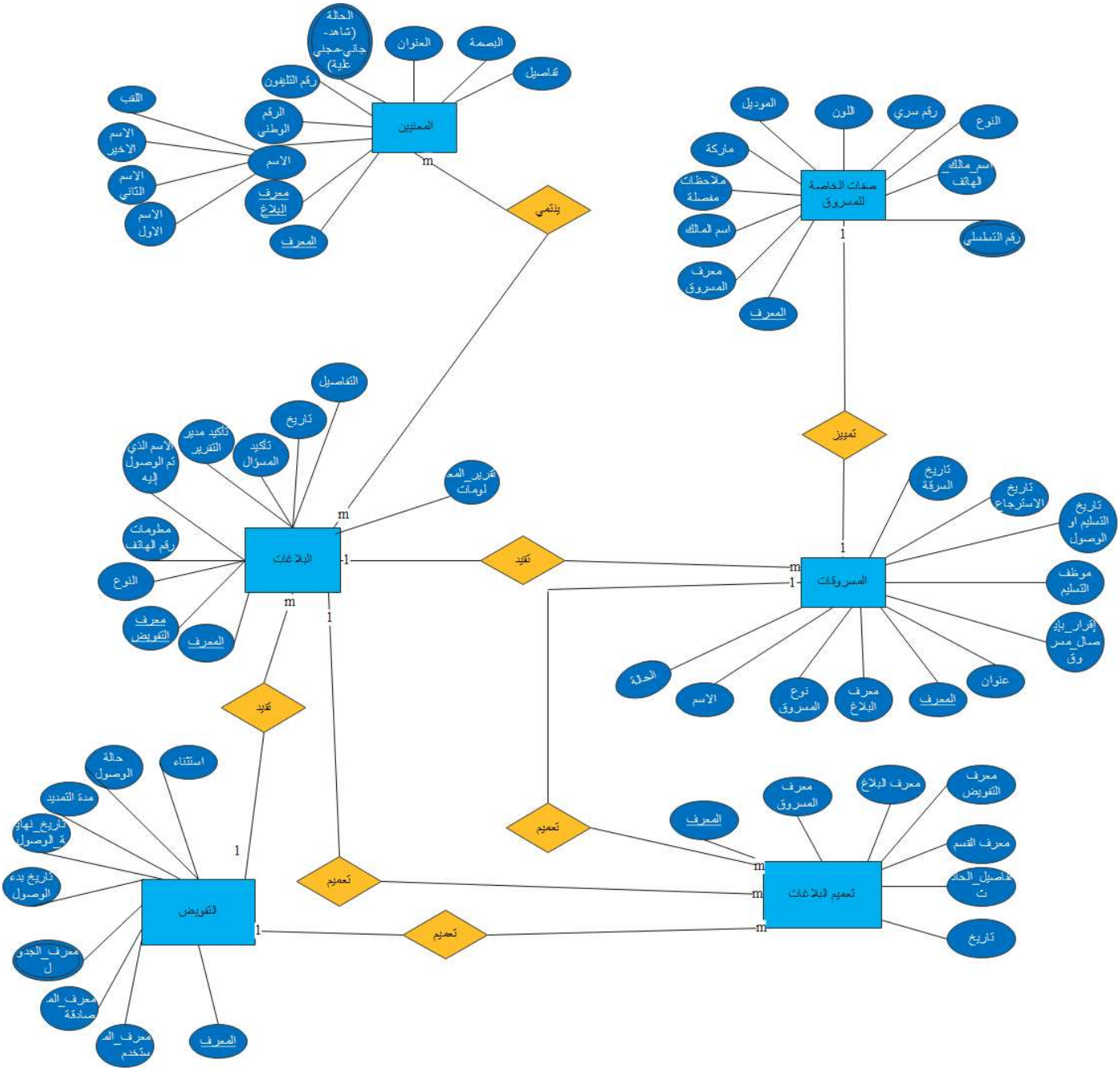

**sequence diagram :record report(3.4) شكل**




**sequence diagram : login(3.5) شكل**

## ER diagram 3.7.4






**ER diagram (3.6) شكل**

## 3.8 الخطة الأمنية لقواعد البيانات

يكون ذلك بتمكين المستخدمين ومنحهم صلاحيات وصول محددة وفقًا لاحتياجات النظام. يعمل النظام بشكل تسلسلي، حيث يتم التحقق من هوية المستخدم، ثم يتم إجراء التحقيق في حالة الفشل، ثم يتم تفويض صلاحيات الوصول وتحديد فترة الوصول، وفي النهاية يتم الوصول إلى الجداول المخصصة للمستخدم.
سيتم استخدام جدول المستخدمين لإضافة مستخدمين جدد وتحديد معلوماتهم مثل اسم المستخدم وكلمة المرور ونوع المستخدم وقاعدة الصلاحيات. ستأخذ قيم صلاحيات المستخدمين من جدول الصلاحيات، حيث يتم تعريف صلاحيات لكل قاعدة أو دور في النظام.
يتواجد أيضاً جدول المصادقة الذي يحتوي على طبقات متعددة للتحقق من هوية المستخدم. يرتبط هذا الجدول بجدول المستخدمين، حيث يتم استدعاء معلومات المستخدم للتحقق من صحته. يتضمن جدول المصادقة رمز تحقق OTP الذي يتم إرساله عبر البريد الإلكتروني في كل مرة يتم فيها تسجيل الدخول، بالإضافة إلى التحقق من بصمة الإصبع ورقم تسلسلي لجهاز المستخدم. يتم تعيين جهاز فريد لكل مستخدم يستخدمه للوصول إلى قواعد البيانات.

يتم التحقق أيضًا من عنوان IP الخاص بكل مستخدم، ويجب أن يكون فريدًا وثابتًا لكل مستخدم. في حالة محاولة الدخول ببيانات مصادقة غير صحيحة مرات متكررة، يتم إرسال إشعار للمستخدم للإشارة إلى فشل التحقق.

عندما يتم التحقق وتجاوز عدد محاولات الفشل، يتم وضع المستخدم تحت التحقيق. يتم استخدام جدول التحقيق لعزل المستخدم وحظره لفترة محدودة حتى يتم التأكد من هويته. يتم طرح أسئلة حول الصفات الشخصية للتحقق من هويته، بالإضافة إلى إرسال رمز تحقق عبر الرسائل القصيرة إلى رقم هاتفه المحمول. يتم استخدام آليات مختلفة حسب انتهاكات المستخدم، ويمكن أن يتطلب التحقق من جميع الطبقات للتأكد من صحة هويته.

بعد ذلك، يمر المستخدم بمرحلة التفويض، حيث يتم استخدام جدول التفويض لتحديد صلاحيات المستخدم للوصول إلى الجداول المحددة له. يتم تحديد فترة ووقت بدء وانتهاء الوصول، ويمكن تمديد فترة الوصول حسب الحاجة.

يجب ملاحظة أن جميع الجداول في النظام مغلقة ولا يمكن الوصول إليها مباشرة عن طريق المستخدمين أو المخترقين. الوصول إلى الجداول يتم فقط عن طريق جدول الوصول الذي يكون الجدول الوحيد الذي يحتوي على صلاحية الوصول إلى الجداول كما يوجد استثناء للجداول التي تحتاج إلى ربط، حيث يكون الجداول مقفلة ببعضها البعض، ولا يمكن الوصول إليها إلا عن طريق جدول التفويض.
تمتلك نظام البلاغات آليات متعددة للحماية والتحقق من هوية المستخدمين، بما في ذلك الأسئلة الشخصية، ورموز التحقق OTP، والبصمة الإصبعية، والرقم التسلسلي لجهاز المستخدم، وعنوان IP. يتم استخدام هذه الآليات للتأكد من صحة هوية المستخدم وحماية النظام من المحاولات غير المصرح بها.

- **السياسة الأمنية للقواعد البيانات**

سياسة الأمان لقواعد البيانات تشمل مجموعة من الإجراءات والسياسات التي تهدف إلى حماية البيانات المخزنة في قاعدة البيانات من الوصول غير المصرح به وضمان سلامتها وسرية المعلومات.

**بعض أهم جوانب سياسة الأمان لقواعد البيانات:**

1- تحديد صلاحيات الوصول يمكن ان يتم تحديد صلاحيات الوصول للمستخدمين والمشرفين بناءً على مستوى الاحتياجات والمسؤوليات. يجب أن يتم اعتماد نظام تمثيل الهوية والمصادقة للتحقق من هوية المستخدم ومنح الصلاحيات المناسبة.
2- تأمين الاتصالات يجب تأمين الاتصالات بين تطبيقات قواعد البيانات والعملاء أو الأجهزة الأخرى. يمكن استخدام بروتوكولات التشفير الآمنة مثل SSL/TLS لضمان سرية وسلامة البيانات أثناء النقل.
3- التحقق والتحقق المتعدد العوامل يجب تطبيق آليات التحقق المتعدد العوامل للتأكد من هوية المستخدمين قبل السماح لهم بالوصول إلى قاعدة البيانات. يمكن استخدام كلمات المرور القوية والرموز التحقيقية والبصمات الإصبعية وغيرها من العوامل لتعزيز الأمان.
4- تتبع النشاطات والمراقبة يجب تسجيل جميع النشاطات والعمليات في قاعدة البيانات، بما في ذلك محاولات الوصول غير المصرح بها وأنشطة التعديل والحذف. يساعد هذا التتبع في الكشف عن أي أنشطة غير مشروعة وتوفير أدلة للتحقيق في حالة وقوع انتهاك أمني.
5- نسخ احتياطي واستعادة البيانات يجب تنفيذ استراتيجية نسخ احتياطي منتظمة لقاعدة البيانات وتخزين النسخ الاحتياطية في موقع آمن. يساعد ذلك في استعادة البيانات في حالة حدوث فقدان أو تلف للمعلومات.
6- لتشفير تحدد سياسية التشفير أنواع البيانات التي يجب تشفيرها. يتم تحديد البيانات الحساسة والمعلومات الخاصة التي يجب حمايتها بواسطة التشفير.
7- تحديثات البرامج وإصلاح الثغرات يجب تطبيق التحديثات الأمنية وإصلاح الثغرات الأمنية في قاعدة البيانات والبرامج المرتبطة بها بشكل منتظم. يساعد ذلك في تقليل فرص استغلال الثغرات الأمنية ومخاطر الاختراق.
8- التعامل مع التهديدات والاستجابة الطوارئ يجب وضع إجراءات استجابة للطوارئ تتضمن كيفية التعامل مع الانتهاكات الأمنية والاختراقات المحتملة. يجب تحديد فرق الاستجابة للطوارئ وتوفير خطة لمعالجة الحوادث الأمنية وتقييم التأثير واستعادة النظام.
9- تدريب الموظفين يجب توفير تدريب منتظم للموظفين المشتركين في إدارة وصيانة قاعدة البيانات بشأن ممارسات الأمان والسياسات وإجراءات الاستجابة للطوارئ. يساعد ذلك في رفع مستوى الوعي الأمني والحد من الأخطاء البشرية.

## 3.9 الخطة الأمنية للأكواد البرمجية

تأمين الكود البرمجي هو عملية لحماية التطبيقات وقواعد البيانات من الاختراق والوصول غير المصرح به فعندما يتم اختراق الكود البرمجي، يصبح من الممكن للمهاجمين استغلال الثغرات الأمنية الموجودة في التطبيق للوصول إلى قاعدة البيانات والحصول على المعلومات الحساسة.

- **الهجمات الشائعة**

يتم تنفيذ العديد من الهجمات الشائعة مثل هجمات حقن SQL والهجمات عبر فرقة التصنيف الجانبية (XSS) والتصيد الاحتيالي (Phishing). ثغرات تجاوز المصادقة أو ثغرات تجاوز الصلاحيات، إذا لم يتم تصحيح هذه الثغرات الأمنية، فإن المهاجمين يمكنهم استغلالها والوصول إلى قاعدة البيانات والحصول على المعلومات الحساسة.

- **الفرضيات**

من خلال تأمين الكود البرمجي و استخدام لغة برمجية كائنية التوجه ، نظام البلاغات سوف يكون قادر على تجنب هذه الهجمات الشائعة وتتم حماية قاعدة البيانات من الوصول غير المصرح به وهذه بعض الفرضيات في النظام لتأمين الكود البرمجي :

- استخدام التجزئة والتجميع باستخدام الكبسولة والتجزئة (Encapsulation and Abstraction).

**النتائج المتوقعة:**

تقسيم الشفرة إلى كلاسات مستقلة تتفاعل مع بعضها البعض بواجهات محددة. هذا يسهل الصيانة وإدارة البرنامج ويقلل من فرص وجود أخطاء الأمان والثغرات.

- تنفيذ قواعد الوصول بواسطة استخدام كلاسات خاصة وتحديد صلاحيات الوصول المناسبة.

**النتائج المتوقعة:**

تنفيذ الوصول لقاعدة البيانات بتحديد الكلاسات التي تتعامل مع البيانات الحساسة ومنح صلاحيات الوصول عبر الكلاسات المناسبة للمستخدمين والأدوار.

- التحقق من صحة البيانات المدخلة من قبل المستخدمين، وأنها تتوافق مع الصيغ والقيود المتوقعة قبل تنفيذ أي عمليات على قاعدة البيانات واستخدام كلاسات خاصة لتنفيذ التحقق من صحة البيانات المدخلة قبل إجراء عمليات على قاعدة البيانات و تتضمن هذه الكلاسات التحقق من تنسيق البيانات، وفحص القيود والقواعد المنطقية، وتنفيذ إجراءات التصحيح اللازمة.

**النتائج المتوقعة:**

هذا ساعد سوف يساعد في منع هجمات حقن الشيفرة (Code Injection) والوقاية منها.

- استخدام بيانات معلمات الاستعلام (Prepared Statements) بدلاً من تضمين القيم المدخلة مباشرة في الاستعلامات.

**النتائج المتوقعة:**

ذلك يمنع هجمات حقن الشيفرة (SQL Injection)، حيث يتم تنسيق وتعامل مع المدخلات بشكل صحيح وآمن.

- سوف نطبق مبدأ الحد الأدنى لصلاحيات الوصول (Least Privilege Principle).

**النتائج المتوقعة:**

تخصيص أذونات الوصول لكل مستخدم بدقة، وتقليل الامتيازات غير الضرورية والوصول الكامل إلى البيانات.

- استخدام كلاسات خاصة لتنفيذ عمليات التشفير وفك التشفير لحماية البيانات وتخزينها ونقلها مشفرة الي قاعدة البيانات وتتضمن هذه الكلاسات وظائف لتشفير وفك تشفير البيانات باستخدام تقنيات مثل AES (Advanced Encryption Standard) أو RSA (Rivest-Shamir-Adleman).

**النتائج:**

حماية البيانات قبل نقلها او تخزينها الي قواعد البيانات مما يزيد من حماية البيانات الحساسة .

## 3.10 الخطة الأمنية للنقل البيانات عبر الشبكة

واحدة من أهم التحديات التي يواجها النظام هي ضمان أمان وسرية نقل البيانات عبر الشبكة ومن أجل تحقيق ذلك، يتم استخدام تقنيات متقدمة مثل MPLS VPN.

في سياق نظام البلاغات، يتم استخدام سيرفر لتنفيذ إجراءات التحقق والتأكد من هوية الأجهزة وصلاحيتها قبل السماح لها بالوصول إلى السيرفر الذي يحتوي على البيانات الحساسة. هذه الإجراءات تشمل التحقق من عنوان IP للأجهزة والتحقق من الأرقام التسلسلية للأجهزة المصرح بها. بالإضافة إلى ذلك، يتم استخدام سيرفر ثالث يحتوي على جداول إدارة قواعد البيانات وسجلات المراقبة والتحكم.

باستخدام هذه الإجراءات، يتم ضمان أمان نقل البيانات وحمايتها من الوصول غير المصرح به. يتم التحقق من هوية الأجهزة وصلاحيتها قبل الوصول إلى البيانات الحساسة، مما يحمي النظام ويحفظ سرية المعلومات المرسلة ويقلل من مخاطر الوصول غير المصرح به.

بالاعتماد على تقنية MPLS VPN، يتم توفير شبكة افتراضية خاصة تمامًا عبر الشبكة العامة مع تشفير حركة البيانات وعزلها عن الأجهزة غير المصرح بها. هذا يوفر أعلى مستويات الأمان والخصوصية لنقل البيانات في نظام البلاغات.

باستخدام هذه الحلول التقنية المتقدمة، يمكن تحقيق نقل آمن وموثوق للبيانات في نظام البلاغات. إن التحقق من هوية الأجهزة وصلاحيتها، إلى جانب استخدام شبكة افتراضية خاصة، يساهمان في حماية النظام والمعلومات الحساسة وضمان سرية البيانات المرسلة.

