

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ & ΔΙΚΤΥΩΝ
2024-2025

Firebase Authentication (Google)



ΚΑΝΟΥΣΗΣ ΑΛΕΞΑΝΔΡΟΣ
1083813
a.kanousis@ac.upatras.gr

ΣΤΕΡΓΙΟΠΟΥΛΟΣ ΓΕΩΡΓΙΟΣ
1083861
gstergiopoulos@ac.upatras.gr

Περιεχόμενα

| | |
|---|----|
| Υπηρεσία Firebase Authentication (Google) | 3 |
| Περιγραφή υπηρεσίας..... | 3 |
| Δυνατότητες υπηρεσίας..... | 3 |
| Υποστήριξη Αυθεντικοποίησης | 3 |
| Multi-Factor Authentication (MFA)..... | 4 |
| Custom Authentication Systems..... | 4 |
| Ολοκλήρωση με το οικοσύστημα Firebase | 5 |
| Διαχείριση Χρηστών και Πρόσβασης | 5 |
| Παραμετροποιήσεις..... | 5 |
| Case Studies..... | 6 |
| Email and Password Login | 9 |
| Social Login (Google) | 10 |
| Anonymous Login | 10 |
| Password-less Login (via Email)..... | 11 |
| Phone Login..... | 13 |
| Παράρτημα | 14 |
| Κώδικας..... | 14 |
| Οδηγίες Εγκατάστασης | 14 |
| Demo Video..... | 14 |

Υπηρεσία Firebase Authentication (Google)

Περιγραφή υπηρεσίας

Οι περισσότερες σύγχρονες εφαρμογές, χρειάζεται να γνωρίζουν την ταυτότητα κάθε χρήστη που της χρησιμοποιεί. Συνεπώς, είναι υψίστης σημασίας να διαθέτουν ένα σύστημα αυθεντικοποίησης χρηστών, το οποίο προστατεύει τόσο τα δεδομένα των χρηστών αλλά και εξασφαλίζει στους διαχειριστές των εφαρμογών ότι μόνο εξουσιοδοτημένοι χρήστες θα έχουν πρόσβαση στην εφαρμογή.

Το Firebase Authentication είναι μια υπηρεσία που παρέχει η Google και δίνει την δυνατότητα στους δημιουργούς web και mobile εφαρμογών να κάνουν αυθεντικοποίηση των χρηστών. Είναι σχεδιασμένο να απλοποιεί την διαδικασία της αυθεντικοποίησης για τους developers εξασφαλίζοντας την ασφάλεια των δεδομένων και επιτρέποντας τους να προσθέσουν login και registration με διάφορους τρόπους και με ελάχιστο κώδικα. Αξιοποιώντας τον έλεγχο ταυτότητας Firebase, οι προγραμματιστές μπορούν να επικεντρωθούν στη δημιουργία λειτουργιών με επίκεντρο τον χρήστη, αφού έχουν εξασφαλίσει, μέσω των υποδομών της Google, την ασφαλή και αποδοτική διαχείριση των ταυτοτήτων των χρηστών.

Σημαντικό επίσης είναι πως η υπηρεσία διαθέτει pre-built UI που μπορεί να ενσωματωθεί στις εφαρμογές των προγραμματιστών κάνοντας την διαδικασία ακόμα πιο εύκολη, πράγμα που εμείς δεν αξιοποιήσαμε ωστόσο στα case studies μας.

Όσον αφορά τους χρήστες, η αξιοποίηση του Firebase Auth από τις εφαρμογές, έχει διάφορα πλεονεκτήματα. Για αρχή, το γεγονός ότι τα στοιχεία τους διαχειρίζονται από μια εταιρεία όπως η Google, τους εμπνέει μεγαλύτερη ασφάλεια, από ένα σύστημα αυθεντικοποίησης υλοποιημένο από κάποιον άγνωστο developer. Επιπλέον, το Firebase, παρέχει μια σειρά υπηρεσίες που θα δούμε παρακάτω, παρέχοντας στον χρήστη διάφορες επιλογές ταυτοποίησης που έχουν σκοπό να διευκολύνουν τον χρήστη.

