



استراتيجيات امن المعلومات لحماية قواعد البيانات



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



2018 : اختراق جوجل بلس Google +
وتسريب بيانات 52.5 مليون مستخدم – ماهذه البيانات ???



م . صالح بن عبدالله الشري

مستشار في أمن معلومات والامن السيبراني
مدرب معتمد في تقنية المعلومات

- ماجستير علوم حاسب (Computer Science) مرتبة الشرف الاولى
- بكالوريوس هندسة حاسب (Computer Engineer)
- حاصل على درجة "مستشار" من هيئة المهندسين السعوديين
- متخصص في امن الشبكات والامن السيبراني
- خبرة 20 سنة في تقنية المعلومات
- حاصل على العديد من الشهادات المهنية في مجال الشبكات وامن المعلومات
- CCNA ,CCNP , CISSP, PMP, security + ,ITILv3 , FS consultant
- مدرب معتمد من المؤسسة العامة للتدريب المهني والتقني في مجال تقنية المعلومات
- حاصل على شهادة TTT لتدريب واعداد المدربين
- دورة امن المعلومات في هيئة المهندسين السعوديين
- العديد من الدورات ومحاضرات توعوية
- مهتم بالاعمال التطوعية والمجتمعية في مجال التقنية

اجندة المحاضرة



تشفير البيانات الحساسة



أساليب التحايل
والاستخدام السيء
للنظام



أسئلة الحضور



تحديث الأنظمة
وتحديد صلاحيات
الاستخدام



استراتيجيات لحماية
قواعد البيانات



التحديات الأمنية
والاختراقات لقواعد
البيانات

مقدمة عن قواعد البيانات



الحقل				
اسم الشخص	اسم الأب	اسم العائلة	مولد الشخص	تعريف الشخص
مريم	عبدالله	الحمد	2\4\1990	1
نورة	تركي	الحسن	4\5\1991	2
شهد	خالد	الفهد	3\9\1998	3
خلود	محمد	الخلد	1\7\1991	4

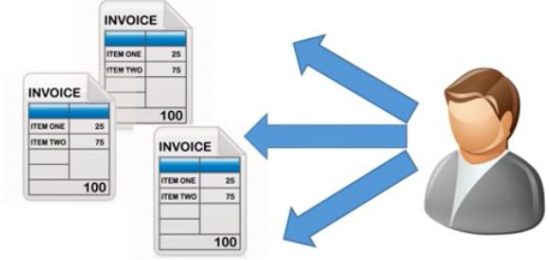
السجل

عناصر بيانات منطقية مرتبطة مع بعضها البعض بعلاقة رياضية وهي منظّمة من معلومات مهيكلّة أو البيانات المخزّنة عادةً بصيغة إلكترونيّة .

- تتكون من جدول واحد أو أكثر.
- ويتكون الجدول من سجل (صف) أو أكثر
- ويتكون السجل من حقل أو أكثر.

- عادةً ما تكون قاعدة البيانات تحت تحكم نظام إدارة قاعدة بيانات DBMS

قواعد البيانات DataBase



قواعد البيانات DataBase

ومثال عليه السجل الخاص بموظف معين يتكون من عدة حقول مثل رقم الموظف - اسم الموظف - درجة الموظف - تاريخ التعيين - الراتب - القسم التابع له،

تخزن في جهاز الحاسوب على نحو منظم، حيث يقوم برنامج (حاسوب) يسمى محرك قاعدة البيانات database engine بتسهيل التعامل معها والبحث ضمن هذه البيانات، وتمكين المستخدم من الإضافة والتعديل عليها.