## 3.11 الخطة الأمنية للنظام بشكل عام

- **تسجيل الأحداث(Logging)** : تسجيل جميع الأحداث والأنشطة المهمة في النظام، مثل محاولات الاختراق، والوصول غير المصرح به، والأخطاء النظامية، والأنشطة الشبيهة بالتهديدات. يتم تخزين سجلات الأحداث في ملفات سجل (log files) لاحق الاستعراض والتحليل.
- **رصد الشبكة(Network Monitoring) :** استخدام أدوات رصد الشبكة لرصد حركة البيانات والاتصالات عبر الشبكة. يتم تحليل حركة الشبكة للكشف عن أنشطة مشبوهة مثل محاولات الاختراق والاعتداءات السامة. يمكن استخدام تقنيات مثل اكتشاف التسلل (Intrusion Detection) واكتشاف التسلل المتقدم (Advanced Intrusion Detection) لرصد التهديدات.
- **مراقبة الوصول(Access Monitoring) :** مراقبة وتسجيل الوصول إلى النظام والبيانات. تتبع عمليات تسجيل الدخول والخروج، والأذونات الممنوحة للمستخدمين، والتغييرات في صلاحيات الوصول. يمكن استخدام أنظمة إدارة الهوية والوصول (Identity and Access Management) لمراقبة وإدارة الوصول بشكل فعال.
- **اكتشاف التهديدات (Threat Detection) :** استخدام تقنيات اكتشاف التهديدات للكشف عن أنشطة غير مصرح بها ومشبوهة. تشمل هذه التقنيات استخدام أنظمة الكشف عن الاختراق (Intrusion Detection Systems)وأنظمة الكشف عن التهديدات المتقدمة (Advanced Threat Detection) التي تحلل السلوك وتحدد الأنماط الغير طبيعية والتهديدات المحتملة.

- **تقييم الضعف(Vulnerability Assessment) :** إجراء تقييم دوري للنظام لتحديد الثغرات والضعف في التهديدات الأمنية المحتملة. استخدام أدوات تقييم الضعف للفحص والاختبار وتحليل النظام وتحديد الثغرات التي يمكن استغلالها من قبل المهاجمين.

- **التحليل الأمني(Security Analytics) :** استخدام تقنيات التحليل الأمني لتحليل البيانات والسجلات واكتشاف الأنماط والتهديدات الجديدة. يمكن استخدام تقنيات التعلم الآلي والذكاء الاصطناعي لتحليل البيانات الكبيرة والكشف عن تهديدات أما بالنسبة للطرق المستخدمة في مراقبة الأمان في النظام، فإليك بعض الأمثلة الإضافية التي يمكن استخدامها:

1. **رصد السجلات الأمنية(Security Log Monitoring)** : مراقبة سجلات الأمان والمراقبة في النظام بحثًا عن أنشطة غير معتادة أو مشتبه بها. تحليل السجلات الأمنية لتحديد التهديدات المحتملة وتقديم إشعارات للمسؤولين الأمنيين لاتخاذ إجراءات مناسبة.

**2. رصد السلامة(Safety Monitoring)** : رصد السلامة لضمان سلامة النظام ومكوناته. يشمل ذلك رصد الأداء والاستجابة والاستخدام الصحيح للموارد، والتحقق من سلامة البرامج والتطبيقات، والكشف عن أية حالات غير طبيعية أو مشكلات في النظام.

3. **رصد التهديدات الخارجية (External Threat Monitoring)**: رصد التهديدات الأمنية القادمة من خارج النظام، مثل هجمات الاختراق والهجمات الموزعة من الخدمة (DDoS) والبرمجيات الخبيثة. استخدام أدوات مثل أنظمة الكشف عن الاختراق الخارجي (External Intrusion Detection Systems)وأنظمة الحماية من الهجمات الموزعة (DDoS Protection Systems) لرصد ومعالجة هذه التهديدات.

4. **التحقق من الامتثال(Compliance Monitoring)** : مراقبة الامتثال للمعايير الأمنية والتشريعات المعمول بها في المؤسسة. التحقق من مطابقة النظام لمتطلبات الأمان والخصوصية والتزامات القوانين المعمول بها، وتقديم تقارير وإشعارات في حالة وجود انتهاكات أمنية.

# الفصل الرابع :التصميم

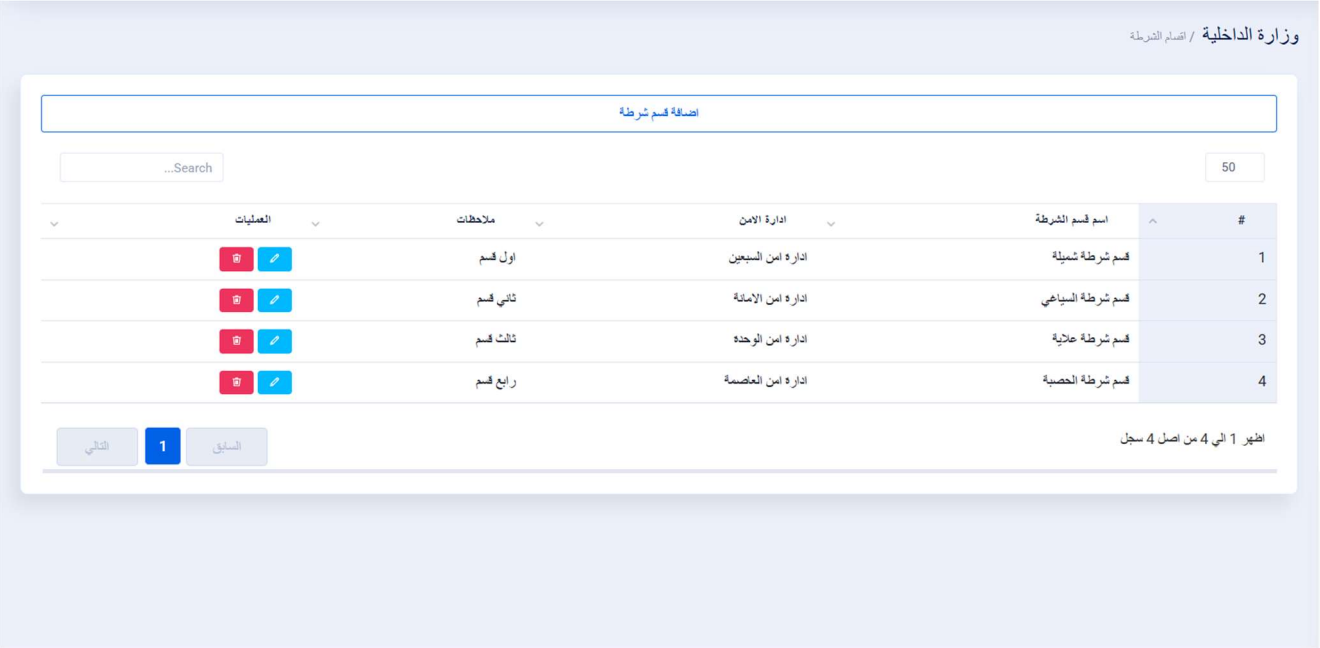
## 4.1 مقدمة

في هذا القسم، سيتم عرض الواجهات الرسومية لنظام البلاغات الأمني، والتي تم تصميمها لتكون بسيطة وسهلة الاستخدام بهدف تسهيل عملية تقديم البلاغات ومتابعتها من قبل المستخدمين. تم تصميم الواجهات مع مراعاة تجربة المستخدم وسلاسة التفاعل، كما روعي فيها وضوح العناصر وسرعة الوصول إلى الوظائف الأساسية للنظام.

## 4.2 الواجهات

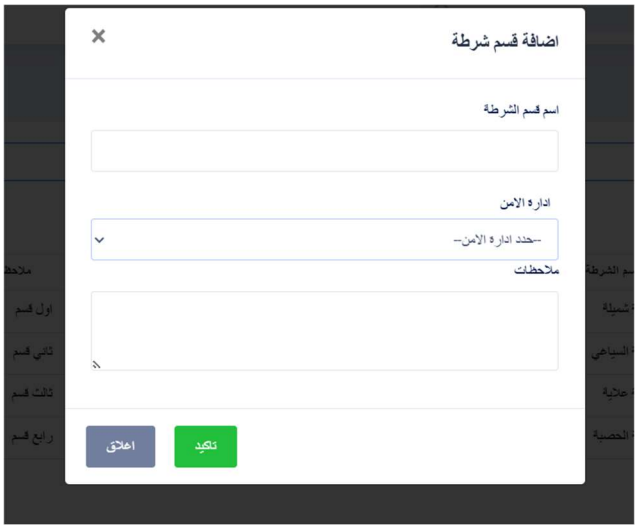
### 4.2.1 واجهات نظام البلاغات

1. واجهة أقسام الشرطة : يتم فيها إدارة أقسام الشرطة



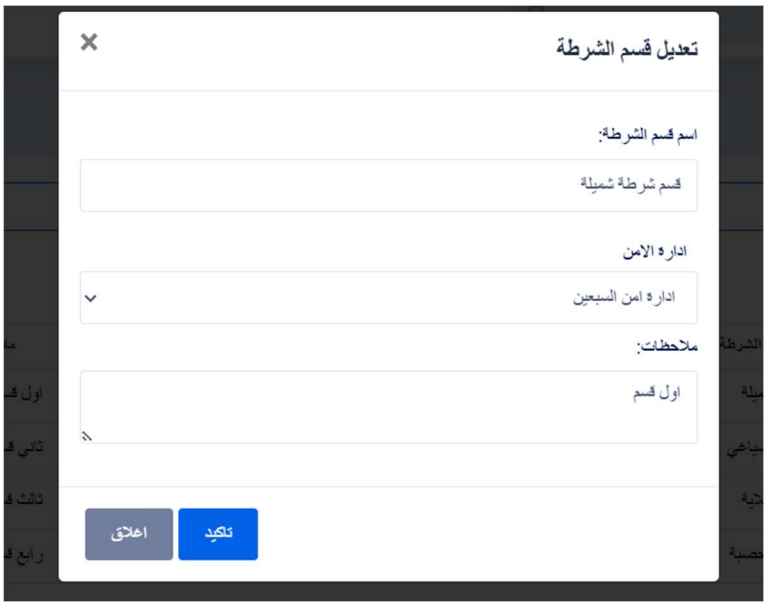

شكل (4.1) واجهة إدارية لإدارة وتنظيم أقسام أو وحدات الشرطة المختلفة.

2. إضافة أقسام الشرطة




**شكل (4.2) واجهة لإضافة قسم شرطة جديد، تتضمن حقولاً لاسم القسم ومديره وملاحظات، مع زري "حفظ" و "إلغاء".**

3. تعديل على أقسام الشرطة

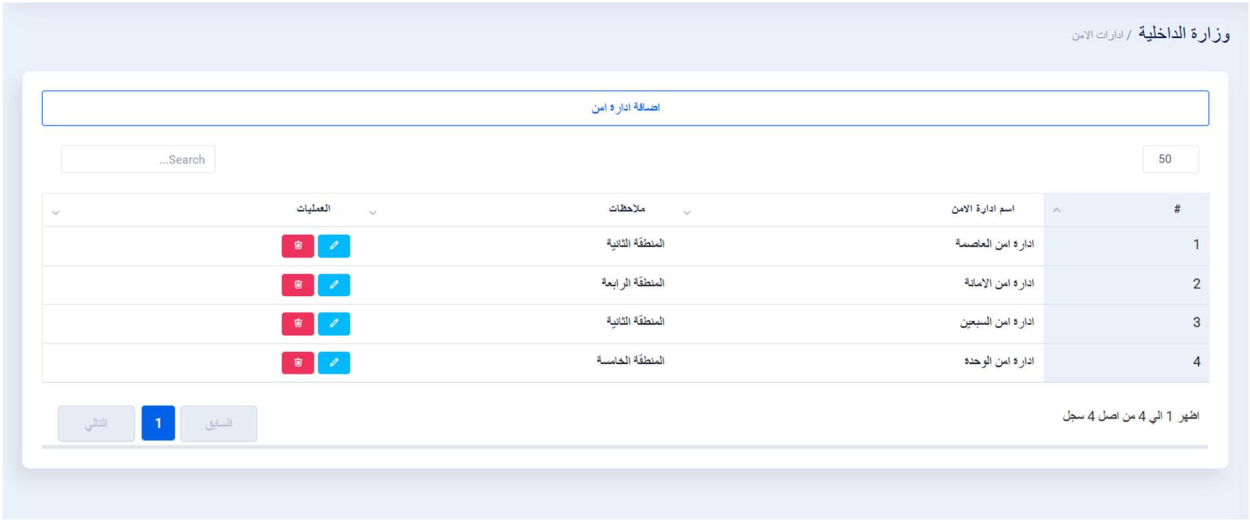



**شكل (4.3) واجهة لتعديل بيانات قسم شرطة حالي، مع حقول لاسم القسم ومديره وملاحظاته، وأزرار للحفظ أو الإلغاء.**

4. حذف قسم الشرطة

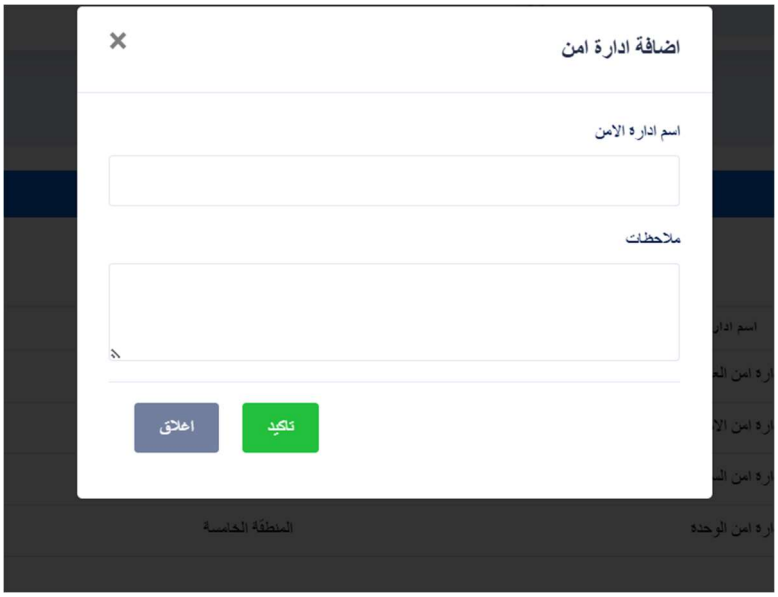

**شكل (4.4) نافذة تأكيد حذف القسم.**

5. واجهه إدارات الأمن : يتم فيها إدارة إدارات الأمن .



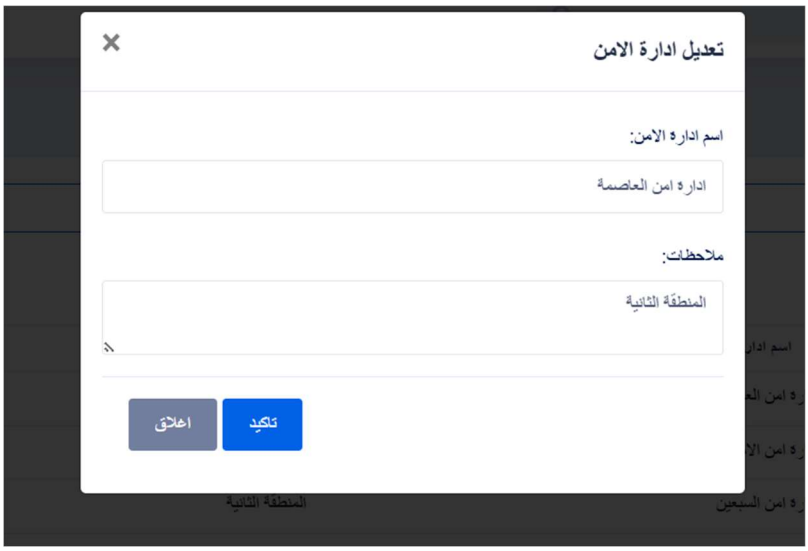

**شكل (4.5) قائمة إدارات الأمن.**

6. إضافة إدارة الأمن




**شكل (4.6) واجهة لإدخال اسم إدارة الأمن وملاحظات عنها.**

7. تعديل على إدارة الأمن

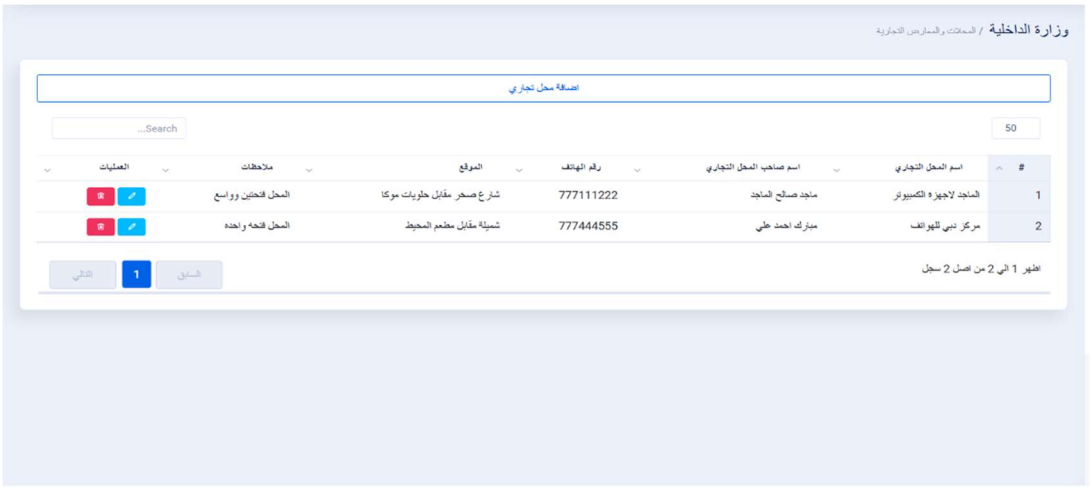



**شكل (4.7) واجهة تعرض حقولاً لتعديل اسم إدارة الأمن ("إدارة أمن المخصصة") وملاحظاتها ("المنطقة الثانية")**

8. حذف إدارة الأمن

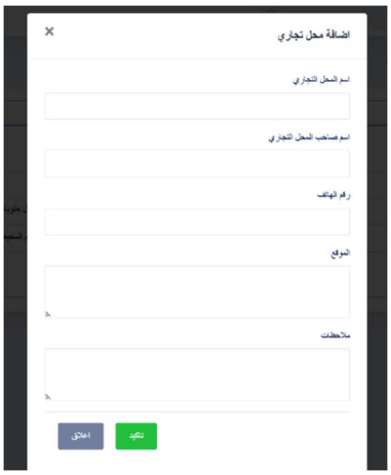

**شكل (4.8) إجراء أمان قياسي للتأكد من أن المستخدم ينوي بالفعل إزالة إدخال إدارة الأمن.**

9. واجهه المحلات التجارية :يتم فيها إدارة المحلات التجارية.