Δυνατότητες υπηρεσίας

Η υπηρεσία προσφέρει ένα ευρύ φάσμα δυνατοτήτων, καθιστώντας την μια ευέλικτη λύση για τους προγραμματιστές, οι οποίοι μπορεί να επιλέξουν ανάλογα την υπηρεσία τους διαφορετικές επιλογές εισόδου ή και να τις συνδυάσουν. Οι δυνατότητες αυτές αναλύονται στην συνέχεια.

Υποστήριξη Αυθεντικοποίησης

Η είσοδος στην εφαρμογή μπορεί να γίνεται με διάφορους τρόπους που υποστηρίζονται από την υπηρεσία. Αρχικά κάθε χρήστης μπορεί να χρησιμοποιεί το προσωπικό του Email και Κωδικό Πρόσβασης που έχει επιλέξει κατά την διαδικασία του registration.

Επιπλέον, υπάρχει η δυνατότητα του Social Login που παρέχει απρόσκοπτη ενοποίηση με δημοφιλείς παρόχους ταυτότητας όπως το Google, το Facebook, το GitHub, η Apple και άλλα ακόμα. Με αυτή την δυνατότητα ο χρήστης δεν χρειάζεται να δημιουργεί ξεχωριστό λογαριασμό για την εφαρμογή αυτή αλλά να χρησιμοποιεί τους λογαριασμούς του από κάποια άλλη υπηρεσία.

Μια άλλη επιλογή για την αυθεντικοποίηση των χρηστών που δίνεται από την υπηρεσία είναι το Phone Authentication. Ο χρήστης συνδέεται στην εφαρμογή, αφού λάβει έναν κωδικό μίας χρήσης που περιέχεται σε ένα μήνυμα SMS που λαμβάνει στο κινητό που ορίζει ο ίδιος.

Επιπλέον υπάρχει και η επιλογή του Passwordless Login που μοιάζει με αυτή του Phone Authentication αλλά σε αυτή την περίπτωση ο χρήστης λαμβάνει ένα email το οποίο εμπεριέχει ένα link το οποίο πατώντας του δίνει πρόσβαση στην υπηρεσία.

Τέλος υπάρχει και η δυνατότητα του Anonymous Authentication, όπου ο χρήστης έχει πρόσβαση στην εφαρμογή κάνοντας χρήση προσωρινών ανώνυμων λογαριασμών για έλεγχο ταυτότητας με το Firebase. Αυτοί οι προσωρινοί ανώνυμοι λογαριασμοί μπορούν να χρησιμοποιηθούν για να επιτρέψουν στους χρήστες που δεν έχουν εγγραφεί ακόμα στην εφαρμογή να συνεργάζονται με δεδομένα που προστατεύονται από κανόνες ασφαλείας. Εάν ένας ανώνυμος χρήστης αποφασίσει να εγγραφεί στην εφαρμογή, μπορεί να συνδέσει τα διαπιστευτήρια σύνδεσής του με τον ανώνυμο λογαριασμό, ώστε να συνεχίσει να εργάζεται με τα προστατευμένα δεδομένα του σε μελλοντικές περιόδους σύνδεσης.

Multi-Factor Authentication (MFA)

Το MFA είναι ένα πρόσθετο επίπεδο ασφαλείας που χρησιμοποιείται για την επαλήθευση της ταυτότητας ενός χρήστη πέρα από ένα όνομα χρήστη και κωδικό πρόσβασης. Απαιτώντας πολλαπλές μορφές επαλήθευσης, το MFA μειώνει σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης, ακόμη και αν παραβιάζονται τα διαπιστευτήρια σύνδεσης.