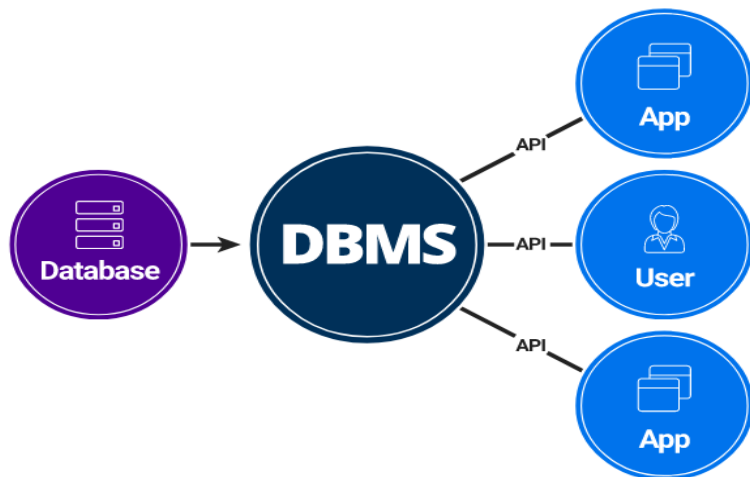
أكثر نظم قواعد البيانات استخداما أوراكل Oracle، سايبيس Sybase، و MS SQL.



الحقل

اسم_الشخص	اسم_الاب	اسم_العائلة	مولد_الشخص	تعريف_الشخص
مريم	عبدالله	الحمد	2\4\1990	1
نورة	تركي	الحسن	4\5\1991	2
شهد	خالد	القهد	3\9\1998	3
خلود	محمد	الخلد	1\7\1991	4

السجل



قواعد البيانات DataBase

 @salnahi

 0555161888

أهمية قواعد البيانات



أهمية قواعد البيانات DataBase

- ❑ تخزين كمية ضخمة من البيانات بأنواع مختلفة
- ❑ السرعة في الوصول إلى المعلومات والبيانات
- ❑ البحث عن المعلومات المهمة والمخزنة
- ❑ زيادة المرونة في بيئة العمل
- ❑ تسهيل تخزين البيانات والمعلومات الهامة وتحقيق قدر من الامان والسرية
- ❑ حل المشاكل من خلال الوصول للمعلومات بشكل يسير وسهل وليس عشوائياً
- ❑ تسريع عملية التطوير ومركزية البيانات والحد من التكرار

التحديات الأمنية والاختراقات لقواعد البيانات

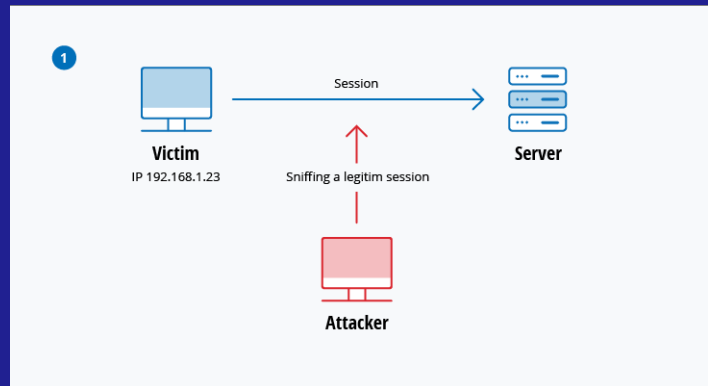


حجب الخدمة Denial of service



هو جعل خادم قاعدة بيانات أبطأ كثيرا أو حتى غير متاحة للمستخدمين على الإطلاق.

