Ghost
Production Brief

פרקים

01 סיכום מנהלים
02 אבטחה ויציבות
03 מה נשאר

מה בעצם עשינו כאן? תסביר כמו לדירקטוריון.

CONFIDENTIAL · PRODUCTION READINESS BRIEF

ביצענו "שיפוץ לפני פתיחה לקהל" — לא בנינו בניין חדש.

דמיינו מפעל שכבר מייצר מוצר מצוין, אבל לפני שפותחים את השער ללקוחות חיצוניים — עברנו ביקורת מהנדס, אבטחה, כבישים ומערכות גיבוי. זה בדיוק מה שקרה ב-Ghost: המוצר עבד, אבל לא היה מוכן לעומס, לפריצות ולתקלות בשטח.

התהליך חולק לחמישה שלבים, כמו חמש קומות בבדיקת בטיחות: קודם מנעולים ומפתחות (אבטחה), אחר כך מערכות כיבוי אש אוטומטיות (יציבות), שומרים בכניסה (הקשחה), שיפוץ חדרי המתנה (ביצועים ו-UX), ומצלמות אבטחה בלובי (ניטור).

5	16	+60	0
שלבי הבשלה	משימות שבוצעו	קבצים שעודכנו	מפתחות בקוד לקוח

Ghost
Production Brief

פרקים

01 סיכום מנהלים

02 אבטחה ויציבות

03 מה נשאר

מה השתנה בפועל? תן אנלוגיות.

- **אבטחה — "החלפת מנעולים והוצאת מפתחות מהכיס"**
  מפתח OpenAI שהיה חשוף בקוד הלקוח הוסר. כמו להוציא מפתח ראשי מתחת לשטיח הכניסה ולהעביר אותו לכספת בבנק. הדמו עובר דרך שרת מוגן, לא דרך הדפדפן.
- **אבטחה — "שומר בדלת הנתונים הרגישים"**
  רשימות לידים, קורות חיים וחשבונות דמו ננעלו מאחורי טוקן אדמין. כמו מחסן עם כספות — לא כל מי שנכנס לבניין רואה את התוכן.
- **אבטחה — "תיקון דלתות שלא ננעלו"**
  תוקנו חורים שאפשרו לגשת לשיחות של אחרים (IDOR). כמו דלתות משרד שנפתחו עם מפתח של שכן — עכשיו כל מפתח פותח רק את החדר שלו.
- **יציבות — "מערכת כיבוי אש אוטומטית + כפתור עצירה"**
  נוסף CI שבודק כל שינוי לפני מיזוג (כמו בדיקת מפעל לפני משמרת). תוקן ביטול תגובות בזמן אמת, מניעת "הבזקים" במעבר בין שיחות, ואישור לפני מחיקה.
- **הקשחה — "שומר בכניסה + מגבלת גודל חבילות"**
  Rate limiting על פעולות יקרות (כמו מגביל כניסות לקונצרט). הגבלת גודל תמונות והעלאות. CVs מוגנים — כמו ארכיון שדורש תעודה מיוחדת.
- **תשתית — "גנרטור גיבוי לבניין בודד"**
  החלטנו להישאר על שרת יחיד מוקשח (לא לבנות עיר חדשה עכשיו). שופרו מיגרציות DB, ניקוי זיכרון, וכיבוי מסודר של תהליכי רקע.

שלבים 0–3: אבטחה · יציבות · הקשחה · תשתית

כל שינוי נבדק: smoke tests + build + סריקת סודות

פרקים

01 סיכום מנהלים

02 אבטחה ויציבות

03 מה נשאר

אז אנחנו מוכנים לפרודקשן? מה עדיין דורש יד אנושית?

- **ביצועים — "פירוק מזוודות כבדות לפני העלייה למטוס"**
  פיצול קוד לחבילות קטנות יותר, זיכרון חכם לרכיבים חמים. כמו לא לטעון את כל המזוודות לתא המטען אחת — כל אחת במקום הנכון.
- **ניטור — "מצלמות ומד חום בלובי"**
  נוספו בדיקות בריאות עמוקות (/health/ready), מזהה מעקב לכל בקשה, ותמיכה ב-Sentry לדיווח תקלות. כמו מרכז בקרה שרואה מי נכנס, מתי, ומה קרה.
- **תוצאה — "הבניין עבר בדיקה, אבל עדיין לא נפתח לקהל"**
  המערכת חזקה משמעותית: אין מפתחות בחוץ, יש שומרים, יש כפתור חירום, יש מצלמות. אבל לפני פתיחה מלאה — שלוש פעולות ידניות חובה.
- **ידנית 1 — "ביטול מפתח ישן בכספת החיצונית"**
  לסובב ולבטל את מפתח OpenAI שנחשף בעבר ב-Dashboard. כמו לבטל כרטיס אשראי שאבד — גם אחרי שהחלפנו את המנעול.
- **ידנית 2–3 — "ניקוי ארכיון + דיפלוי ראשון עם סודות חדשים"**
  ניקוי היסטוריית git מהמפתח הישן (דורש אישור מפורש). דיפלוי עם GHOST_DEMO_API_KEY ו-GHOST_ADMIN_TOKEN מוגדרים מראש.

בשורה התחתונה: עברנו מ"בית שעובד" ל"בית מבוטח, מבוקר ומוכן לפתיחה" — עם רשימת פעולות קצרה לסגירה סופית לפני הדלת נפתחת לעולם.

השלב הבא: סיבוב מפתח · דיפלוי · בדיקת עומס