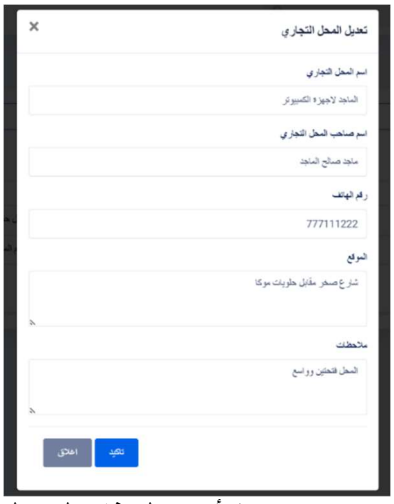

**شكل (4.9) واجهة تعرض قائمة بالمحلات التجارية الموجودة مع تفاصيل مثل اسم صاحب المحل، رقم الهاتف، الموقع، وملاحظات.**

10. إضافة المحلات التجارية




**شكل (4.10) واجهة تحتوي على نموذج (فورم) لإدخال بيانات محل تجاري جديد.**

11.تعديل على المحلات التجارية

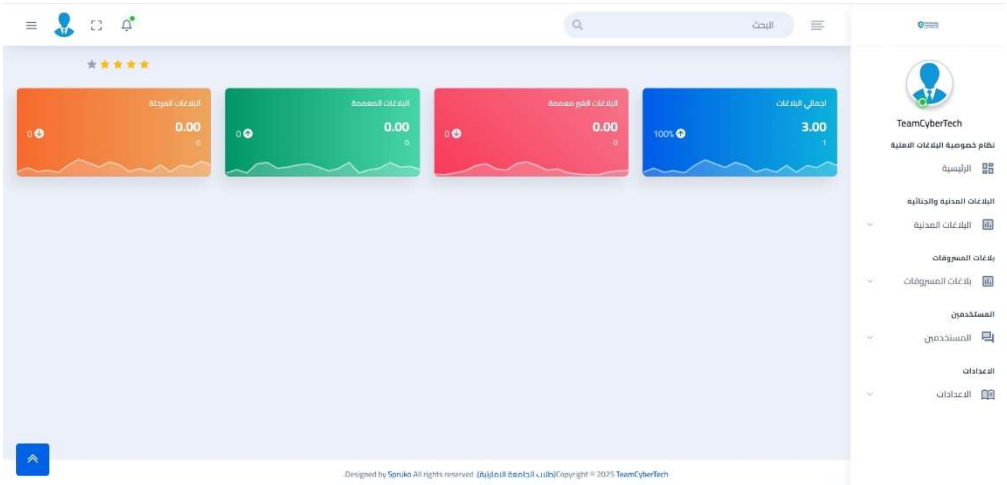



**شكل (4.11) واجهة مستخدم تتيح تحديث أو تعديل تفاصيل محل تجاري موجود، بما في ذلك بيانات المالك، رقم الهاتف، والموقع، وهي عملية نموذجية في أنظمة إدارة الأعمال أو السجلات التجارية.**

12. حذف المحلات التجارية

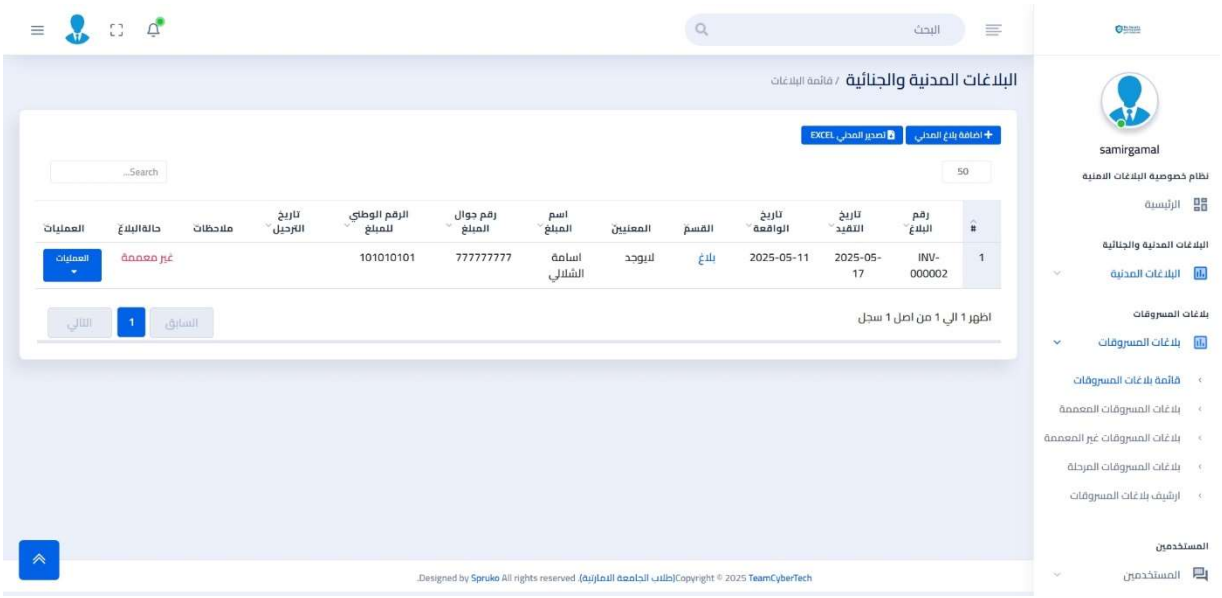

**شكل (4.12) الصورة تعرض خطوة تأكيد حذف ضمن نظام لإدارة المحلات التجارية، حيث يطلب النظام من المستخدم تأكيد رغبته في حذف عنصر معين يُسمى "إدارة الأمن"**

13. لوحة التحكم الرئيسية للبلاغات



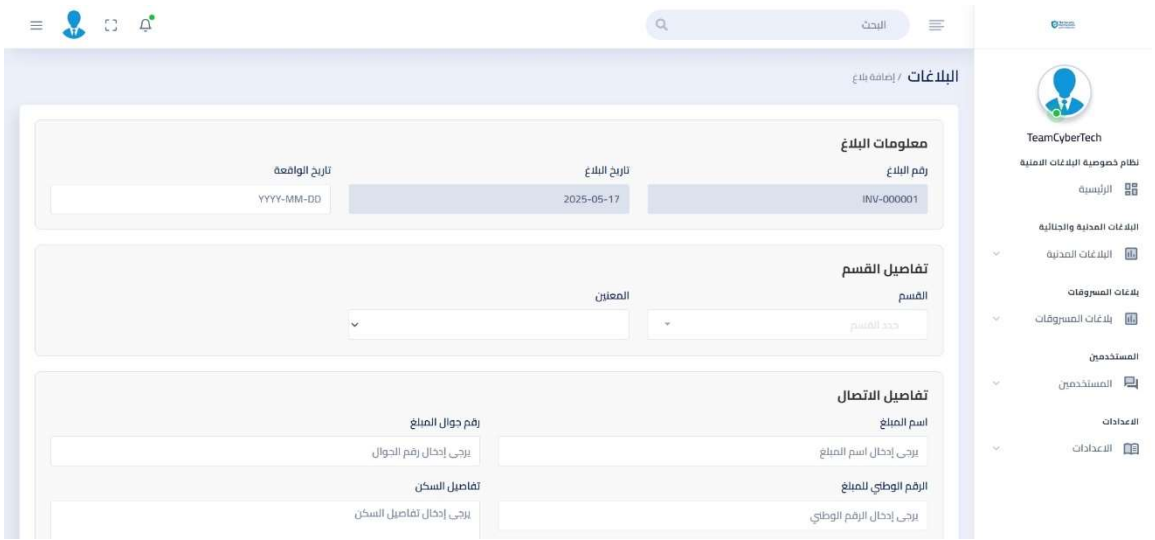

**شكل (4.13) لوحة تحكم لإدارة أنواع مختلفة من البلاغات، وتقدم نظرة سريعة على حالتها الحالية (مفتوحة، قيد المعالجة، مكتملة، جديدة) ضمن نظام تم تطويره بواسطة "TeamCyberTech". وهي مصممة لمنح المسؤولين أو المستخدمين فهمًا فوريًا لحجم عمل البلاغات.**

14.قائمة البلاغات



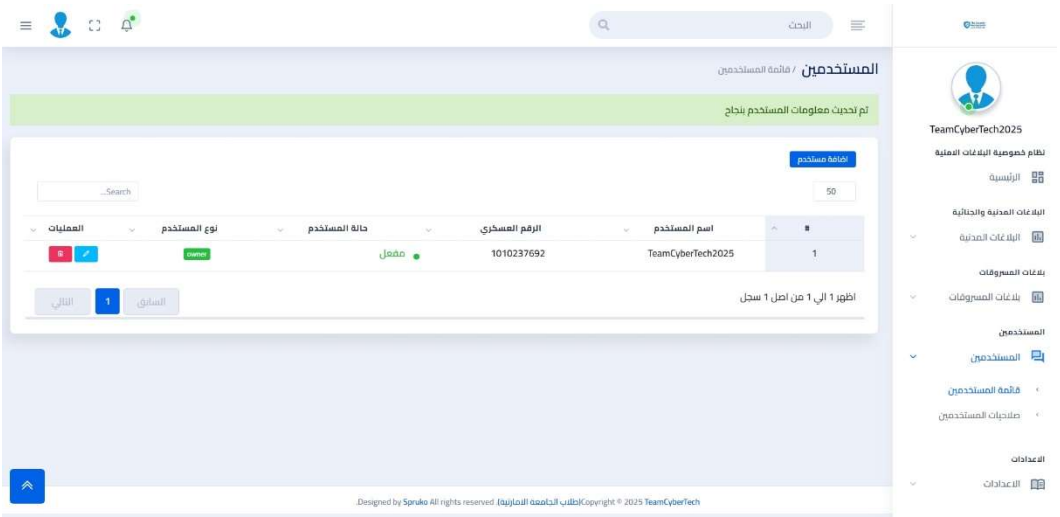

**شكل (4.14) لوحة تحكم مصممة لتمكين مسؤول أو مستخدم مخول من عرض وتتبع وإدارة مختلف البلاغات أو الشكاوى.**

15. واجهة إضافة البلاغات



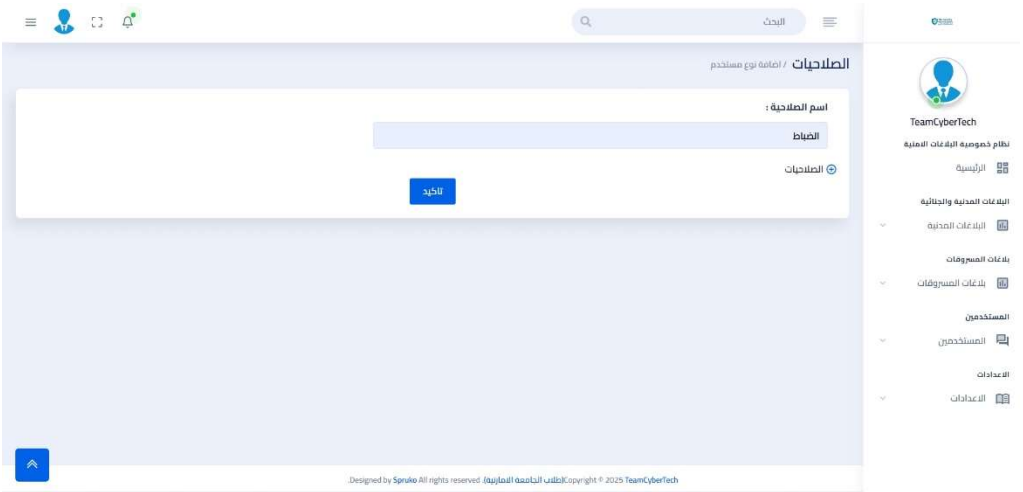

**شكل (4.15) أداة لمستخدمي النظام لتقديم بلاغات أو تقارير جديدة بشكل منظم، من خلال ملء التفاصيل ذات الصلة بالحادثة أو الموضوع المبلغ عنه.**

16.واجهة المستخدمين



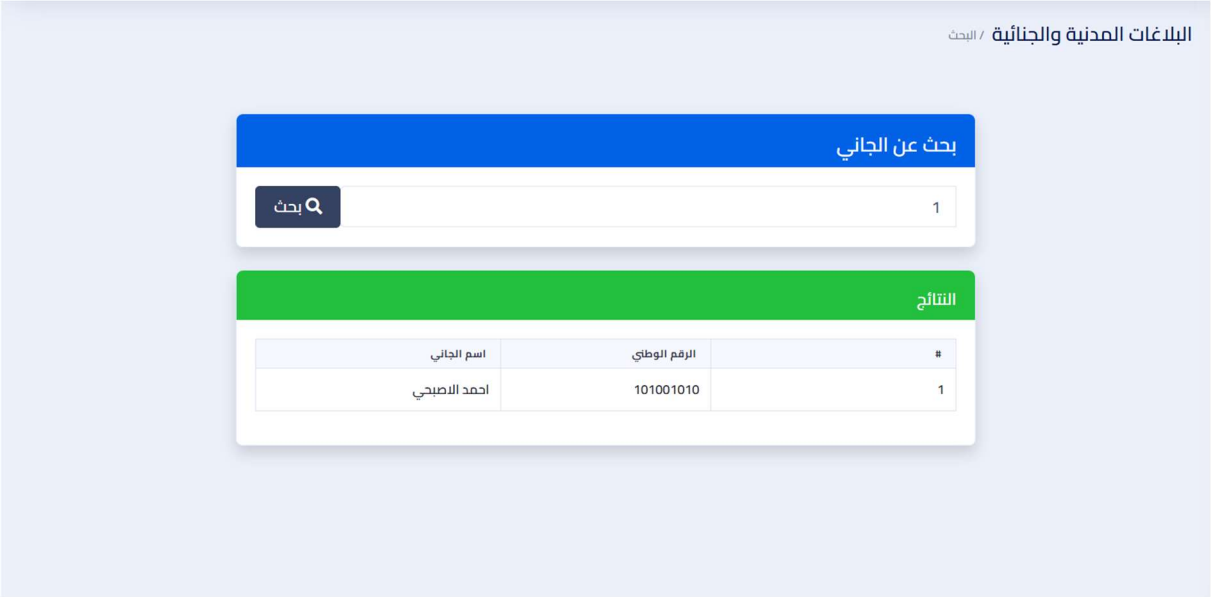

**شكل (4.16) أداة لمسؤولي النظام لإدارة حسابات المستخدمين، وعرض تفاصيلهم، وتنفيذ إجراءات عليهم، وتأكيد نجاح عمليات الإضافة.**

17. واجهة إنشاء Role جديد



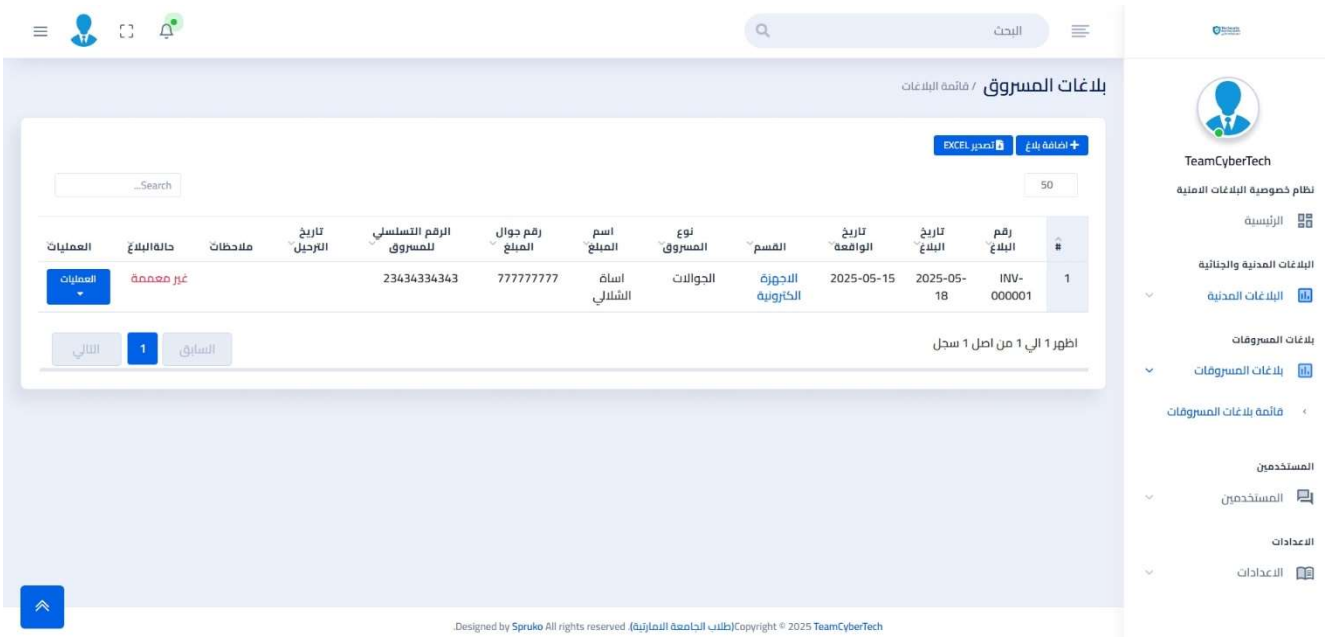

**شكل (4.17) أداة للمسؤولين لتعريف وتخصيص صلاحيات وأدوار مختلفة للمستخدمين.**

18. واجهة الاستعلام عن البلاغات




**شكل (4.18) واجهة حث ضمن نظام بلاغات، مصممة خصيصًا للبحث عن معلومات حول الأفراد المصنفين كجناة/متهمين بناءً على معايير مثل رقمهم الوطني والاسم، على الأرجح للبلاغات المدنية والجنائية.**