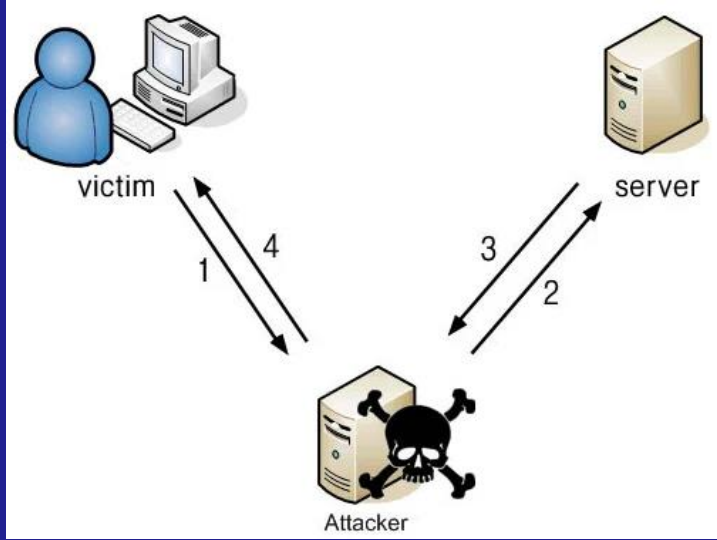
ربما أن هجوم حجب الخدمة لم يسفر عن الإعلان أو فقدان معلومات قاعدة البيانات، إلا انه يمكن يكلف كثير من خسارة الوقت والمال.



لاستيعاب التجارة الإلكترونية وفائدة الأنظمة الموزعة ، فان قاعدة البيانات صممت لكي توزعَ في نمط خادم الزبون .
المهاجمون يمكن أن يستخدموا برامج ملتقطة يمكنها رصد والتقاط تيارات البيانات من قاعدة البيانات ، والحصول على بعض المعلومات السرية ، مثل رقم بطاقة الائتمان لأحد العملاء .

هجوم الالتقاط sniff attack

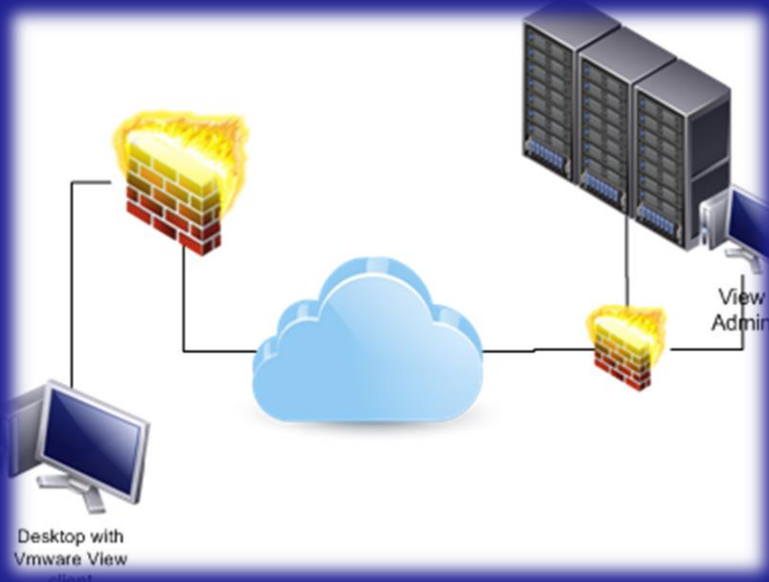




هجوم الخداع spoofing attack



المهاجمون يستخدمون تطبيق ويب قانوني لدخول قاعدة البيانات، وبعد ذلك يسترجع البيانات من قاعدة البيانات وعمل بعض الصفقات الغير قانونيه والسرقة . الحصول على اسم المستخدم وكلمة السر وسيستخدمها في الدخول على قاعدة بيانات الشركة



برنامج ضار يدرج في النظام. يستقر عادة في أنظمة التشغيل . حصان طروادة يمكنه تعديل قاعدة البيانات دون أن يلحظ ذلك من قبل المدير .

