ΤΟ ΕΓΧΕΙΡΙΔΙΟ · ΕΚΔΟΣΗ 1

Vibe101

Από τη λευκή σελίδα σε ένα ασφαλές, νόμιμο και ευρέσιμο προϊόν – ένα κουτάκι τη φορά. Δεν χρειάζονται γνώσεις προγραμματισμού.

ΔΩΡΕΑΝ ΔΕΙΓΜΑ

ΕΛΛΗΝΙΚΑ

Πώς να χρησιμοποιήσεις τον οδηγό

Ακολούθησε τη σειρά

Κάθε κεφάλαιο προϋποθέτει ότι το προηγούμενο έχει τελειώσει. Αν προσπεράσεις, το project μπερδεύεται.

Τσέκαρε το κουτάκι

Κάθε βήμα έχει ένα κουτάκι. Κάνε κλικ σε πρόγραμμα ανάγνωσης PDF (Preview, Acrobat, Chrome) και μένει τσεκαρισμένο όταν αποθηκεύσεις.

Αντίγραψε τις εντολές

Τα σκούρα πλαίσια είναι κείμενα για επικόλληση στο Claude. Αντικατέστησε ό,τι είναι σε [αγκύλες] με τα δικά σου.

Εμπιστεύσου το «Τελείωσες όταν»

Κάθε βήμα κλείνει με έναν έλεγχο που βλέπεις μόνος σου. Αν δεν τον βλέπεις, το βήμα δεν έχει τελειώσει.

Κόλλησες;

Επικόλλησε το ακριβές μήνυμα σφάλματος στο Claude και γράψε: «εξήγησέ το απλά και μετά διόρθωσέ το». Ποτέ μην επικολλάς κωδικούς ή κλειδιά.

Πρώτα τα χρήματα

Κάθε κεφάλαιο σημειώνει τι κοστίζει και πώς μπαίνει όριο. Βάλε τα όρια πριν χτίσεις, όχι μετά.

Το Vibe101 είναι εκπαιδευτικό υλικό και όχι νομική, φορολογική ή ασφαλιστική συμβουλή για τη δική σου περίπτωση. Οι νόμοι και οι κανόνες των πλατφορμών αλλάζουν: έλεγξε τους ισχύοντες κανόνες στη χώρα σου ή ρώτησε επαγγελματία πριν ανοίξεις το προϊόν.

Περιεχόμενα

00 **Ιδέα και πεδίο** — Ξέρε τι χτίζεις, για ποιον, και τη μικρότερη έκδοση που αξίζει να βγει.

01 **Λογαριασμοί και εργαλεία** — Οι λίγοι λογαριασμοί που χρειάζεσαι, με τη σωστή σειρά, και σε τι χρησιμεύει ο καθένας.

02 **Στήσιμο του project** — Ένας φάκελος, ένα αποθετήριο, ένα αρχείο μνήμης — για να μη χάνεται τίποτα.

03 **Χτίζοντας με το Claude** — Πώς να ζητάς, να ελέγχεις και να βγάζεις μικρές αλλαγές χωρίς να χαλάς τίποτα.

04 **Πρώτα η ασφάλεια** — Κράτα τα μυστικά κρυφά, κλείδωσε τη βάση, βάλε όρια στα έξοδα, επιτέθηκε στη δική σου εφαρμογή.

05 **Νομικός έλεγχος** — Οι παγίδες που φέρνουν πρόστιμα στις μικρές ιστοσελίδες: συναίνεση, γραμματοσειρές, email, ανανεώσεις.

06 **Χρήματα και μηνύματα** — Πληρωμές, email και AI χωρίς εκπλήξεις στον λογαριασμό.

07 **Ανέβασμα στον αέρα** — Σε πραγματικό domain, με έναν ασφαλή τρόπο ανάπτυξης (deploy).

08 **Να σε βρίσκουν Google και Bing** — Sitemaps, canonicals, ανακατευθύνσεις και webmaster tools, σωστά.

09 **Εκκίνηση και πρώτοι πελάτες** — Νόμιμη προσέγγιση, περιεχόμενο και τι να μετράς.

10 **Λειτουργία και συντήρηση** — Αντίγραφα ασφαλείας, ενημερώσεις, αλλαγή κλειδιών και ήρεμη λίστα για έκτακτα.

ΚΕΦΑΛΑΙΟ 04

Πρώτα η ασφάλεια

Κανείς δεν μπορεί να διαβάσει, να αλλάξει ή να σου φορτώσει λογαριασμό για κάτι που δεν του ανήκει. Κάνε αυτό το κεφάλαιο πριν δείξεις το προϊόν σε οποιονδήποτε.