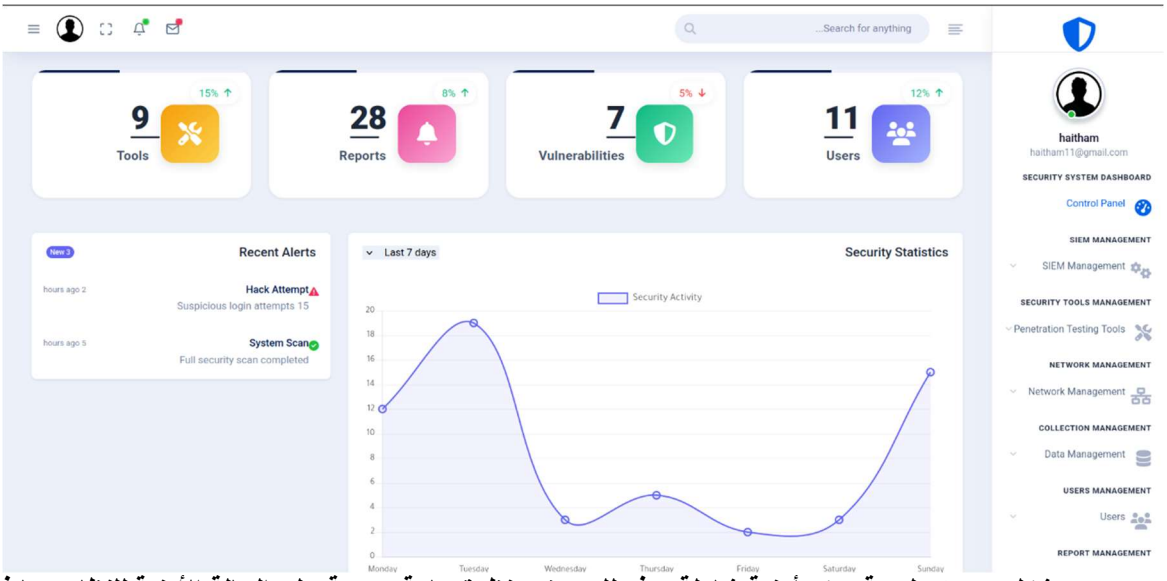
19.واجهة المسروقات




**شكل (4.19) الواجهة تتيح للمستخدمين عرض وإدارة بلاغات/تقارير متعلقة بالمسروقات، مع تفاصيل مثل التواريخ، والمسؤولين، وحالات البلاغات.**

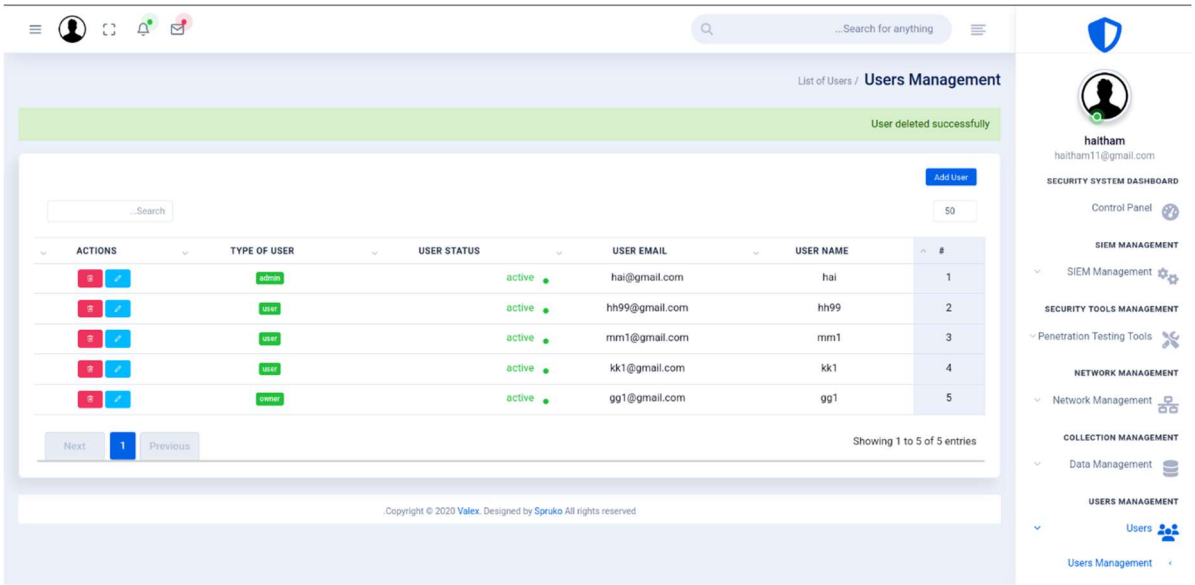
### 4.2.2 واجهات نظام الامني

1. لوحة التحكم الأمنية



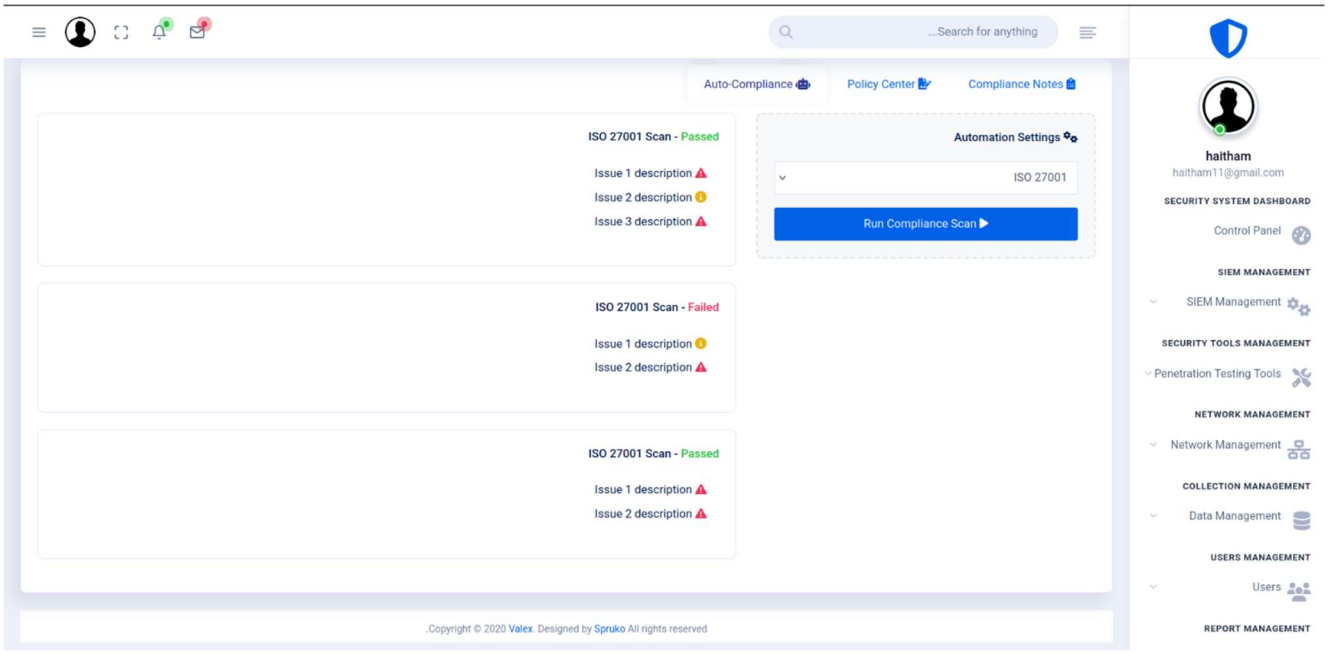

**شكل (4.20) لوحة تحكم أمنية شاملة توفر للمستخدم نظرة عامة سريعة على الحالة الأمنية للنظام، بما في ذلك أعداد الأدوات والتقارير والثغرات والمستخدمين، بالإضافة إلى أحدث التنبيهات ورسم بياني لنشاط الأمان بمرور الوقت.**

2. واجهة إدارة المستخدمين



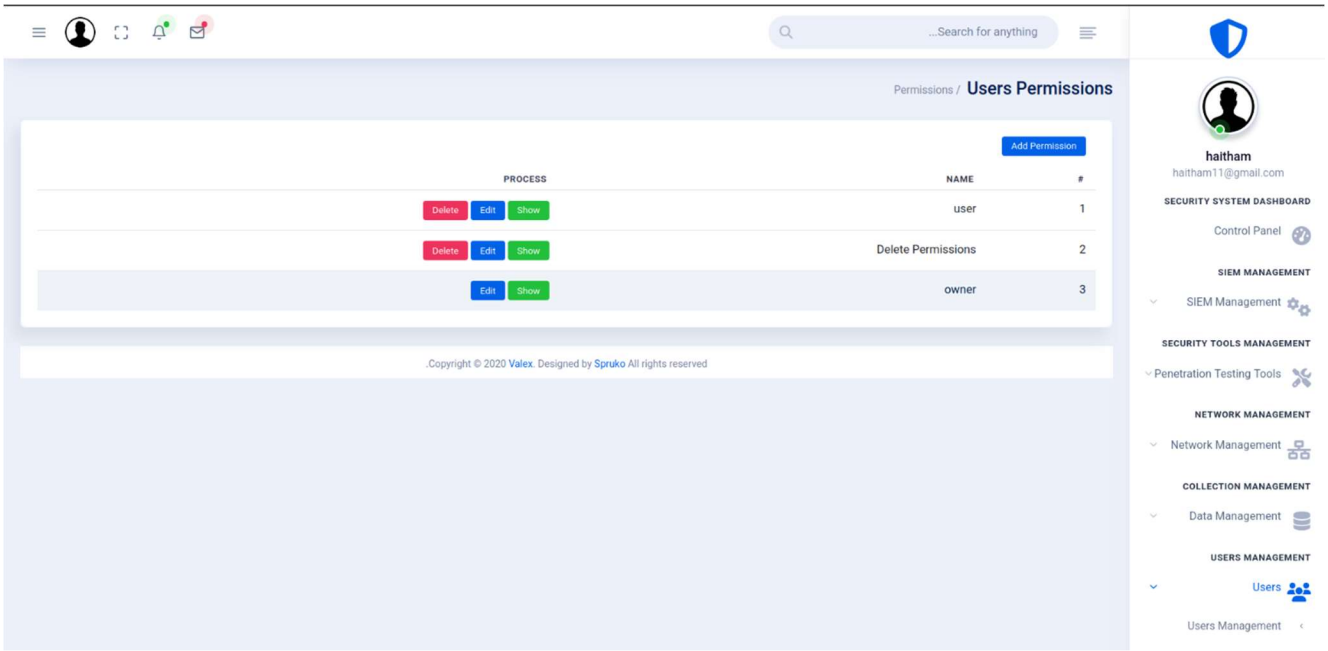

**شكل (4.21) واجهة إدارة مستخدمين مباشرة تسمح للمسؤولين بعرض وإضافة وتنفيذ إجراءات (مثل الحذف أو التعديل) على حسابات المستخدمين**

3. ادارة سياسة الامتثال للأصول



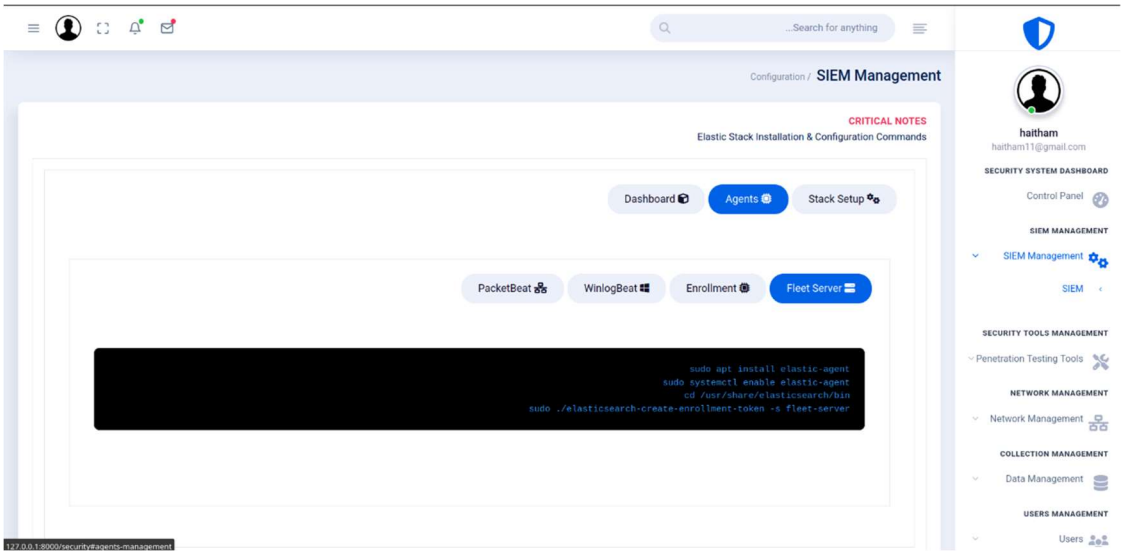

**شكل (4.22) نظامًا مصممًا لمساعدة المؤسسات في الحفاظ على الامتثال للمعايير مثل ISO 27001 عن طريق إجراء فحوصات آلية، والإبلاغ عن المشكلات، وتوفير خيارات لإعادة تشغيل الفحوصات.**

