

تقرير تحسين الأداء والأمان للنظام

تقرير تحسين الأداء والأمان للنظام

مقدمة

النظام الحالي الخاص بإدارة طلبات السحب والإيداع ولوحة التحكم المباشرة، تم إعداد هذا التقرير لتوضيح أهم التحسينات المقترحة لرفع:

- مستوى الأمان
- سرعة الأداء
- استقرار النظام
- قابلية التوسع
- جودة تجربة المستخدم
- الاحترافية التقنية

ويهدف هذا التقرير إلى مساعدة العميل على تطوير النظام ليصبح أكثر استقراراً واعتمادية في بيئات العمل الحقيقية.

أولاً: تحسينات الأمان (Security Improvements)

1. استخدام HTTPS وتشفير الاتصال

الوضع الحالي

الاتصال بالموقع قد يتم عبر HTTP غير المشفر.

المشكلة

أي بيانات يتم إرسالها مثل:

- رقم البطاقة
- CVV
- المبالغ
- بيانات الحساب

يمكن اعتراضها أثناء النقل عبر الشبكة.

التحسين المقترح

تفعيل:

SSL / TLS

HTTPS

الفوائد

- تشفير كامل للبيانات أثناء النقل .
- حماية من هجمات Man In The Middle.
- رفع موثوقية النظام .
- تحسين تقييم محركات البحث .
- منع اعتراض بيانات العملاء .

2. تشفير البيانات الحساسة داخل قاعدة البيانات

الوضع الحالي

يتم حفظ بعض البيانات الحساسة كنصوص مباشرة داخل قاعدة البيانات.

المشكلة

في حال اختراق قاعدة البيانات سيتم كشف البيانات مباشرة.

التحسين المقترح

تشفير البيانات الحساسة باستخدام:

AES Encryption

OpenSSL

البيانات التي يجب تشفيرها

- cardnumber
- cvv
- expiredate
- wallet_number

الفوائد

- حماية البيانات حتى في حال اختراق السيرفر .
- الامتثال للمعايير الأمنية .
- تقليل مخاطر تسرب البيانات .

3. حماية لوحة التحكم من Brute Force

الوضع الحالي

لا يوجد نظام منع لمحاولات تسجيل الدخول المتكررة.

المخاطر

- تخمين كلمات المرور .
- اختراق لوحة الإدارة .

التحسين المقترح

إضافة:

- عدد محاولات محدود .
- حظر مؤقت IP.
- Google reCAPTCHA.
- تسجيل محاولات الدخول .

الفوائد

- تقليل احتمالية الاختراق .
- منع الهجمات الآلية .

4. استخدام CSRF Protection

الوضع الحالي

طلبات POST لا تحتوي على CSRF Token.

المخاطر

إمكانية تنفيذ طلبات مزورة من مواقع خارجية.

التحسين المقترح

إضافة:

`$_SESSION['csrf_token']`

وفحصه مع كل عملية حساسة.

الفوائد

- منع تنفيذ العمليات المزورة .
- حماية العمليات الإدارية .

5. تحسين حماية Sessions

التحسينات المقترحة

تفعيل:

```
session_regenerate_id(true);
```

وضبط:

```
httponly
```

```
secure
```

```
samesite
```

الفوائد

- منع سرقة الجلسات .
- حماية تسجيل الدخول .

6. تسجيل النشاطات (Activity Logs)

التحسين المقترح

إنشاء جدول:

```
activity_logs
```

لتسجيل:

- تغيير الحالة
- تسجيل الدخول
- التعديلات
- العمليات الحساسة

الفوائد

- تتبع العمليات .

- معرفة مصدر المشاكل .
- دعم التدقيق الأمني .

7. إخفاء أخطاء قواعد البيانات

الوضع الحالي

قد يتم عرض أخطاء PDO مباشرة.

المخاطر

- كشف أسماء الجداول .
- كشف بنية النظام .

التحسين المقترح

عرض رسائل عامة فقط للمستخدم.

مثال:

حدث خطأ بالنظام

مع حفظ التفاصيل داخل Log داخلي.

الفوائد

- تقليل المعلومات المتاحة للمهاجم .

8. التحقق من المدخلات Validation

التحسينات المطلوبة

التحقق من:

- طول البطاقة
- نوع البيانات
- الصيغ
- المبالغ
- المدخلات الفارغة

الفوائد

- تقليل البيانات الخاطئة .
- حماية إضافية من الهجمات .

9. تفعيل Content Security Policy

التحسين المقترح

إضافة Headers مثل:

Content-Security-Policy
X-Frame-Options
X-XSS-Protection

الفوائد

- منع XSS.
- منع Clickjacking.

10. فصل صلاحيات المستخدمين

التحسين المقترح

إضافة أدوار:

- Super Admin
- Employee
- Viewer

الفوائد

- تقليل الوصول غير المصرح .
- تنظيم الإدارة .

ثانياً: تحسينات الأداء (Performance Improvements)

1. استخدام WebSocket بدلاً من AJAX Polling

الوضع الحالي

يتم التحديث كل:

setInterval(...)

المشكلة

- استهلاك زائد للسيرفر .
- طلبات متكررة غير ضرورية .