ΧΡΟΝΟΣ
2–3 ώρες

ΧΡΕΙΑΖΕΣΑΙ
Τον φάκελο του project, τον πίνακα ελέγχου της βάσης, το Claude Code

01 Κράτα τα μυστικά έξω από τον κώδικα

Μυστικό είναι κάθε κωδικός, API key ή token. Αν μπει στον κώδικα, όποιος δει τον κώδικα μπορεί να το χρησιμοποιήσει. Ό,τι βρίσκεται στον browser είναι δημόσιο, άρα ένα κλειδί στον front-end κώδικα είναι κλειδί που διέρρευσε.

- Βάλε τα μυστικά μόνο σε αρχείο `.env.local` (ή στην οθόνη Environment Variables του host σου).
- Πρόσθεσε `.env*` στο `.gitignore` και κλείδωσε το αρχείο: `chmod 600 .env.local`.
- Οι μεταβλητές που ξεκινούν με `VITE_` ή `NEXT_PUBLIC_` στέλνονται σε κάθε επισκέπτη. Ποτέ μυστικό εκεί.
- Πριν από κάθε commit τρέξε `git status`. Ποτέ `git add -A` χωρίς να κοιτάξεις.

ΕΠΙΚΟΛΛΗΣΕ ΣΤΟ CLAUDE

```
Έλεγξε αυτό το project για μυστικά στον κώδικα ή στο ιστορικό git, για αρχεία .env που δεν είναι στο .gitignore και για τιμές που μοιάζουν με μυστικά σε μεταβλητές VITE_ ή NEXT_PUBLIC_. Κατάγραψε κάθε εύρημα και διόρθωσέ το. Μην τυπώσεις τις τιμές των μυστικών.
```

> **ΤΕΛΕΙΩΣΕΣ ΟΤΑΝ** Το `git status` δεν δείχνει κανένα αρχείο `.env` και ο παραπάνω έλεγχος δεν αναφέρει τίποτα.

02 Κλείδωσε τη βάση δεδομένων

Η βάση σου έχει δύο κλειδιά. Το δημόσιο ζει στον browser· το μυστικό ζει μόνο στον server σου. Το Row Level Security (RLS) είναι ο κανόνας που εμποδίζει το δημόσιο κλειδί να διαβάζει γραμμές άλλων.

- Ενεργοποίησε το RLS σε κάθε πίνακα. Πίνακας με RLS και χωρίς policy είναι κλειστός — η ασφαλής προεπιλογή.
- Γράψε ένα policy ανά ανάγκη («ο χρήστης βλέπει μόνο τις δικές του γραμμές»). Απλά και σύντομα.
- Χρησιμοποίησε το μυστικό κλειδί μόνο σε κώδικα server, ποτέ στον browser.

ΕΠΙΚΟΛΛΗΣΕ ΣΤΟ CLAUDE

```
Κατάγραψε όλους τους πίνακες της βάσης. Για καθέναν πες μου αν το RLS είναι ενεργό και δείξε τα policies του. Ενεργοποίησε το RLS όπου είναι κλειστό και γράψε το μικρότερο policy που αφήνει έναν συνδεδεμένο χρήστη να διαβάζει και να αλλάζει μόνο τις δικές του γραμμές.
```

> **ΤΕΛΕΙΩΣΕΣ ΟΤΑΝ** Με το δημόσιο κλειδί μόνο, δεν μπορείς να διαβάσεις γραμμή άλλου χρήστη. Δοκίμασέ το και δες το σφάλμα.

03 Βάλε όριο αιτημάτων σε κάθε δημόσια ή ακριβή διαδρομή

Ό,τι μπορεί να καλέσει ένας άγνωστος — σύνδεση, εγγραφή, φόρμα επικοινωνίας, AI chat — μπορεί να κληθεί 10.000 φορές από ένα script. Το όριο λέει «πολλά αιτήματα, δοκίμασε αργότερα».

- Όριο ανά διεύθυνση IP και, μετά τη σύνδεση, ανά χρήστη.
- Οι host που τρέχουν πολλά μικρά αντίγραφα του server (serverless) δεν μοιράζονται μνήμη, οπότε ένας μετρητής στη μνήμη δεν δουλεύει. Χρησιμοποίησε κοινό χώρο, όπως Redis ή πίνακα βάσης.
- Επέστρεψε την τυπική απάντηση `429 Too Many Requests`.