4. إدارة صلاحيات المستخدم



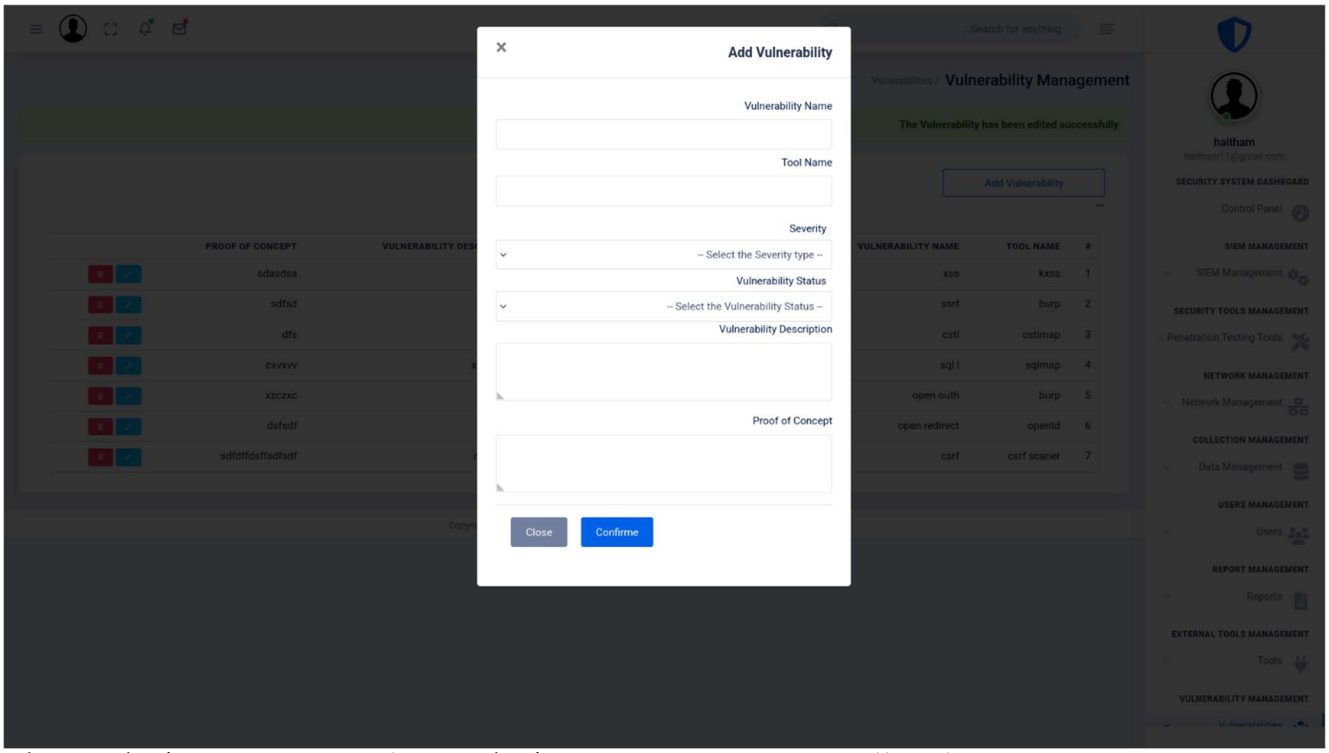

**شكل (4.23) إدارة والتحكم في الصلاحيات الممنوحة للمستخدمين داخل النظام.**

5. اضافة ايجنت للSIEM



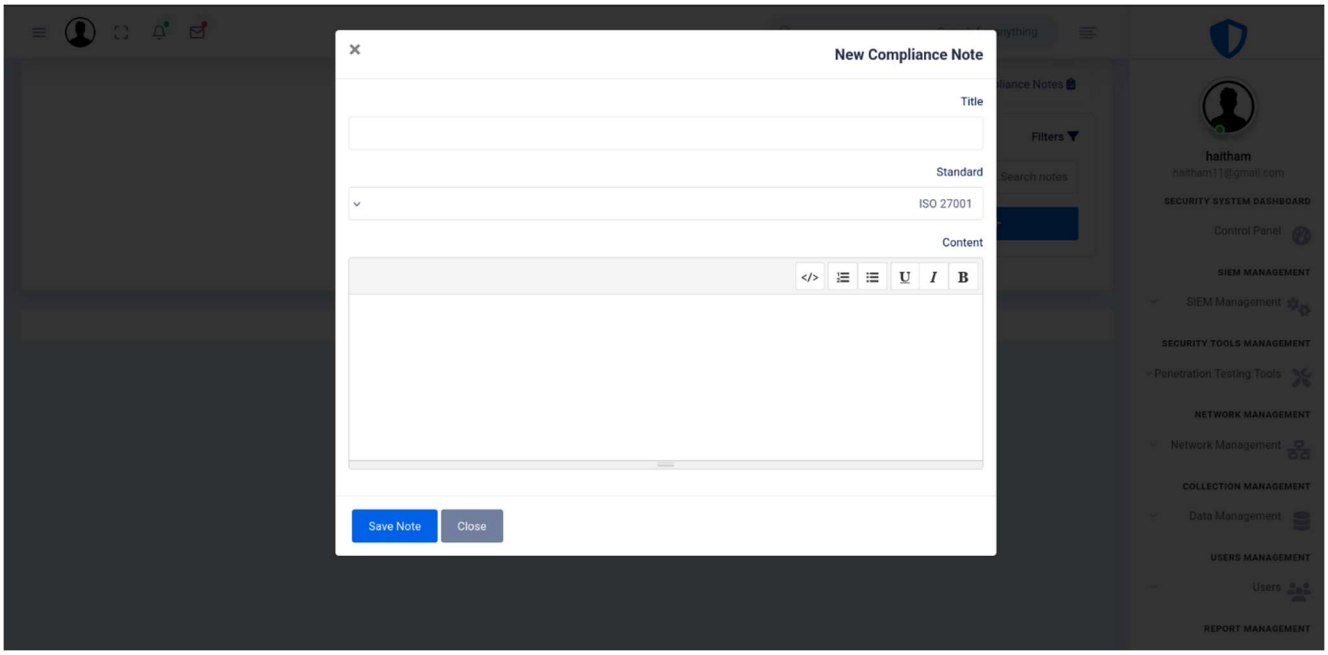

**شكل (4.24) واجهة مستخدم لإدارة SIEM، مع التركيز بشكل خاص على عملية نشر وتكوين الوكلاء لجمع البيانات، وعلى الأرجح باستخدام مكونات من Elastic Stack**

6. اضافة ثغره تم اكتشافها



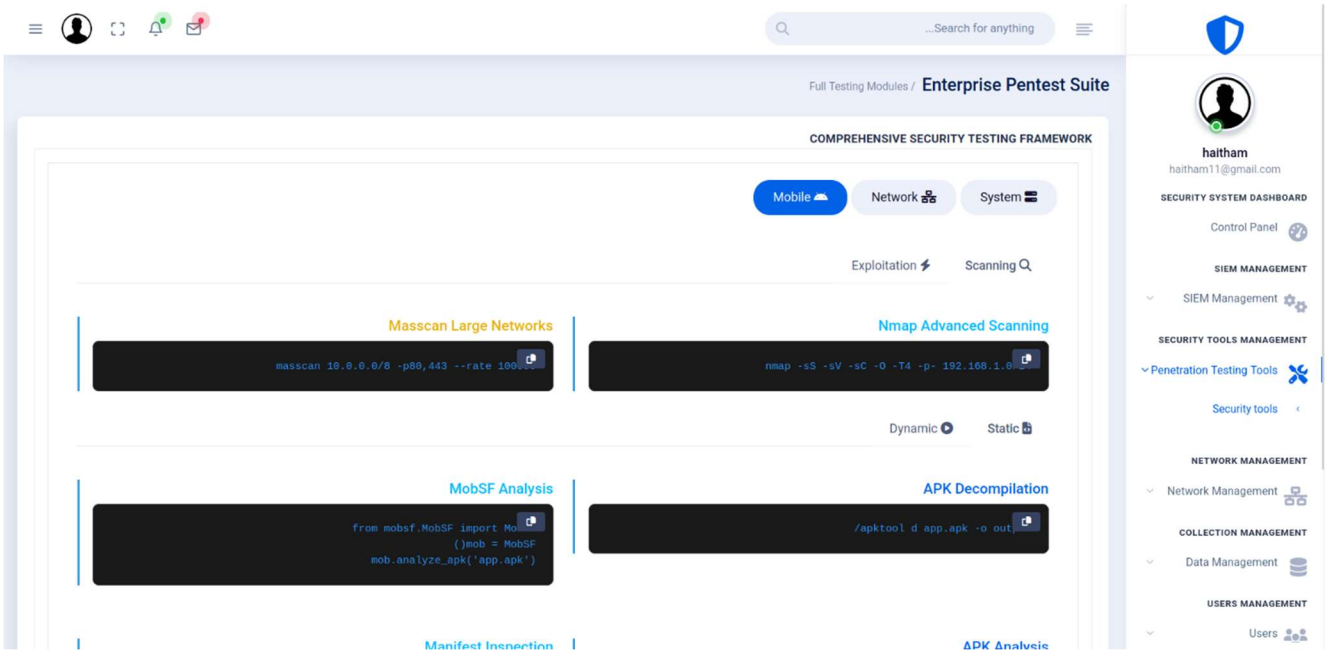

**شكل (4.25) تسمح هذه النافذة للمستخدم بإدخال تفاصيل ثغرة أمنية تم اكتشافها( توثيق الثغرات الأمنية المكتشفة في النظام)**

7. اضافة ملاحظة للامتثال الأمني



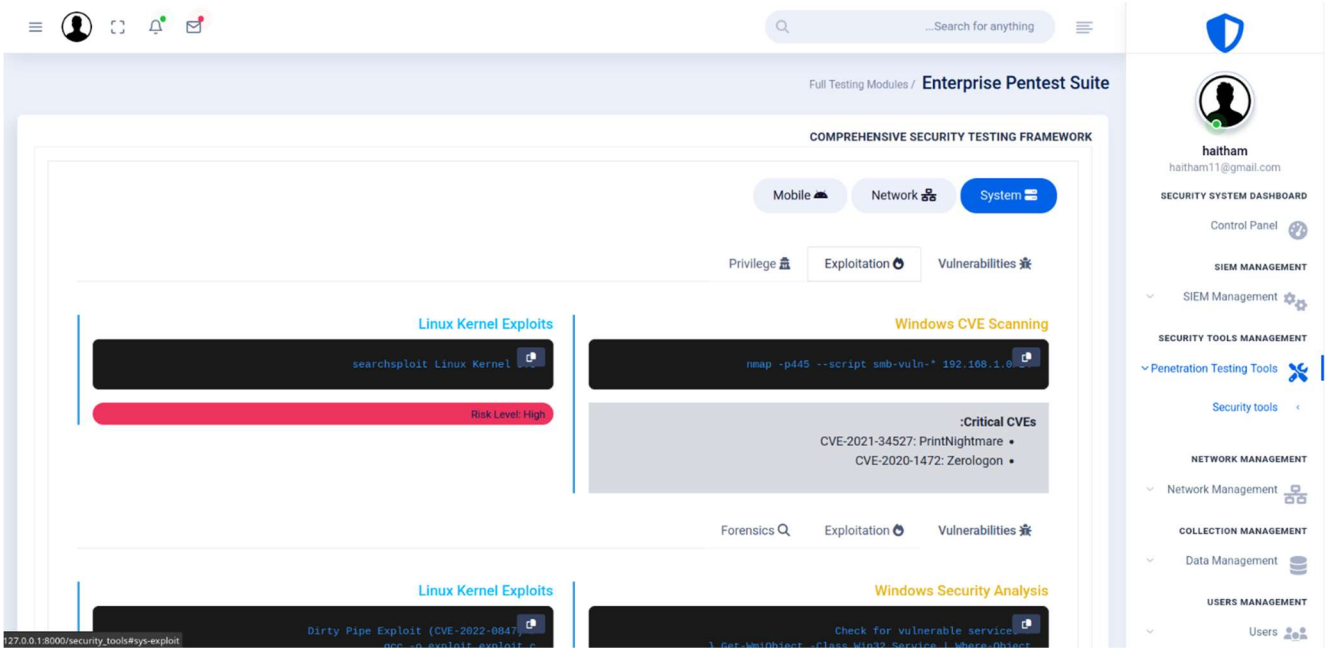

**شكل (4.26) توثيق الملاحظات أو الإجراءات أو التفاصيل المحددة المتعلقة بمدى التزام المنظمة بالمعايير الأمنية.**

8. الأدوات الرسمية والمعترفة لاختبار الاختراق الموبايل



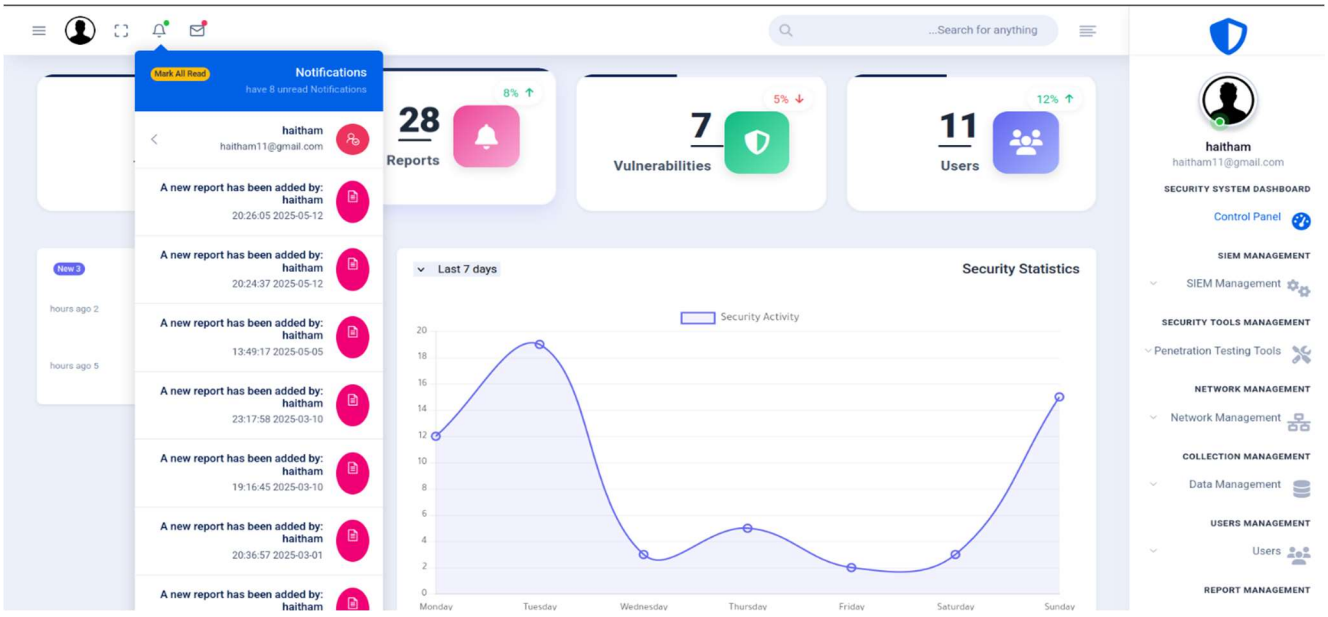

**شكل (4.27) أدوات وتقنيات اختبار الاختراق المخصصة للأجهزة المحمولة ضمن إطار " Comprehensive Security Testing Framework" (إطار عمل اختبار الأمن الشامل).**

9. الأدوات الرسمية والمعترفة لاختبار الاختراق أنظمة التشغيل



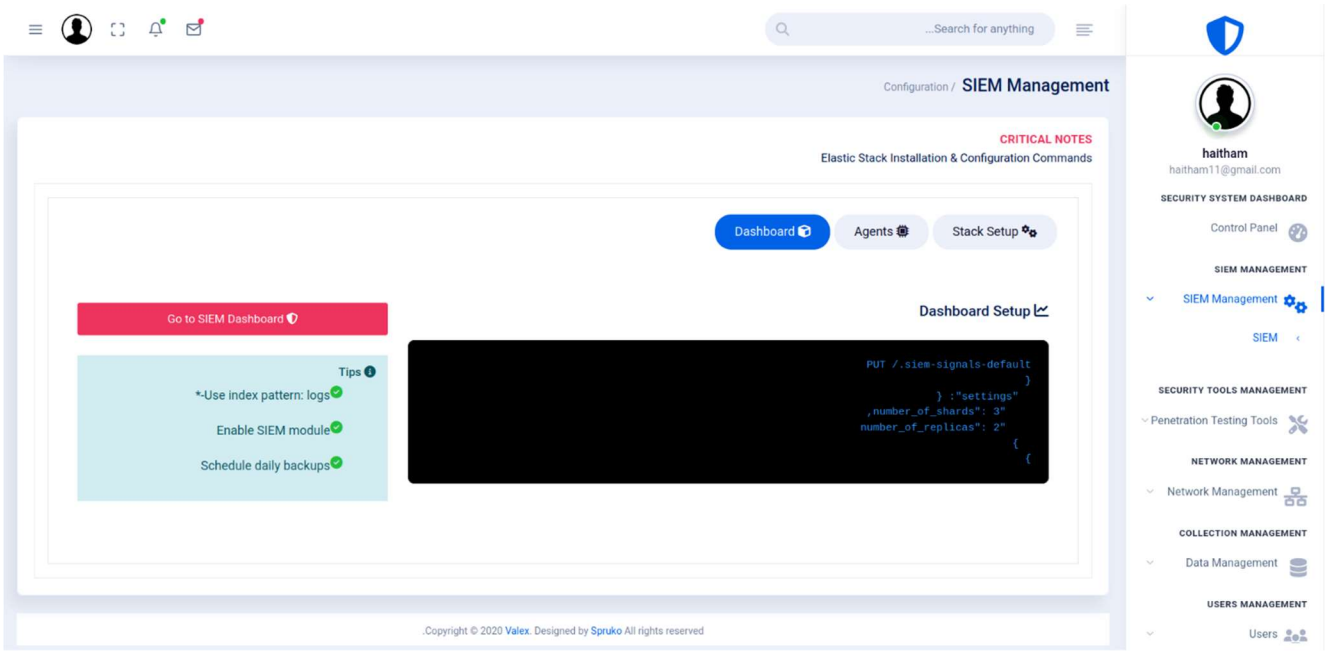

**شكل (4.28) أقسامًا لتصنيف أدوات الاختبار حسب نوع الهدف (Mobile, Network, System) وحسب نوع الهجوم (Privilege, Exploitation, Vulnerabilities). توجد أمثلة لأدوات أو أوامر لاكتشاف استغلالات نواة لينكس (Linux Kernel Exploits) وفحص ثغرات ويندوز (Windows CVE Scanning)، بالإضافة إلى ذكر ثغرات حرجة (Critical CVEs).**