Υπάρχουν δύο τρόποι να γίνει το MFA μέσω του Firebase. Ο πρώτος είναι με SMS ενώ ο δεύτερος είναι η χρήση time-based one-time password (TOTP). Με τον δεύτερο τρόπο οι χρήστες που προσπαθούν να μπουν στην εφαρμογή θα λαμβάνουν έναν request για να εισάγουν ένα TOTP. Για να το λάβουν πρέπει να χρησιμοποιήσουν ένα authenticator app, ικανό να δημιουργεί έγκυρους κωδικούς TOTP.

Custom Authentication Systems

Οι προγραμματιστές μπορούν να ενσωματώσουν τα προσαρμοσμένα συστήματα ελέγχου ταυτότητας χρησιμοποιώντας το σύστημα ελέγχου ταυτότητας Firebase που βασίζεται σε tokens. Αυτή η προσέγγιση επιτρέπει μεγαλύτερη ευελιξία, επιτρέποντας την ενοποίηση με παλαιού τύπου συστήματα ή την αντιμετώπιση μοναδικών επιχειρηματικών απαιτήσεων. Τα προσαρμοσμένα token μπορούν να δημιουργηθούν σε έναν ασφαλή διακομιστή και να επικυρωθούν από το Firebase, παρέχοντας μια ασφαλή και απρόσκοπτη εμπειρία χρήστη

προσαρμοσμένη στις συγκεκριμένες ανάγκες. Το πλεονέκτημα αυτής της μεθόδου είναι ότι μπορεί να υλοποιηθεί οποιοσδήποτε τρόπος αυθεντικοποίησης όπως πχ single sign-on (SSO), άλλες πλατφόρμες social login, που δεν υποστηρίζονται από το Firebase κλπ.

Ολοκλήρωση με το οικοσύστημα Firebase

Το Firebase Authentication ενσωματώνεται αβίαστα με άλλες υπηρεσίες Firebase, όπως το Firestore, το Firebase Realtime Database και το Firebase Cloud Functions, δίνοντας τη δυνατότητα στους προγραμματιστές να δημιουργούν εφαρμογές πλούσιες σε δυνατότητες. Για παράδειγμα, οι χρήστες με έλεγχο ταυτότητας μπορούν να έχουν απρόσκοπτη πρόσβαση στις βάσεις δεδομένων του Firestore, ενεργοποιώντας ενημερώσεις σε πραγματικό χρόνο ή λειτουργίες από την πλευρά του διακομιστή που βασίζονται σε καταστάσεις ελέγχου ταυτότητας. Επιπλέον, το Firebase Hosting μπορεί να οδηγήσει στην πλήρη ολοκλήρωση με το περιβάλλον της Firebase, καθώς προσφέρει δυνατότητα Hosting της web υπηρεσία που έχει δημιουργηθεί και κάνει χρήση του Firebase Auth. Αυτές οι λειτουργίες της Firebase, απλοποιούν την ανάπτυξη εφαρμογών και επιτρέπουν στους developers να επικεντρωθούν στη βελτίωση της βασικής εφαρμογής αντί να αναλώνονται στην δημιουργία και συντήρηση ξεχωριστών συστημάτων ελέγχου ταυτότητας.


Διαχείριση Χρηστών και Πρόσβασης

Το Firebase Authentication παρέχει ολοκληρωμένα εργαλεία για τη διαχείριση λογαριασμών χρηστών, συμπεριλαμβανομένης της δημιουργίας, της ενημέρωσης και της διαγραφής προφίλ χρηστών. Οι προγραμματιστές μπορούν εύκολα να εφαρμόσουν λειτουργίες όπως επαναφορά κωδικού πρόσβασης, επαλήθευση email και έλεγχος πρόσβασης.

Η διαχείριση πρόσβασης βελτιστοποιείται μέσω της ενσωμάτωσης με τους κανόνες ασφαλείας του Firebase, επιτρέποντας στους προγραμματιστές να ορίζουν αναλυτικές πολιτικές πρόσβασης που συνδέονται άμεσα με τις καταστάσεις ελέγχου ταυτότητας. Αυτό διασφαλίζει ότι οι χρήστες μπορούν να έχουν πρόσβαση μόνο σε δεδομένα ή λειτουργίες που έχουν εξουσιοδότηση να χρησιμοποιούν, βελτιώνοντας την ασφάλεια και τη συμμόρφωση της εφαρμογής.