التحسين المقترح

استخدام:

WebSocket

Socket.IO

Ratchet PHP

الفوائد

- تحديث لحظي حقيقي .
- تقليل الضغط على السيرفر .
- استجابة أسرع .

2. تحميل البيانات الجزئي Lazy Loading

الوضع الحالي

تحميل كامل الجدول كل مرة.

المشكلة

بطء عند زيادة عدد السجلات.

التحسين المقترح

تحميل:

- السجلات الجديدة فقط .
- أو . Pagination Server Side

الفوائد

- تحسين السرعة .
- تقليل استهلاك الإنترنت .

3. تحسين الفهارس Indexes

التحسين المقترح

إضافة فهارس على:

status
created_at
type
numberaccount

الفوائد

- تسريع البحث .
- تسريع الفرز .
- تسريع التقارير .

4. استخدام Cache

التحسين المقترح

استخدام:

Redis
Memcached

لتخزين

- الجلسات
- النتائج المتكررة
- الإعدادات

الفوائد

- تقليل ضغط قاعدة البيانات .
- تحسين سرعة الاستجابة .

5. ضغط الملفات وتقليل الأحجام

التحسين المقترح

تفعيل:

GZIP Compression

Minify CSS/JS

الفوائد

- تحميل أسرع .
- استهلاك أقل للبيانات .

6. تحسين استعلامات SQL

التحسين المقترح

بدلاً من:

SELECT *

استخدام:

SELECT id,status,amount

الفوائد

- تقليل استهلاك الذاكرة .
- تسريع الاستعلامات .

7. استخدام Queue للمهام الثقيلة

التحسين المقترح

تنفيذ العمليات الخلفية عبر Queue.

مثل:

- الإشعارات
- التصدير
- السجلات

الفوائد

- عدم تجميد الواجهة .
- أداء أفضل .

ثالثاً: تحسينات تجربة المستخدم (UX Improvements)

1. إشعارات Toast احترافية

بدلاً من:

alert()

استخدام:

SweetAlert

Toastr

الفوائد

- واجهة احترافية .
- تجربة أفضل .

2. إضافة لوحة إحصائيات

تتضمن

- عدد الطلبات
- عدد السحب
- عدد الإيداع
- الطلبات المعلقة
- الطلبات المقبولة

الفوائد

- رؤية أوضح للإدارة .

3. دعم الوضع الليلي

الفوائد

- راحة المستخدم .
- مظهر احترافي .

4. تحسين تصميم الجوال

الفوائد

- دعم الأجهزة المحمولة .
- سهولة الإدارة من الهاتف .

رابعاً: تحسينات البنية التقنية (Architecture)

1. استخدام MVC Architecture

الوضع الحالي

المنطق مختلط مع الواجهة.

التحسين المقترح

تقسيم:

- Models
- Views
- Controllers

الفوائد

- سهولة التطوير .
- سهولة الصيانة .

2. استخدام API REST

الفوائد

- ربط تطبيقات الهاتف .
- ربط أنظمة أخرى .
- فصل الواجهة عن السيرفر .

3. استخدام Composer

الفوائد

- إدارة المكتبات .
- تحديث سهل .
- تنظيم المشروع .

خامساً: تحسينات المراقبة والإدارة

1. نظام نسخ احتياطي تلقائي

الفوائد

- حماية البيانات .
- استعادة سريعة .

2. نظام مراقبة الأخطاء

أدوات مقترحة

- Sentry
- Bugsnag

الفوائد

- اكتشاف المشاكل بسرعة .

3. مراقبة الأداء

أدوات مقترحة

- New Relic
- Grafana

الفوائد

- معرفة الاختناقات .

تقرير تحسين الأداء والأمان للنظام

- تحليل استهلاك السيرفر .

سادساً: توصيات احترافية مستقبلية

تطوير تطبيق موبايل

باستخدام:

- Flutter
- React Native

إضافة OTP Verification

للتحقق من العمليات.

إضافة نظام إشعارات فورية

- Telegram Bot
- Email
- SMS

إضافة نظام تقارير متقدم

يشمل:

- الرسوم البيانية
- الإحصائيات
- التحليلات

الخلاصة

النظام الحالي يعتبر قاعدة جيدة وقابلة للتطوير، لكن تطبيق التحسينات السابقة سيؤدي إلى:

تحسين الأمان عبر:

تقرير تحسين الأداء والأمان للنظام

- التشفير
 - حماية الجلسات
 - الحماية من الهجمات
 - تسجيل النشاطات
- تحسين الأداء عبر:

- WebSocket
 - Cache
 - تحسين قواعد البيانات
 - التحميل الجزئي
- تحسين الإدارة عبر:

- لوحات إحصائية
 - صلاحيات
 - مراقبة مباشرة
- تحسين تجربة المستخدم عبر:

- إشعارات حديثة
- تصميم متجاوب
- تحديثات لحظية
- الدعم الفني من خلال رقم موبايل و واتس اب
- تضمين بيانات المستخدم من اجل التواصل مثل رقم موبايل او ايميل

وبذلك يصبح النظام أكثر جاهزية للاستخدام الاحترافي والإنتاجي على نطاق واسع.