وضع حصان طروادة في نظام قاعدة البيانات إما عن طريق خارجي او طرف داخلي

حصان طروادة Trojan Horse



@salnahi

0555161888

تحديث الأنظمة وتحديد صلاحيات الاستخدام



التهيئة و الضبط المناسب للقواعد البيانات

- عدم قبول طلبات الإتصال من جهات غير موثوق
- ضبط الحد الأقصى للمحاولات الفاشلة
- إن الأخطاء البرمجية والثغرات في أنظمة إدارة قواعد البيانات تعتبر من المصادر التي تضعف أمن النظام، لذلك من المهم والضروري جدا متابعة التحديثات الجديدة و الحصول عليها من قبل منتج النظام و تنصيبها حال توفرها



إستخدام وسائل تحديد صلاحيات الإستخدم Access Control Methods
المناسبة

وهي آليات معينة لتحديد صلاحيات ونطاق المستخدم للوصول إلى البيانات،
فبناءً على هوية المستخدم يمكن تحديد تلك الصلاحيات.

يوجد هنالك ثلاثة طرق معروفة يمكن إستخدامها

تحديد الصلاحيات



تعتبر هذه الطريقة من أكثر الطرق صرامة، ففي هذه الطريقة لا يمكن للمستخدم منح صلاحية الوصول إلى البيانات لمستخدم آخر. بل على العكس جميع الصلاحيات مثبتة و معروفة و لا يوجد هنالك مرونة في تحديد الصلاحيات على مستوى البيانات.

تستخدم غالبا هذه الطريقة في التطبيقات العسكرية، حيث من المؤلف أن نجد التصنيف سري Secret و سري للغاية Top Secret

ضبط الوصول الإلزامي Mandatory Access Control MAN



بدلاً من منح الصلاحيات للمستخدم مباشرة ، يمكن منح الصلاحيات إلى أدوار أو مناصب معينة Roles و من ثم إسناد المستخدمين إلى الأدوار المناسبة لهم . في هذه الطريقة يحصل المستخدم على جميع الصلاحيات الموجودة في الدور المسند إليه.

ضبط الوصول المرتكز على الدور Role Based Access Control



تعتبر هذه الطريقة من أقل الطرق صرامة، ففي هذه الطريقة يمكن للمستخدم منح صلاحية الوصول إلى البيانات لمستخدم آخر. وتحتوي هذه الطريقة على شئ من الخطورة، حيث يمكن إعطاء مستخدم صلاحيات لا يجب أن يملكها.

ضبط الوصول الإختياري Discretionary Access Control

ماذا تحمي في قواعد البيانات؟



ماذا نحمي في قواعد البيانات

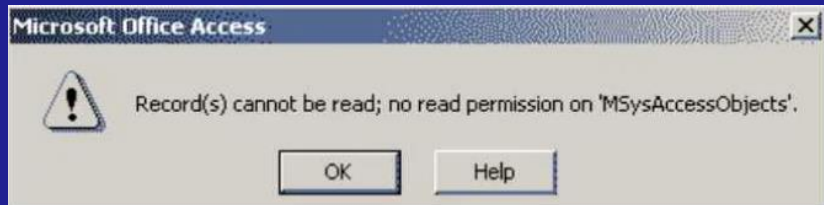
حماية المعلومات الموجودة فيها ولحمايتها يجب حماية الصفات الثلاث الرئيسية التي تركز عليها المعلومات (السرية، السلامة، التوفر)

- السرية : ضمان أن الأطراف المسموح لها فقط

- السلامة : ضمان أنه لا يمكن لأي شخص غير مصرح به أو البرامج الضارة تغييرها

- التوافرية : يجب أن لا تزال قواعد البيانات متاحة للأشخاص المصرح لهم

أساليب التحايل والاستخدام السيء للقواعد البيانات



- منح بعض الموظفين صلاحيات الوصول مع الوقت يصبح له القدرة على التحكم الكامل في قاعدة البيانات .

منع إساءة الاستخدام عن طريق محدودية الوصول والتصريح له فقط الوصول للمعلومات التي يحتاجها.

إساءة استخدام الامتيازات





الثغرات في نظام التشغيل



وجود ثغرات أمنية في أنظمة التشغيل الأساسية مثل ويندوز ولينكس ويونيكس وما إلى ذلك والخدمات التي ترتبط بقواعد البيانات قد تؤدي إلى الوصول غير المصرح به وهذا قد يؤدي إلى هجوم تعطيل الخدمة Denial of service

- تنزيل تحديثات نظام التشغيل المتعلقة بالأمن عندما تصبح متاحة.