ΕΠΙΚΟΛΛΗΣΕ ΣΤΟ CLAUDE

```
Κατάγραψε όλες τις δημόσιες διαδρομές API του project. Πρόσθεσε όριο αιτημάτων σε καθεμία,
με κοινό χώρο που δουλεύει σε serverless hosting. Αυστηρότερα όρια σε σύνδεση, εγγραφή,
αποστολή email και AI. Πρόσθεσε τεστ που στέλνει 30 γρήγορα αιτήματα και περιμένει 429.
```

ΤΕΛΕΙΩΣΕΣ ΟΤΑΝ Τριάντα γρήγορα αιτήματα στη διαδρομή σύνδεσης καταλήγουν σε `429`.

04 Θωράκισε τη σύνδεση

Το να κρύψεις ένα κουμπί δεν είναι ασφάλεια. Ο server πρέπει να ελέγχει ποιος είσαι και τι δικαιούσαι σε κάθε αίτημα.

- Έλεγχος δικαιωμάτων στον server για κάθε ενέργεια, όχι μόνο στην οθόνη.
- Απαίτησε αξιοπρεπή κωδικό (12+ χαρακτήρες) ή χρησιμοποίησε σύνδεση με magic link· πρόσφερε 2-βήματη επαλήθευση στους διαχειριστές.
- Επιβράδυνε τις επαναλαμβανόμενες αποτυχίες. Ποτέ προεπιλεγμένο username ή κωδικός.
- Περιοχές διαχείρισης: επέτρεψε μόνο συγκεκριμένη λίστα email προσωπικού.

ΕΠΙΚΟΛΛΗΣΕ ΣΤΟ CLAUDE

```
Έλεγξε κάθε διαδρομή που αλλάζει δεδομένα. Δείξε μου ποιες ελέγχουν στον server την
ταυτότητα και το δικαίωμα του χρήστη και ποιες βασίζονται στο ότι η οθόνη κρύβει την
επιλογή. Διόρθωσε τα κενά και πρόσθεσε τεστ που καλεί κάθε προστατευμένη διαδρομή χωρίς
σύνδεση και περιμένει άρνηση.
```

ΤΕΛΕΙΩΣΕΣ ΟΤΑΝ Αν καλέσεις διαδρομή διαχείρισης χωρίς σύνδεση, παίρνεις σφάλμα — ποτέ δεδομένα.

05 Βάλε πλαφόν σε ό,τι κοστίζει (AI και πληρωμένες υπηρεσίες)

Ένα bug, ένας βρόχος ή ένας επιτιθέμενος μπορεί να κάνει ένα AI ή SMS feature λογαριασμό τεσσάρων ψηφίων μέσα σε μια νύχτα. Τα πλαφόν μετατρέπουν την καταστροφή σε ενόχληση.

- Όρισε σκληρό μηνιαίο όριο στον πίνακα του παρόχου.
- Δώσε σε κάθε χρήστη μηνιαία ποσόστωση (credits) και σταμάτα όταν τελειώσει.
- Βάλε μέγιστο αριθμό βημάτων σε κάθε βρόχο που καλεί πληρωμένη υπηρεσία.
- Ενεργοποίησε ειδοποίηση δαπάνης στο email σου.

ΕΠΙΚΟΛΛΗΣΕ ΣΤΟ CLAUDE

```
Βρες κάθε κλήση σε πληρωμένο API στο project (AI, SMS, email, χάρτες). Για καθεμία πρόσθεσε μηνιαία ποσόστωση ανά χρήστη, μέγιστο αριθμό επαναλήψεων βρόχου και σαφές σφάλμα όταν φτάνει το όριο. Κατάγραψε τι άλλαξες.
```

ΤΕΛΕΙΩΣΕΣ ΟΤΑΝ Έφτασες επίτηδες στο όριο στο τεστ και βλέπεις το σαφές σφάλμα, όχι κρασάρισμα.

06 Αποτυχία προς την ασφαλή πλευρά

Όταν ένας έλεγχος ασφαλείας δεν μπορεί να τρέξει — λείπει κλειδί, πέφτει μια υπηρεσία — η απάντηση πρέπει να είναι «όχι». Ένας έλεγχος που κλείνει σιωπηλά όταν λείπει το κλειδί του είναι ανοιχτή πόρτα.

- Ψάξε κώδικα του τύπου «έλεγξε μόνο αν υπάρχει το κλειδί». Κάν' τον να αρνείται.
- Αφαίρεσε κάθε «προσωρινή» παράκαμψη πριν την έναρξη.

ΕΠΙΚΟΛΛΗΣΕ ΣΤΟ CLAUDE

```
Ψάξε στον κώδικα για ελέγχους ασφαλείας που παραλείπονται όταν λείπει ένα μυστικό ή μια ρύθμιση (captcha, υπογραφή webhook, auth). Άλλαξε τον καθένα ώστε να απορρίπτει το αίτημα, και εξήγησε κάθε αλλαγή σε μία γραμμή.
```

ΤΕΛΕΙΩΣΕΣ ΟΤΑΝ Αν αφαιρέσεις το μυστικό, η προστατευμένη ενέργεια απορρίπτεται, δεν επιτρέπεται.