10.الاشعارات



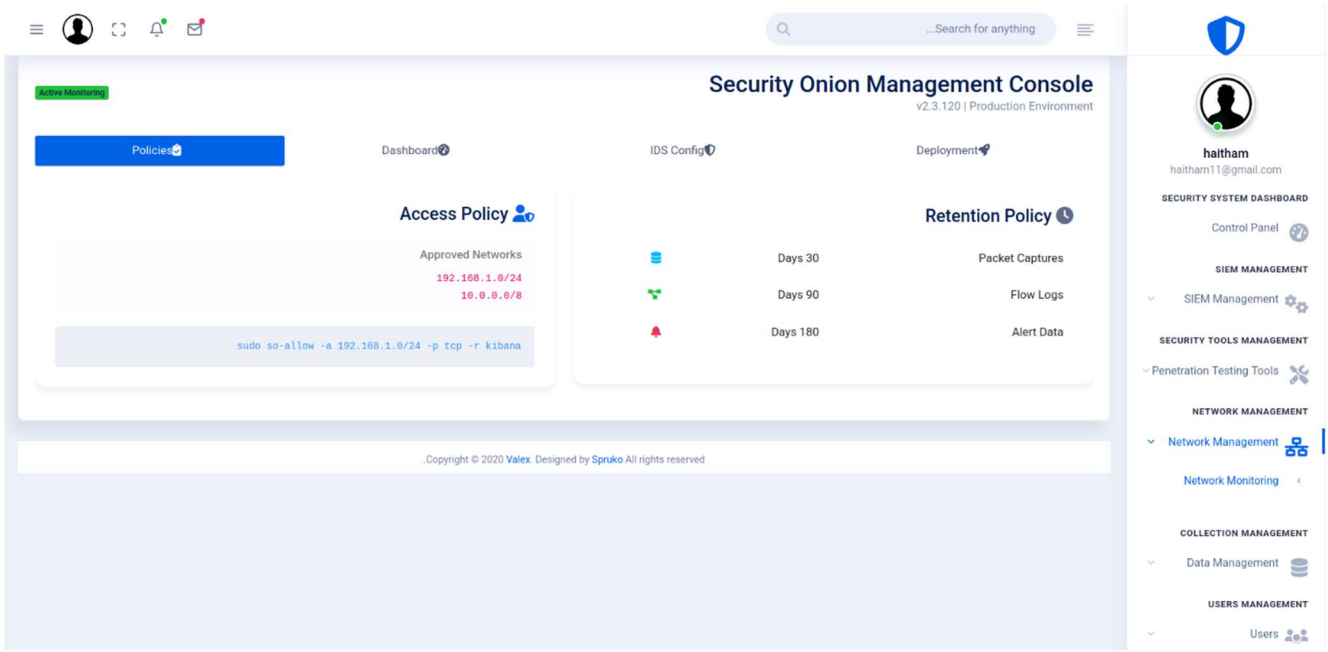

**شكل (4.29) عرض إحصائيات علوية سريعة لعدد التقارير ، الثغرات الأمنية ، والمستخدمين.**

11.الوصول الى SIEM Dashboard



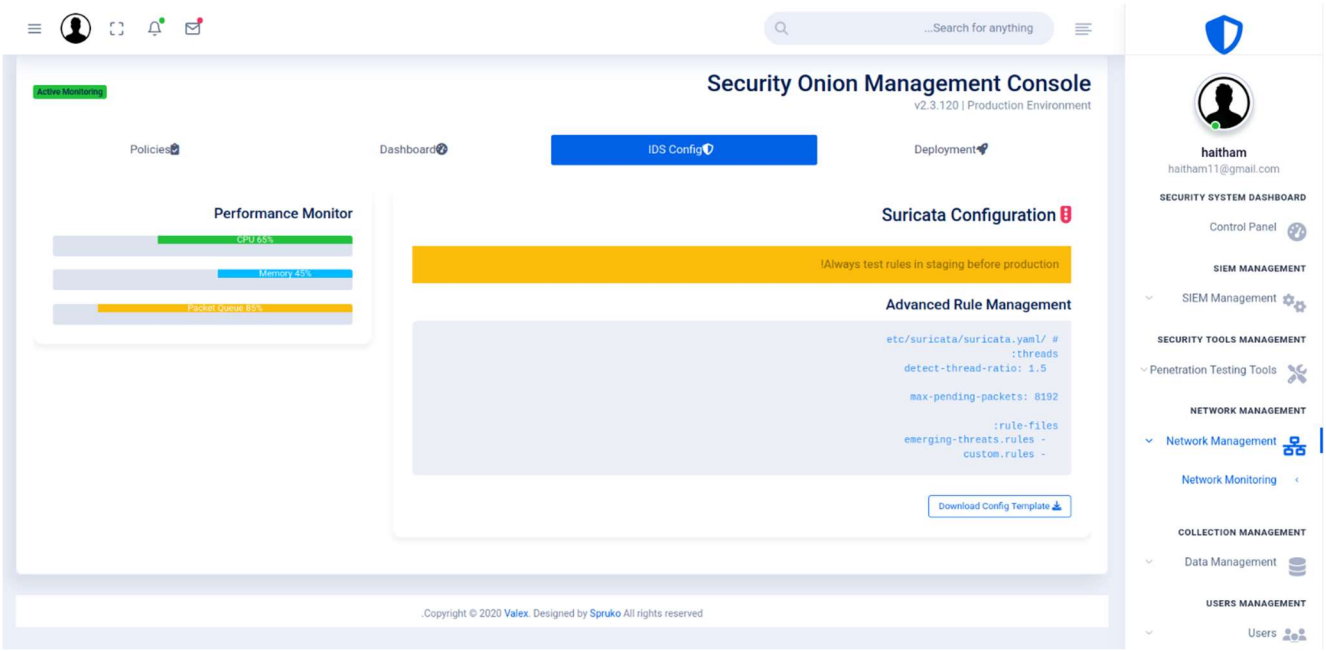

**شكل (4.30) لوحة تحكم إدارة معلومات وفعاليات الأمن.**

12.امنية وإدارة تهديدات الشبكة



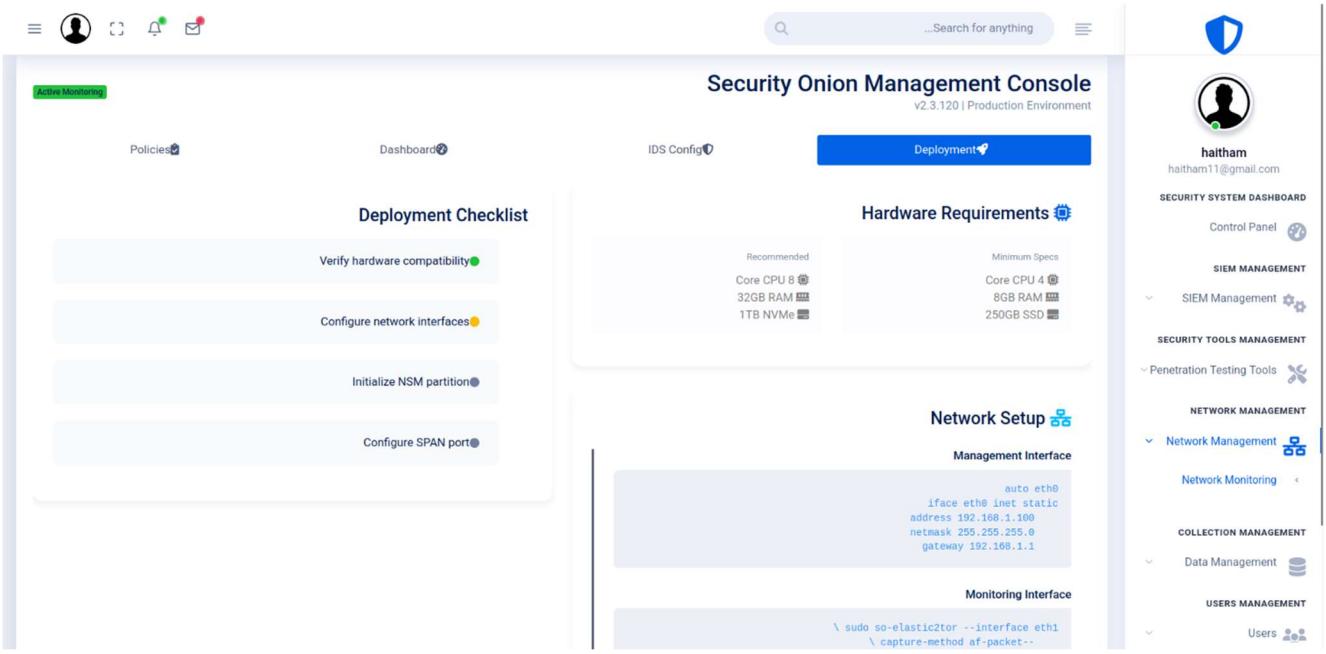

**شكل (4.31) مراقبة حركة مرور الشبكة، واكتشاف التهديدات، وإدارة سياسات الأمان، مع التركيز على الاحتفاظ بالبيانات والتحكم في الوصول إلى الشبكة.**

الاعدادات



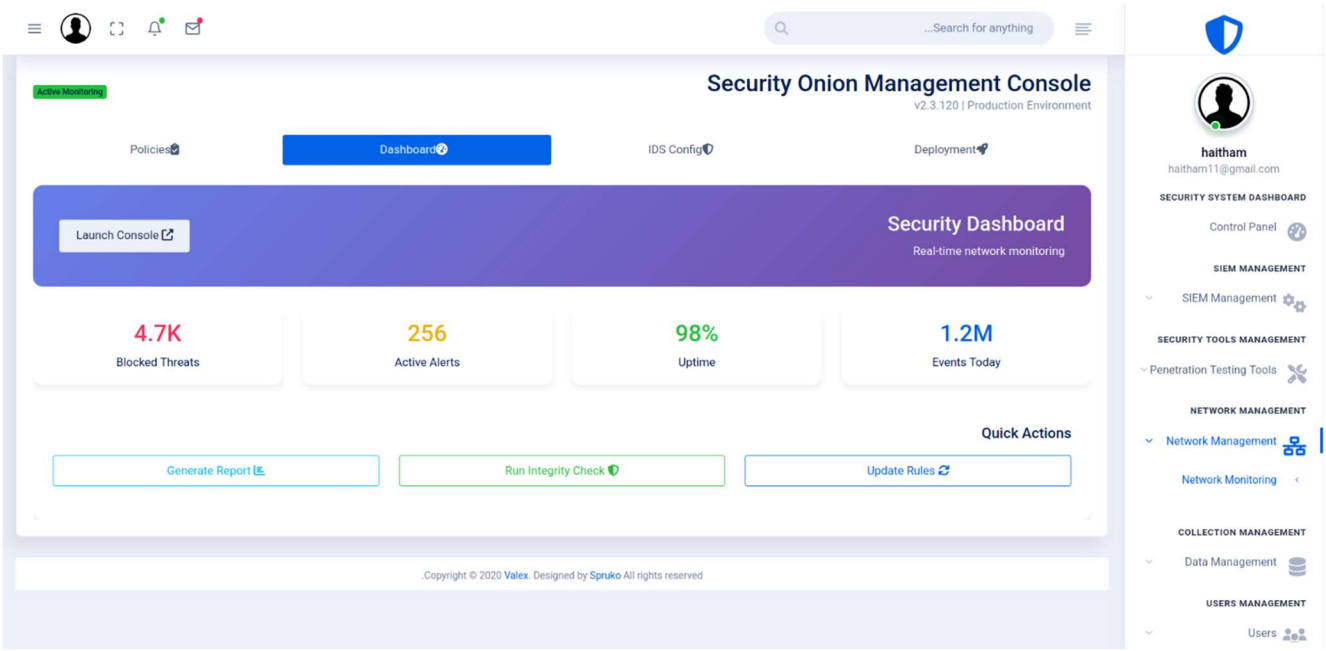

**شكل (4.32) امنية وإدارة تهديدات الشبكة (إعدادات)**

الملاحظات والتطوير



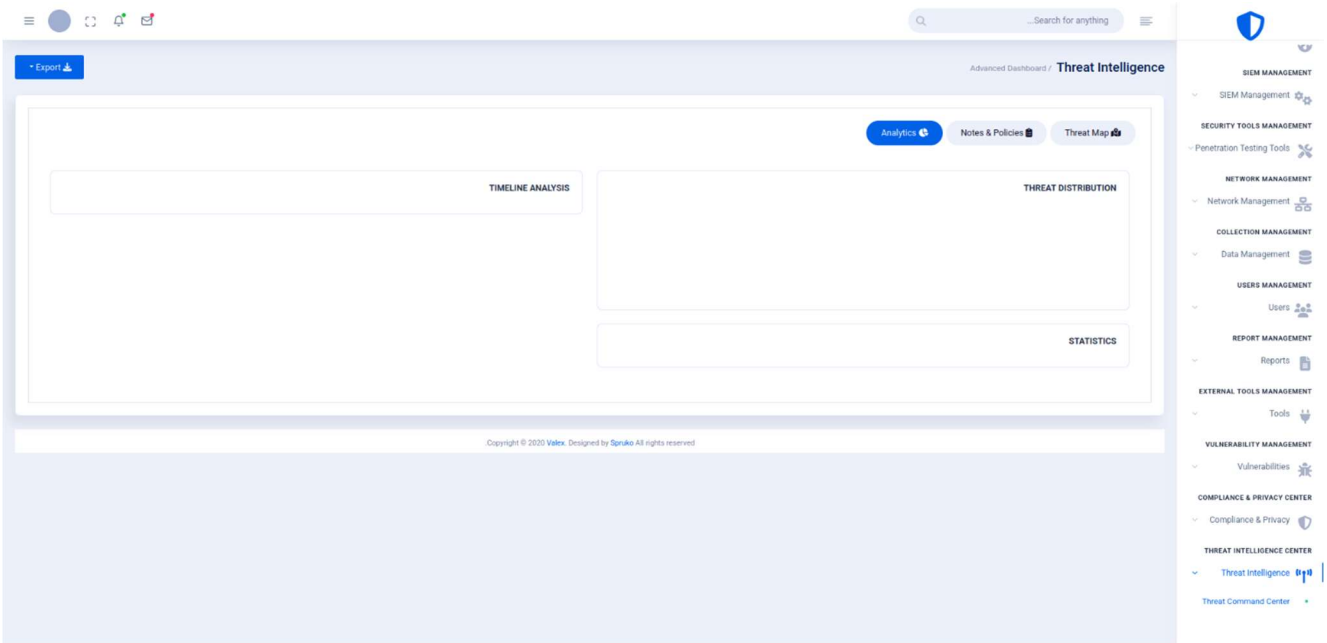

**شكل (4.33) نظرة عامة على لوحة تحكم نظام "Security Onion" الذي يستخدم لإدارة الأمن السيبراني، وقائمة التحقق للنشر، متطلبات الأجهزة، إعدادات الشبكة، وأقسام الإدارة المختلفة داخل النظام.**

الوصول الى Dashboard



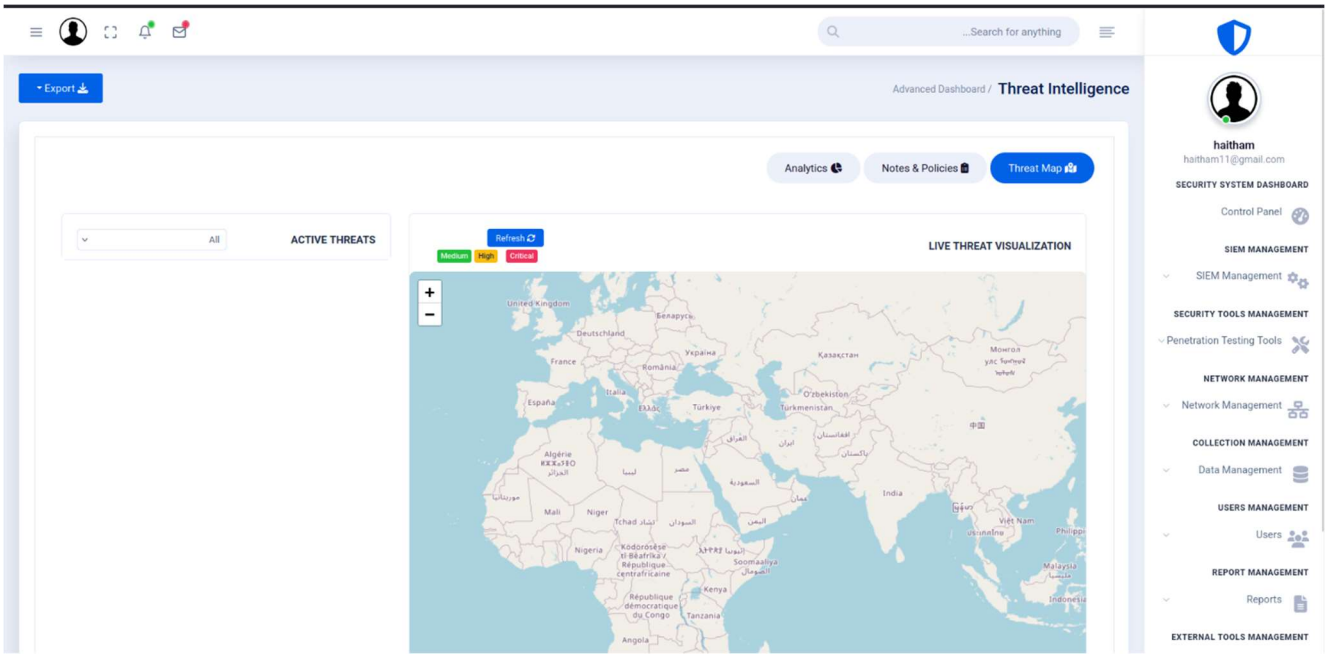

**شكل (4.34) لوحة تحكم رئيسية لنظام أمني تتيح الوصول السريع الى وظائف الإدارة العامة.**

13.تحليل الاستجابة للتهديدات



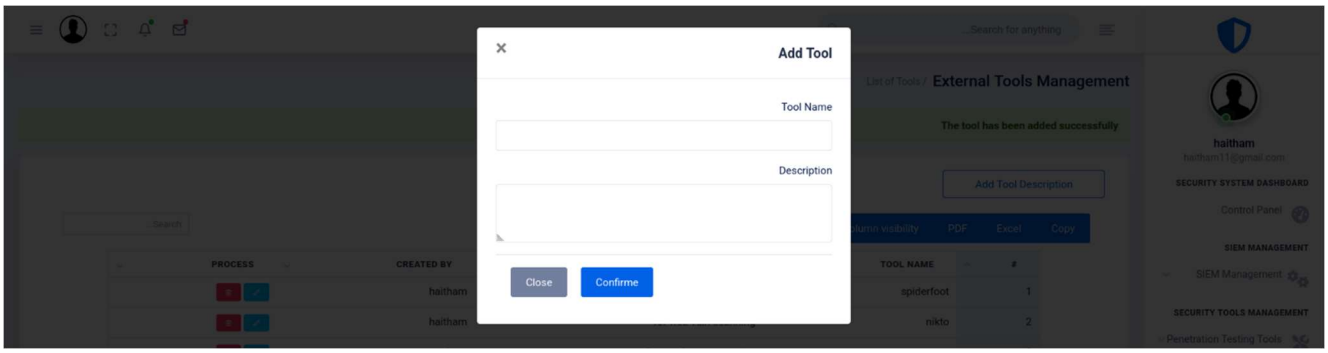

**شكل (4.35) أدوات لتحليل الأحداث عبر الزمن وعرض توزيع التهديدات، وإحصائيات مفصلة.**

14.خريطة التهديدات الحية



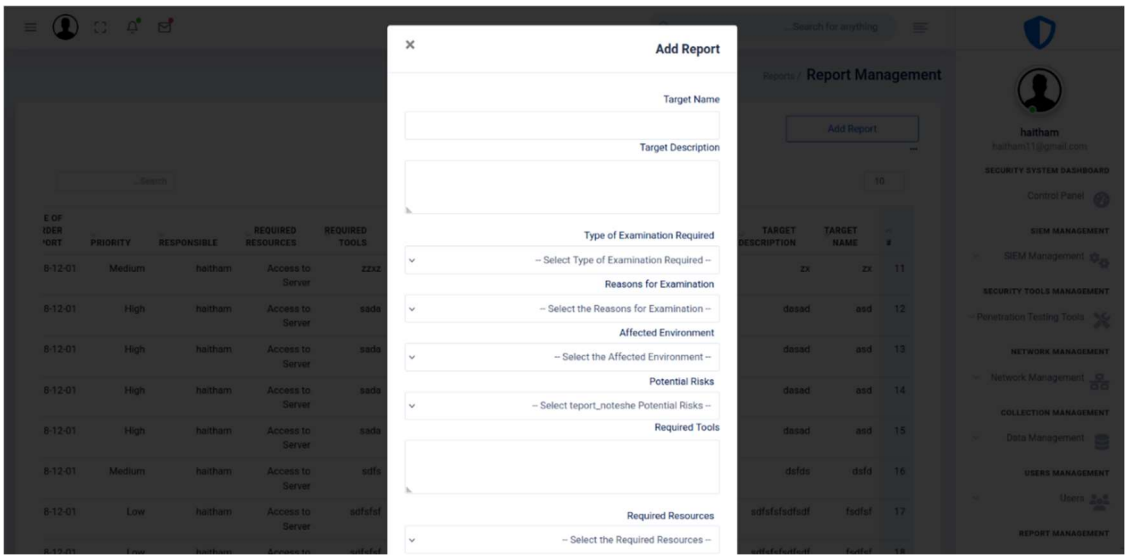

**شكل (4.36) عرضًا مرئيًا للتهديدات السيبرانية النشطة على خريطة عالمية، مما يساعد المستخدمين على فهم التوزيع الجغرافي وخطورته.**