في هجوم حقن SQL المرتكب عادة يتم إدخال أو حقن بيانات قاعدة بيانات غير مصرح بها إلى قناة بيانات SQL الضعيفة أو الغير محمية، وعادة يتم استهداف قنوات البيانات التي تشمل الإجراءات المخزنة ومدخلات تطبيق الويب، ثم يتم تمرير هذه البيانات المحقونة إلى قاعدة البيانات حيث يتم تنفيذها باستخدام حقن SQL، وبالتالي المهاجم ربما كسب وصول غير مقيد إلى قاعدة البيانات بأكملها.

حقن SQL injection





SQL Injection Attack (SQLi)

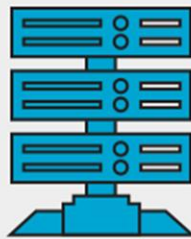
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.



WEBSITE
INPUT FIELDS

2. Malicious SQL query is validated & command is executed by database.

2



DATABASE

3. Hacker is granted access to view and alter records or potentially act as database administrator.

3



HACKER

حقن SQL injection



SQL Injection

 @salnahi

 0555161888

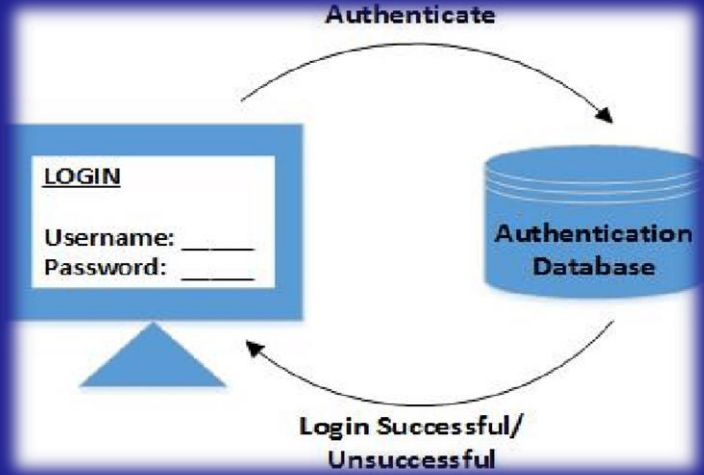


ومن الممكن مكافحة حقن SQL عن طريق الجمع بين ثلاث تقنيات فعالة:

- ❑ أنظمة منع الاختراق IPS التي تتفقد حركة قاعدة البيانات وتحدد الهجمات التي استهدفت والثغرات
- ❑ والتحكم بالوصول على مستوى الاستعلام (query-level access control) الذي يقوم بتحديد الامتيازات للحد الأدنى من العمليات والمعلومات المطلوبة.
- ❑ Event Correlation ترابط الحدث

حقن SQL injection





- الهندسة الاجتماعية Social engineering

- Brute force

ينبغي استخدام أقوى تقنيات المصادقة (الرموز، الشهادات، الصفات الحيوية وغيرها)

أقوى السياسات واستخدام المصادقة المتبادلة والمصادقة متعددة العوامل.

ضعف المصادقة



@salnahi

0555161888



- يجب أن يتم تسجيل المعاملات الحساسة أو العادية التي تتم في قاعدة البيانات بطريقة آلية لتسوية الحوادث
- الكشف عن وجود انتهاك وتتبع الانتهاك لنقطة معينة من الزمن ولمستخدم معين.

ضعف التعقب





عادة ما تكون النسخة الاحتياطية للبيانات المخزنة غير محمية من الهجوم، ونتيجة لذلك هناك عدة انتهاكات أمنية شملت سرقة أشرطة النسخ الاحتياطية والأقراص الصلبة لقاعدة البيانات.