07 Επιτέθηκε στη δική σου εφαρμογή

Ένας πράσινος σαρωτής αποδεικνύει λίγα. Δοκίμασε να τη χαλάσεις όπως θα έκανε ένας άγνωστος και κράτα τα τεστ για πάντα.

- Ζήτα δεδομένα άλλου χρήστη αλλάζοντας τον αριθμό στο URL.
- Κάλεσε κάθε διαδρομή χωρίς σύνδεση, με λάθος σύνδεση και με τεράστιο input.
- Γράψε `<script>` σε κάθε πεδίο κειμένου και δες τι εμφανίζεται.
- Πάτα δύο φορές γρήγορα το κουμπί αγοράς.

ΕΠΙΚΟΛΛΗΣΕ ΣΤΟ CLAUDE

```
Λειτούργησε ως επιτιθέμενος απέναντι σε αυτή την εφαρμογή στον τοπικό μου υπολογιστή. Γράψε αυτοματοποιημένα τεστ που δοκιμάζουν: ανάγνωση δεδομένων άλλου χρήστη, κλήση προστατευμένων διαδρομών χωρίς σύνδεση, υπερβολικά μεγάλα input, script injection σε πεδία κειμένου και διπλή υποβολή πληρωμής. Τρέξε τα και πες τι πέρασε.
```

ΤΕΛΕΙΩΣΕΣ ΟΤΑΝ Κάθε τεστ επίθεσης αποτυγχάνει να μπει και τα τεστ είναι αποθηκευμένα στο project.

08 Καθάρισε και μετά ανέβασε

Εκεί που μένουν τα υπολείμματα κρύβονται οι διαρροές. Κάν' το πριν το πρώτο δημόσιο deploy και μετά από κάθε μεγάλη αλλαγή.

- Σβήσε σκουπίδια: `.DS_Store`, logs, φακέλους build, αρχεία δοκιμών, άχρηστα πακέτα.
- Αν ένα κλειδί επικολλήθηκε ποτέ σε chat, email ή commit, θεώρησέ το διαρρευμένο: φτιάξε νέο και σβήσε το παλιό.
- Έλεγξε τα δημόσια αρχεία δεδομένων. Ένα αρχείο προς λήψη με τηλέφωνα ή email ιδιοκτητών είναι παραβίαση.

ΕΠΙΚΟΛΛΗΣΕ ΣΤΟ CLAUDE

```
Κατάγραψε αρχεία στο repo που δεν πρέπει να γίνουν commit (σκουπίδια, logs, build, αρχεία env, υπολείμματα τεστ) και ό,τι στο δημόσιο bundle περιέχει προσωπικά δεδομένα. Αφαίρεσέ τα και πρόσθεσε τις σωστές γραμμές στο .gitignore.
```

> ΤΕΛΕΙΩΣΕΣ ΟΤΑΝ Το `git status` είναι καθαρό και τα δημόσια αρχεία δεν περιέχουν προσωπικά δεδομένα.

Συνηθισμένες παγίδες

- Πραγματική περίπτωση: ένα αδέσποτο `.env.local` έγινε commit μία φορά. Μια ματιά στο `git status` θα το είχε πιάσει.
- Πραγματική περίπτωση: ένα δημόσιο αρχείο δεδομένων έστελνε τηλέφωνα ιδιοκτητών στον browser κάθε επισκέπτη. Κράτα τις ιδιωτικές στήλες έξω από ό,τι κατεβάζει ο browser.
- Ένας μετρητής στη μνήμη μοιάζει με όριο αιτημάτων αλλά δεν κάνει τίποτα σε serverless hosting.
- Κλειδιά που επικολλήθηκαν σε chat θεωρούνται διαρρευμένα. Αντικατέστησέ τα.

← ΠΙΣΩ ΣΤΑ ΠΕΡΙΕΧΟΜΕΝΑ

VIBE101

Μόλις τελείωσες ένα κεφάλαιο από τα έντεκα

Αυτό το δωρεάν δείγμα είναι το Κεφάλαιο 04, Πρώτα η ασφάλεια. Ο πλήρης οδηγός προσθέτει ιδέα και πεδίο, λογαριασμούς, στήσιμο, χτίσιμο με το Claude, νομικό έλεγχο, χρήματα και μηνύματα, ανέβασμα, ορατότητα στην αναζήτηση, εκκίνηση και συντήρηση, καθώς και τελικό έλεγχο και γλωσσάρι.

Πάρε τον πλήρη Vibe101 στο vibe101.eu