15.طلب اضافة اداة جديده



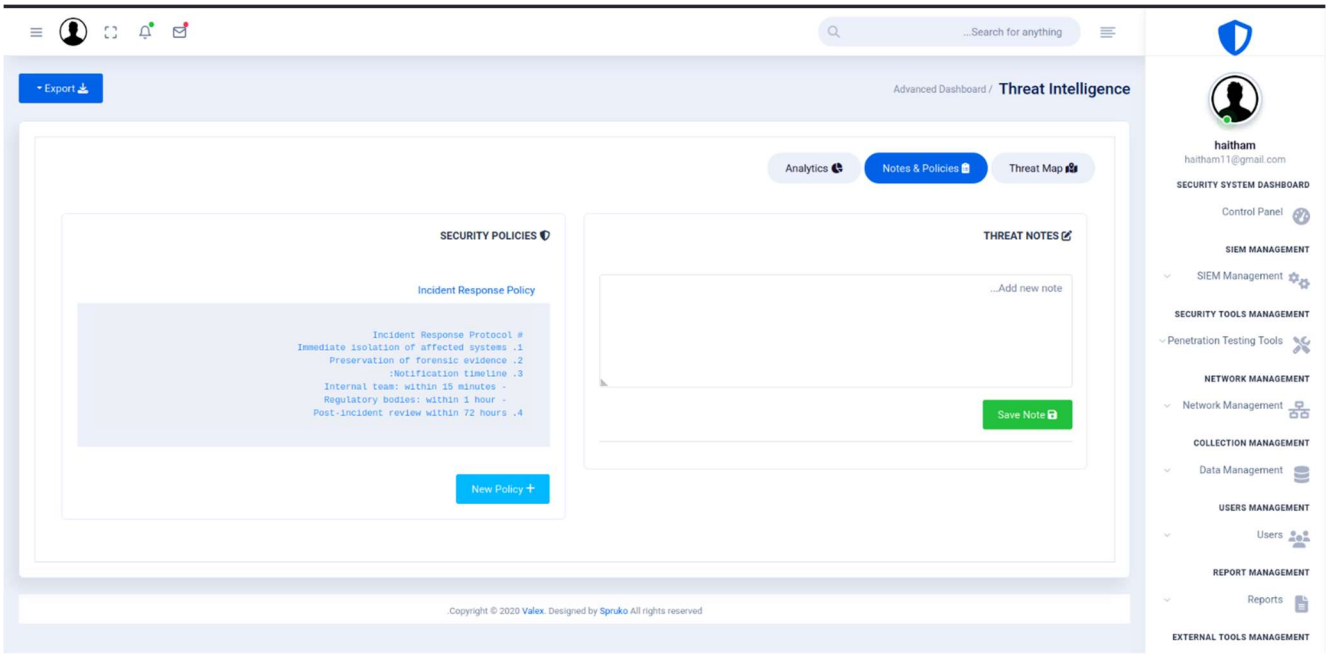

**شكل (4.37) عملية إضافة أداة جديدة إلى نظام متخصص في إدارة الأدوات الأمنية و أدوات تحليل التهديدات، وذلك من خلال نافذة إدخال بيانات بسيطة.**

16.طلب عمل فحص



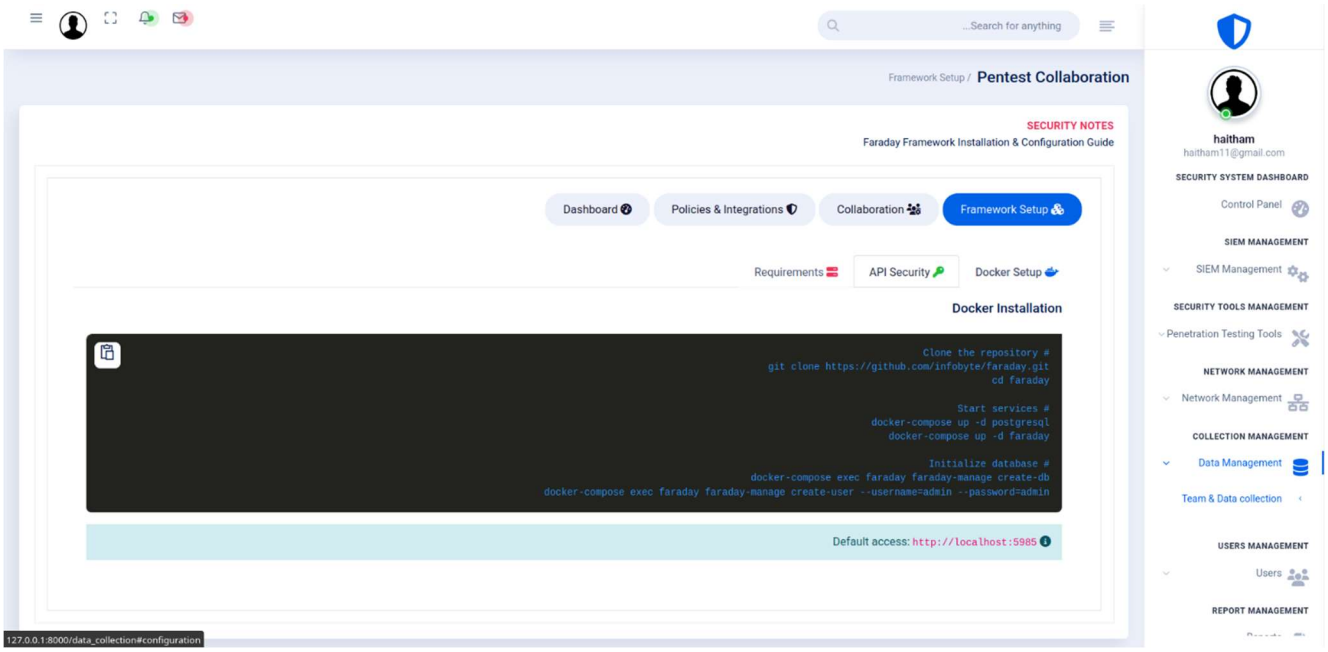

**شكل (4.38) واجهة مستخدم يمكن من خلالها للفرد تقديم طلب لإجراء فحص أمني (مثل اختبار اختراق أو تدقيق) عن طريق تقديم تفاصيل حول الهدف، ونوع الفحص، والأسباب، والبيئة المتأثرة، والمخاطر المحتملة، والأدوات/الموارد المطلوبة. يسهل هذا النموذج بدء عمليات التقييم الأمني.**

17.قسم الاستجابة للتهديدات ( اضافة ملاحظة وسياسة)




**شكل (4.39) واجهة إدارة سياسات الإستجابة للتهديدات وتسجيل الملاحظات المتعلقة بالتهديدات في نظام متكامل لأمن المعلومات.**

18.قسم تجميع البيانات وتحليلها




**شكل (4.40) واجهة إدارة سياسات تجميع وتحليل البيانات الأمنية في سياق اختبار الاختراق.**

# الفصل الخامس :التنفيذ والإختبار

## 5.1 مقدمة

يستعرض هذا الفصل مرحلة تنفيذ النظام الأمني الخاص بالبلاغات، بالإضافة إلى خطوات اختبار وظائفه بشكل منهجي لضمان كفاءته واستقراره. تم تطوير النظام بناءً على المتطلبات المحددة مسبقًا، مع التركيز على الأداء، سهولة الاستخدام، والأمان. وشملت هذه المرحلة بناء المكونات البرمجية، ربطها بقواعد البيانات، وتجربتها تحت سيناريوهات مختلفة لمحاكاة الاستخدام الواقعي مع عرض نتائج تنفيذ النظام

## 5.2 تنفيذ النظام والنتائج

تم تطوير النظام باستخدام إطار العمل Laravel بلغة PHP ، لما يوفره من هيكلية مرنة وآمنة لتطوير تطبيقات الويب، بالإضافة إلى دعمه لأساليب حديثة في البرمجة مثل MVC (Model-View-Controller) وغيرها .تم استخدام MySQL كنظام إدارة قواعد البيانات لما يتميز به من أداء عالٍ واستقرار.

### 5.2.1 بيئة التنفيذ

- نظام التشغيل: Windows 11 .
- إطار العمل : Laravel Framework 8.83.29 .
- خادم الويب: xampp control panel v3.2.4 .
- قاعدة البيانات : mysql Ver 15.1 Distrib 10.4.14-MariaDB .
- إصدارphp : PHP 7.4.9 .

**أدوات إضافية:**

- Composer لإدارة الحزم.
- Laravel Artisan لإدارة المهام.
- Git لإدارة النسخ.

### 5.2.2 مراحل التنفيذ ونتائجها

**1. إعداد بيئة التطوير**

تم إعداد البيئة البرمجية لتطوير المشروع، بما في ذلك تثبيت إطارLaravel ، إعداد قاعدة بياناتMySQL ، وضبط ملفات الإعداد (.env ). كذلك تم تثبيت الأدوات المساعدة مثل Composer وGit.

**النواتج:**

- Laravel project initialized
- الاتصال بقاعدة البيانات مفعل.
- خادم محلي جاهز للعمل XAMPP .

## 2. بناء قاعدة البيانات

تم إنشاء الجداول اللازمة للنظام شملت الجداول الأساسية جدول المستخدمين، جدول البلاغات، وجدول الإدارات أو الجهات المعنية بالرد على البلاغات وغيرها باستخدام Laravel Migrations كما تم ربط الجداول بالعلاقات المناسبة وفقًا لمخطط ERD . كما تم تشفير الحقول بمسميات يمكن العودة لها بتوثيق التالي:

**جدول الحقول وتشفيرها(5.1)**

| Field Name | Description (EN) | الوصف (AR) |
|---|---|---|
| invs_id | Main ID | المعرف الرئيسي. |
| invs_rmmqls_id | Linked Report ID | معرف البلاغ المرتبط |
| invs_usr_id | User Authorization ID | معرف المستخدم المفوض |
| invs_fnm | First Name | الاسم الأول |
| invs_snm | Second Name | الاسم الثاني |
| invs_tnm | Third Name | الاسم الثالث |
| invs_lnm | Last Name (Family Name) | اللقب |
| invs_nid | National ID / Passport Number | الرقم الوطني / رقم الجواز |
| invs_age | Age | العمر |
| invs_msta | Marital Status | الحالة الاجتماعية |
| invs_rlg | Religion | الديانة |
| invs_nat | Nationality | الجنسية |
| invs_pldob | Place and Date of Birth | مكان وتاريخ الميلاد |
| invs_issag | Issuing Authority | جهة الإصدار |
| invs_isdat | Date of Issue | تاريخ الإصدار |
| invs_exdat | Expiration Date | تاريخ الانتهاء |
| invs_type | Role in Incident (Witness 1, Witness 2, Accus | صفة المعني (شاهد أول، شاهد ثاني، جاني، مجني عليه) |
| invs_resgov | Governorate of Residence | المحافظة |
| invs_rescty | City of Residence | المدينة |
| invs_resdir | Directorate of Residence | المديرية |
| invs_resarea | Area/Village | القرية / الحارة |
| invs_rstyp | Type of Residence (Owner / Renter) | نوع السكن (مالك / مستأجر) |
| invs_rentnm | Name of Renter (if applicable) | اسم المؤجر (في حالة مستأجر) |
| invs_rel_lvl | Relation Degree (1st, 2nd, 3rd) | درجة القرابة (أولى، ثانية، ثالثة) |
| invs_rel_fnm | Full Name of Relative | اسم القريب الكامل |
| invs_rel_type | Type of Relation | نوع الصلة |
| invs_rel_phn | Relative’s Phone Number | رقم هاتف القريب |
| invs_rel_addr | Relative’s Address | عنوان سكن القريب |
| invs_jobttl | Job Title | المسمى الوظيفي |
| invs_jobtyp | Type of Work | نوع العمل |
| invs_edlvl | Educational Level | المستوى التعليمي |
| invs_jobloc | Job Location | موقع العمل |
| invs_jobphn | Work Phone Number | رقم هاتف العمل |
| invs_fprt | Fingerprint | البصمة |
| invs_nts | Notes | ملاحظات |
| invs_bya | By (Who created/modified/deleted) | بواسطة من قام بالإجراء |
| invs_ctudt | Created/Updated/Deleted Timestamp | تاريخ ووقت الإنشاء/التعديل/الحذف |
| created_by | User ID who created | معرّف المستخدم الذي أنشأ |
| created_by_name | Name of user who created | اسم المستخدم الذي أنشأ |
| updated_by | User ID who last updated | معرّف المستخدم الذي عدّل |
| updated_by_name | Name of user who last updated | اسم المستخدم الذي عدّل |
| deleted_by | User ID who deleted | معرّف المستخدم الذي حذف |
| deleted_by_name | Name of user who deleted | اسم المستخدم الذي حذف |

| Field Name | Description (EN) | الوصف (AR) |
|---|---|---|
| rm_rcn | Report/Complaint Number | رقم البلاغ/الشكوى |
| rm_dftrc | Date of filing the report/complaint | تاريخ تقديم البلاغ/الشكوى |
| rm_dde | Deportation date | تاريخ الترحيل |
| rm_iay | Issuing Authority | جهة الإصدار البلاغ |
| rm_datoti | Date and time of the incident | تاريخ ووقت الواقعة |
| rm_tcrss | Type: Criminal, Robbery, State Security | النوع: جنائي، سرقة، أمن الدولة |
| rm_ccrp | Classification: Complaint or Report | التصنيف: بلاغ أو شكوى |
| rm_stnr | Status: Notified, Rejected | الحالة: معمم، غير معمم، مرفوض |
| rm_rgnd | Relevant Government: Not Deported/Deported | حالة الترحيل: غير مرحل / مرحل |
| rm_dploci | Details of the Place of the Incident | تفاصيل مكان الواقعة |
| rm_dtofci | Details of the Incident | تفاصيل الواقعة |
| rm_rtpwit | Related Parties with the Incident | أطراف لهم صلة بالواقعة |
| | | |
| rm_ctudt | Created/Updated/Deleted Timestamp | وقت إنشاء أو تعديل أو حذف البلاغ |
| rm_cnfm_mgr | Confirmation by Manager | تأكيد المدير للبلاغ |
| | | |
| rm_updfl | Uploaded file with incident details | رفع ملف لتفاصيل الواقعة |
| rm_nts | Notes | ملاحظات |
| | | |
| created_by_name | Name of user who created | اسم المستخدم الذي أنشأ |
| | | |
| updated_by_name | Name of user who last updated | اسم المستخدم الذي عدل |
| | | |
| deleted_by_name | Name of user who deleted | اسم المستخدم الذي حذف |

**النواتج:**

- جداول مهيكلة في MySQL.
- علاقات مفاتيح خارجية (Foreign Keys) .
- بيانات تجريبية .
- أمنية في حقول الجداول.

## 3. تطوير واجهة المستخدم(Frontend)

تم تطوير واجهة المستخدم باستخدام الأدوات التي يوفرها Laravel بالاعتماد الكامل على التوثيق الرسمي لإطار العمل .تم استخدام Blade Templates لإنشاء واجهات ديناميكية وقابلة لإعادة الاستخدام، إضافة إلى الاعتماد على التعليمات والممارسات الموجودة في توثيق Laravel لإنشاء الواجهات وتنسيقها وربطها مع البيانات القادمة من الخادم.