ولمنع التعرض للنسخ الاحتياطية للبيانات ينبغي أن تكون :
- مشفرة

التعرض للنسخة الاحتياطية للبيانات



استراتيجيات لحماية قواعد البيانات



قاعدة بيانات يتم الوصول إليها عن طريق الشبكة الداخلية أو عن طريق الدخول
عن بعد – تسمى عملية الوصول " بالتصديق "
كل عملية وصول إلى قاعدة البيانات سواء كانت ناجحة أم لا يجب أن تتم
مراقبتها، وإتباع الإجراءات الملائمة لها





المراجعة هي عملية لضمان أن قاعدة البيانات لم يدخلها احد غير مصرح له.
إستراتيجية مراجعة حسابات قاعدة البيانات يجب أن تتضمن عمليات المراقبة
لتصديق سلامة قواعد العمل المتبعة

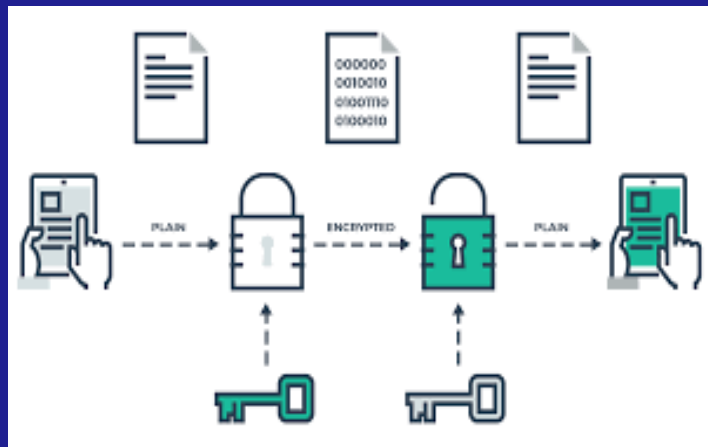
المراجعة والأدوات التحليلية



هيكلية البنية التحتية

تتكون من :

- جدار الحماية وهي آلية تستخدم عادة لمنع التسلل من خارج الشبكة.
- خادم الويب وتطبيقات الويب توفر خدمات متعددة للمستخدم النهائي قبل الوصول إلى قاعدة البيانات.
- طبقة الشبكة الوسط الذي يتم فيه نقل البيانات



التشفير لقواعد البيانات

- تشفير قاعدة البيانات هو عملية تحويل البيانات - التي تم تخزينها في قاعدة بيانات ، وفي تنسيق نص عادي - إلى نص مشفر بمساعدة خوارزمية
- 1- تشفير كامل محرك الأقراص
 - 2- تشفير النظام الجزئي
 - 3- تشفير قاعدة البيانات



التشفير

- التشفير على مستوى البيانات العابرة: وهو للمعلومات الحساسة التي تتحرك داخل الشبكة ويمكن للمهاجم الوصول إليها من خلال التنصت.
- التشفير على مستوى البيانات الثابتة: وهو للمعلومات الحساسة المخزنة في قاعدة البيانات التي من الممكن للمهاجم اختراقها.



طرق لتشفير قواعد البيانات

1. تشفير على مستوى ملفات قواعد البيانات : بشكل كامل على مستوى التخزين، وذلك باستخدام برمجيات أو عتاد خاص لذلك.
2. تشفير على مستوى أعمدة الجداول في قواعد البيانات : يتم تشفير الحقول في جداول البيانات بناء على الأعمدة التي تنتمي إليها.
3. تشفير على مستوى البرنامج التطبيقي الذي يستخدم قواعد البيانات : قبل تخزين البيانات يقوم البرنامج بنفسه بتشفير البيانات.



تغيير كلمة المرور حالما يتم الانتهاء من تثبيت قاعدة البيانات



كلمات المرور لقواعد البيانات



MySQL Users

Add New User

Username

Password

Password (Again)

Strength ⓘ

Very Strong (100/100)

Password Generator

Create User

اسماء المستخدمين لقواعد
البيانات

إزالة حسابات المستخدمين التي ليست قيد الاستخدام

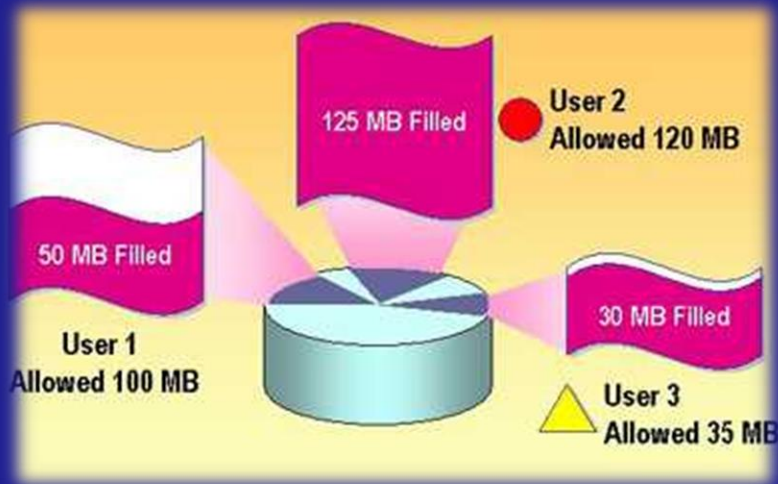
 @salnahi

 0555161888



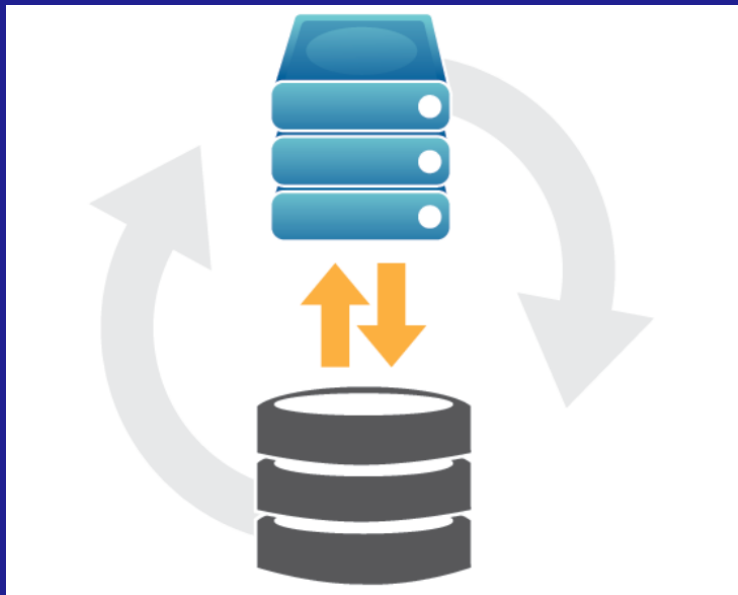
سياسة كلمات المرور

وضع سياسة عالية الحساسية على كلمات المرور للمستخدمين وفرض سياسة
تغييرها كل فترة تجنباً لتعرضها للسرقة أو التسريب



القيود على المستخدمين
والمساحات

تقييد مقدار مساحة التخزين التي تمنح لكل مستخدم في قاعدة البيانات.



النسخ الاحتياطي لقواعد البيانات

- نسخ احتياطية للبيانات بشكل دوري لضمان استعادة البيانات في حالة فقدانها
- تأمين قاعدة البيانات ضد الثغرات الأمنية

أسئلة واستفسارات

للتواصل للتدريب والاستشارات والاستفسارات



salnahi@gmail.com



0555161888



@salnahi



[linkedin.com/in/salnahi](https://www.linkedin.com/in/salnahi)

 @salnahi



0555161888



شكراً لكم