**التركيز في التطوير كان على:**

- تبسيط تجربة المستخدم.
- وضوح عرض البيانات.
- سرعة الاستجابة .

**النواتج:**

- صفحات تم إنشاؤها بواسطة Blade تشمل (تسجيل الدخول، لوحة التحكم، نموذج البلاغ، عرض التفاصيل).
- تكامل كامل مع Controllers و Routes في Laravel .

## 4. تطوير الجانب الخلفي (Back-End)

تم تطوير وظائف النظام الرئيسية باستخدام بنية MVC (Model - View - Controller) لتنظيم الكود وضمان قابلية التوسع والصيانة.تم تطوير كل العمليات الأساسية للنظام مثل إدارة البلاغات، تسجيل الدخول والتسجيل، تحديد الصلاحيات، والتفاعل مع قاعدة البيانات باستخدام Eloquent ORM .

**ما تم تنفيذه:**

**المسارات Routes**

تم تعريف المسارات باستخدام ملفات web.php لربط الطلبات بالوحدات المنطقية المناسبة.

**الوحدات المنطقية Controllers**

تم إنشاء وحدات تحكم خاصة بكل جزء في النظام مثل:

- AuthController للمصادقة.
- ReportController لإدارة البلاغات.
- UserController لإدارة المستخدمين.

**النماذج Models**

تم إنشاء نماذج Eloquent تمثل الجداول الأساسية في قاعدة البيانات مع العلاقات المناسبة (علاقة بلاغ بمستخدم، إلخ).

**التحقق من المدخلات Validation**

تم استخدام Validator وRequest Classes للتحقق من البيانات المدخلة وفقًا لقواعد محددة (مثل التأكد من أن الحقول المطلوبة مكتملة، والصيغ صحيحة).

**التعامل مع الصلاحيات**

استخدم النظام Laravel Policy لتنظيم الصلاحيات بناءً على أدوار المستخدم .

**إرسال الإشعارات**

تم استخدام نظام التنبيهات في Laravel لإرسال إشعارات للمستخدمين عند تحديث حالة بلاغ أو عند تسجيل الدخول، عبر البريد الإلكتروني أو داخل النظام.

**النواتج:**

- ملفات Controller منظمة حسب الوظائف.
- تكامل قوي مع قاعدة البيانات عبر Eloquent .
- نظام حماية مدمج CSRF, Auth middleware .
- وظائف جاهزة للاختبار والتوسع.

## 5.3 اختبار النظام

تمثل عملية اختبار النظام مرحلة مهمة في دورة تطوير البرمجيات، حيث تهدف إلى التأكد من أن النظام يعمل بكفاءة وفقًا للمتطلبات المحددة مسبقًا، ويستجيب بالشكل المطلوب في مختلف السيناريوهات.

### 5.3.1 أنواع الاختبارات

- **اختبارات وظيفية (Functional Testing)** تم اختبار جميع وظائف النظام الأساسية مثل إرسال البلاغات، تسجيل الدخول، تصنيف الحالات، وإدارة المستخدمين.
- **اختبارات التوافق (Compatibility Testing)** تم اختبار النظام على متصفحات متعددة لضمان التوافق.
- **اختبارات الأداء (Performance Testing)** تم قياس سرعة استجابة النظام في حالات الضغط.
- **اختبارات قابلية الاستخدام (Usability Testing)** تم تجربة النظام من قبل مستخدمين لتقييم سهولة التفاعل معه.

## 5.4 النتائج

**1- سهولة الإمساك بالمجرمين**

بفضل نظام البلاغات، يمكن للمواطنين الإبلاغ عن الجرائم بسرعة وسهولة، مما يزيد من فرصة القبض على المجرمين. يمكن للشرطة تلقي البلاغات فورًا واتخاذ التدابير الضرورية للتعامل مع الحالات الجنائية بشكل فعال.

**2- توفير وسيلة تطبيقات لتعميم البلاغات**

يمكن تطوير تطبيقات للهواتف الذكية تتيح للمواطنين إرسال البلاغات مباشرة إلى نقاط الأمنية والمحلات التجارية. هذا يعزز التواصل ويسهل عملية الإبلاغ ويساهم في توفير بيانات أكثر دقة واستجابة أسرع.

**3- توفير حساب لمقدمي البلاغات**

يمكن لكل مقدم بلاغ أن يحصل على حساب في التطبيق المخصص، حيث يمكنه متابعة تطورات قضيته والحصول على تحديثات حول التحقيقات والإجراءات المتخذة من قبل الشرطة. يعزز ذلك الشفافية والثقة بين المواطنين والشرطة.

**4- تسهيل معاملات القسم والرجوع للبيانات**

يمكن لنظام البلاغات تسهيل إدارة ومعالجة المعاملات الداخلية للقسم. يتم توثيق البيانات وتخزينها بشكل منظم، مما يسهل الوصول إلى المعلومات وتحليلها في وقت لاحق. يعزز ذلك كفاءة وفعالية العمل الإداري للشرطة.

**5- الردع الجنائي**

قد يؤدي تحسين أداء الأجهزة الأمنية بفضل نظام البلاغات إلى زيادة الردع الجنائي. عندما يعرف المجرمون أن الشرطة تتلقى البلاغات بسرعة وتتخذ إجراءات فورية، فإنهم قد يترددون في ارتكاب الجرائم خوفًا من القبض عليهم.

# الفصل السادس :الخاتمة

## 6.1 ما تم التوصل إليه في المشروع

1. إنشاء نظام بلاغات أمني متكامل تم تطوير نظام إلكتروني يُمكن الجهات المعنية بالإستجابة للبلاغات بسرعة.
2. تم تنفيذ آليات تشفير وحماية متقدمة لحماية بيانات والبلاغات مع ألية لكشف ثغرات و تصدي للمخاطر.
3. توفير ألية لتوجيه البلاغات مباشرة للجهات المعنية بشكل تلقائي وفعال.
4. لوحة تحكم مركزية للجهات الأمنية تم تطوير لوحة تحكم تتيح للجهات الأمنية الاطلاع على البلاغات، تتبع حالتها، وتوثيق الإجراءات المتخذة.

## 6.2 التوصيات

1. الاستمرار في تحسين الحماية الرقمية يُوصى بتحديث تقنيات التشفير بشكل دوري لمواكبة التهديدات السيبرانية المتغيرة، وضمان بقاء سرية بيانات المستخدمين محمية تمامًا.
2. توسيع التكامل مع أنظمة أخرى يُوصى بربط النظام بمزيد من قواعد البيانات والأنظمة الحكومية لتسريع التحقق من صحة البلاغات ودقة المعلومات.
3. إضافة ميزة التتبع الآمن للمبلغ يمكن تطوير خاصية تمكّن المبلغ من تتبع حالة بلاغه .
4. يُوصى بتحسين واجهة المستخدم للتطبيق والموقع، وتسهيل خطوات الإبلاغ دون تعقيد .
5. إجراء تقييم دوري لأداء النظام ؛ يُقترح إجراء مراجعة تقنية وأمنية للنظام لضمان الجودة والاستجابة للمتغيرات الأمنية.

## 6.3 التحديات

- صعوبة في ربط قاعدة البيانات بسبب تعقيدها وضخامتها.
- مشاكل في استدعاء المكتبات والتأكد من توافقها مع النظام بالإضافة إلى تعارض بعض الأدوات نتيجة اختلاف الإصدارات المستخدمة.
- تحديات في دمج الأعمال المنفصلة وتنسيق جهود أعضاء الفريق معًا بشكل متكامل.
- تعقيد النظام بشكل عام، والسعي لتطويره بطريقة تضمن سهولة الاستخدام للمستخدم النهائي.

## 6.4 الأعمال المستقبلية

1. **دعم الموقع الجغرافي (GPS)**
مثل تصنيف البلاغات تلقائيًا حسب الخطورة أو النوع، واقتراح الإجراءات المناسبة بناءً على البيانات السابقة.

2. **تطوير تطبيق جوال متكامل**
لتحديد موقع البلاغ بدقة وعرضه على خريطة تفاعلية، ما يساعد فرق الاستجابة السريعة في الوصول لموقع الحادث.

3. **دمج ذكاء الاصطناعي لتحليل البلاغات**
يتيح للمستخدمين تقديم البلاغات بسهولة عبر الهاتف، مع إمكانية رفع الصور والموقع.

4. **إتاحة واجهة برمجة تطبيقات (API)**
للسماح بتكامل النظام مع أنظمة أخرى مثل أنظمة الطوارئ أو قواعد بيانات السجل المدني.

5. **ربط النظام بكاميرات المراقبة الذكية**

لتحليل الفيديوهات في الوقت الحقيقي والتقاط الحالات المشبوهة تلقائيًا .

## 6.5 المراجع


[1] Alameri, Thamer, Alhilali, Ahmed Hazim, Ali, Nabeel Salih and Mezaal, Jawad Kadhim, “Crime reporting and police controlling: Mobile and web-based approach for information-sharing in Iraq”, Journal of Intelligent Systems, vol. 31, no. 1, 2022, pp. 726-738. https://doi.org/10.1515/jisys-2022-0034

[2] Strom, K. J., & Smith, E. L., “The future of crime data: The case for the National Incident-Based Reporting System (NIBRS) as a primary data source for policy evaluation and crime analysis”, Criminology & Public Policy, 16(4), 1027-1048, 2017. https://doi.org/10.1111/1745-9133.12336

[3] A. B. Sakpere, A. V. D. M. Kayem and T. Ndlovu, "A Usable and Secure Crime Reporting System for Technology Resource Constrained Context," 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangju, Korea (South), 2015, pp. 424-429, doi: 10.1109/WAINA.2015.97.

[4] Shih, T.-F.; Chen, C.-L.; Syu, B.-Y.; Deng, Y.-Y.,“A Cloud-Based Crime Reporting System with Identity Protection”, Symmetry, 2019, 11, 255. https://doi.org/10.3390/sym11020255

[5] Abdul Salam Shah- Muhammad Fayaz - Asadullah Shah - Shahnawaz Shah, “Testing desktop application: Police station information management system”, International Journal of Software Engineering and Its Applications, Vol. 10, No. 7 (2016), pp. 101-118 http://dx.doi.org/10.14257/ijseia.2016.10.7.10

[6] N. Debnath, R. Uzal, G. Montejano and D. Riesco, “Web Application to Improve Police Management Performance: A Web Application to Prepare Police Stations to Face an ISO 9001: 2008 Certification Process and to Improve Watching Activities of Human Rights”, Seventh International Conference on Information Technology: New Generations, 2101, Las Vegas, NV, USA, 2010, pp. 32-35, doi: 10.1109/ITNG.2010.163.

[7] Sumit R. Farsole, Shreyas B. Kene and V. V. Bhujade, “E-Police Police Record Management System”, International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 2 Issue: 3.

[8] Yee Suzan, Nayef Abdulwahab Mohammed Alduais, “Web-Based Citizen-Police Report System”, Applied Information Technology And Computer Science Vol. 4 No. 2 (2023) 1999 – 2018

[9] Laravel Documentation https://laravel.com/docs/

[10] Php – Laravel (دورة إنشاء برنامج فواتير) by Mora Soft

https://youtube.com/playlist?list=PLftLUHfDSiZ7pKXkpGCoZATm5rF6msj5A&si=OnSy1E-npwFwhxw4

## 6.6 الملحقات

**ملحق[1]**

### 6.6.1 الاستبيانات

**استبيان رضا الموظفين عن نظام البلاغات**

شكرًا لك على المشاركة في هذا الاستبيان. يهدف الاستبيان إلى قياس رضاك وتجربتك في استخدام نظام البلاغات في العمل. يرجى تقديم إجاباتك بناءً على تجربتك الشخصية. جميع الإجابات ستكون سرية ولن يتم الكشف عن هويتك.

الجزء الأول: المعلومات الشخصية

1- الاسم:

2- الوظيفة:

3- القسم/الإدارة:

الجزء الثاني: تجربتك في استخدام نظام البلاغات

4- هل تم توفير تدريبات لك لاستخدام نظام البلاغات؟

- نعم
- لا

5- كيف تقيم سهولة استخدام نظام البلاغات؟

- سهل جدًا
- سهل
- متوسط
- صعب
- صعب جدًا

6- هل كانت واجهة المستخدم سهلة الاستخدام؟

- نعم، كانت سهلة جدًا
- نعم، كانت سهلة
- متوسطة

- لا، كانت صعبة
- لا، كانت صعبة جدًا

7- هل كانت التعليمات والتوجيهات موجودة وواضحة في النظام؟
- نعم، كانت موجودة وواضحة جدًا
- نعم، كانت موجودة وواضحة
- متوسطة
- لا، كانت غير واضحة
- لا، كانت غير موجودة

8- هل كانت هناك مشاكل تقنية أو تعطل في نظام البلاغات؟
- نعم، كانت هناك مشاكل تقنية متكررة
- نعم، لكنها كانت نادرة وتم حلها بسرعة
- لا، لم أواجه أي مشاكل تقنية

9- هل تلقيت تدعيمًا ومساعدة كافية من فريق الدعم الفني في حال وجود مشاكل؟
- نعم، تم تقديم الدعم بشكل ممتاز
- نعم، ولكن قد تكون هناك بعض التحسينات الممكنة
- لا، لم يتم تقديم الدعم بشكل كافي

10- هل تعتقد أن نظام البلاغات يساعد في تحسين كفاءة العمل وتنظيم المعلومات؟
- نعم، بشكل كبير
- نعم، بشكل ملحوظ
- نعم، إلى حد ما
- لا، لا أرى تأثيرًا ملموسًا
- لا، يؤثر سلبًا على الكفاءة والتنظيم

11- هل تعتقد أن نظام البلاغات يضمن سرية وأمان المعلومات المبلغ عنها؟
- نعم، أشعر بالثقة الكاملة في السرية والأمان
- نعم، ولكن قد تكون هناك بعض المخاوف
- لا، أشعر بعدم الثقة في السرية والأمان

12- هل تود تقديم أي تعليقات أو اقتراحات لتحسين نظام البلاغات؟

**استبيان رضا أصحاب المحلات التجارية عن نظام البلاغات**

شكرًا لك على المشاركة في هذا الاستبيان. يهدف الاستبيان إلى قياس رضاك وتجربتك في استخدام نظام البلاغات في محلك التجاري. يرجى تقديم إجاباتك بناءً على تجربتك الشخصية. جميع الإجابات ستكون سرية ولن يتم الكشف عن هويتك.

الجزء الأول: معلومات المحل التجاري

1- اسم المحل التجاري:

2- نوع المحل التجاري (متجر إلكتروني):

4- موقع المحل التجاري:

5-

الجزء الثاني: تجربتك في استخدام نظام البلاغات

4- هل توفير تطبيق البلاغات مناسب بنسبة لك؟

- نعم
- لا

5- كيف تقيم سهولة استخدام تطبيق للبلاغات؟

- سهل جدًا
- سهل
- متوسط
- صعب
- صعب جدًا

6- هل كانت واجهة المستخدم سهلة الاستخدام؟

- نعم، كانت سهلة جدًا
- نعم، كانت سهلة
- متوسطة
- لا، كانت صعبة

- لا، كانت صعبة جدًا

7- هل كانت التعليمات والتوجيهات موجودة وواضحة في النظام؟

- نعم، كانت موجودة وواضحة جدًا
- نعم، كانت موجودة وواضحة
- متوسطة
- لا، كانت غير واضحة
- لا، كانت غير موجودة

8- هل كانت هناك مشاكل تقنية أو تعطل في تطبيق البلاغات؟

- نعم، كانت هناك مشاكل تقنية متكررة
- نعم، لكنها كانت نادرة وتم حلها بسرعة
- لا، لم أواجه أي مشاكل تقنية

9- هل تلقيت تدعيمًا ومساعدة كافية من فريق الدعم الفني في حال وجود مشاكل؟

- نعم، تم تقديم الدعم بشكل ممتاز
- نعم، ولكن قد تكون هناك بعض التحسينات الممكنة
- لا، لم يتم تقديم الدعم

**الجزء الثالث: تعليقات إضافية**

10- هل لديك أي تعليقات أو اقتراحات إضافية حول تطبيق البلاغات؟

## ملحق[2]

### 6.6.2 المقابلة

1- ما هي الخصائص الرئيسية لنظام بلاغات أقسام الشرطة؟

2- ما هي الخطوات المتبعة لتقديم بلاغ لقسم الشرطة؟

3- هل يوجد فرق في إجراءات تقديم البلاغات بين حالات الطوارئ والحالات العادية؟

4- هل هناك متطلبات محددة للمعلومات المطلوب تقديمها عند تقديم بلاغ؟

5- كيف يتم توجيه البلاغات إلى الأقسام المعنية داخل الشرطة؟

6- هل يوجد نظام تتبع لحالة البلاغات المقدمة؟ وكيف يمكن للمواطنين متابعة حالة بلاغهم؟

7- هل يتم توفير واجهات إلكترونية لتقديم البلاغات عبر الإنترنت؟

8- ما هي السبل المتاحة للتواصل مع قسم الشرطة بعد تقديم البلاغ؟

9- هل يتم توفير تقارير أو إحصائيات حول أعداد البلاغات وأنواعها للجمهور؟

10-هل يوجد نظام لجمع ملاحظات المواطنين حول تجربتهم في تقديم البلاغات وكيفية تحسين العملية؟