Παραμετροποιήσεις

Σε όλες τις δυνατότητες του Firebase, δίνεται η δυνατότητα παραμετροποιήσεων. Μπορεί ο διαχειριστής να επιλέξει μεταξύ διάφορων επιλογών ανάλογα με τις απαιτήσεις του. Για παράδειγμα μπορεί να ορίσει πόσο αυστηρές θα είναι οι απαιτήσεις για τον κωδικό, δηλαδή πόσους χαρακτήρες θα πρέπει να είναι, αν θα περιέχει ειδικούς χαρακτήρες κλπ.. Επιπλέον μπορεί να ορίσει, επιλογές όπως αν ίδιος χρήστης μπαίνει με διαφορετικούς τρόπους αυθεντικοποίησης αν θα συνδέονται οι λογαριασμού του μεταξύ τους ή ακόμα μπορεί να ορίσει αν ο χρήστης μπορεί ο ίδιος να εγγραφεί ή να διαγραφεί από την σελίδα. Ενδεικτικά κάποιες φωτογραφίες από παραμετροποιήσεις:

| User account linking | User actions |
|--|---|
| When a user signs in using different identity providers, you can choose to automatically merge accounts on sign in. Learn more | Allow or forbid users from performing the following actions on their own accounts. You can always perform these actions using the Admin SDK. Learn more |
|  Link accounts that use the same email | <input checked="" type="checkbox"/> Enable create (sign-up) <input checked="" type="checkbox"/> Enable delete |

| | |
|---|--|
| <p>Sign-up quota</p> <p>To protect your project from abuse, we limit the number of new Email/Password and Anonymous accounts that your application can create in a day from a single IP address. Learn more</p> <p>Current quota per hour: 100</p> <hr/> <p>You can request temporary quota changes now or schedule them for the future here. Simply specify what you'd like your temporary quota to be, when you'd like the change to take place, and for how long. Please note that quota adjustments can take up to one hour to take effect.</p> <p>Maximum sign ups per hour</p> <input type="text" value="100"/> <p>Start date Time (GMT+2)</p> <div> <input type="text" value="12/24/2024"/> <input type="text" value="12:04"/> </div> <p>Duration (days)</p> <input type="text" value="1"/> | <p>Password policy</p> <p>With password policies, you can improve account security by enforcing password complexity requirements for your users who log in with email and password. Learn more</p> <hr/> <p>Enforcement mode</p> <p>Enforcement mode of password policies</p> <p> <input type="radio"/> Require enforcement Attempts to sign up fail until the user updates to a password that complies with your policy </p> <p> <input checked="" type="radio"/> Notify enforcement Users are allowed to sign up with a non-compliant password, and any missing criteria needed to satisfy the policy are returned </p> <p>Password requirement options</p> <div> <input type="checkbox"/> Require uppercase character <input type="checkbox"/> Require lowercase character </div> <div> <input type="checkbox"/> Require special character <input type="checkbox"/> Require numeric character </div> <div> <input type="checkbox"/> Force upgrade on sign-in </div> <p>Password length requirements</p> <p>Minimum password length</p> <input type="text" value="6"/> |
|---|--|

Case Studies

Ο κώδικας μπορεί να βρεθεί στο [GitHub](#).

Στην παρούσα εργασία, για να δείξουμε τις πρακτικές εφαρμογές του Firebase Authentication υλοποιήσαμε κάποιες από τις υπηρεσίες του Firebase για την είσοδο σε μια εφαρμογή web. Αυτή η υλοποίηση ενσωμάτωσε πολλαπλές μεθόδους ελέγχου ταυτότητας, καθεμία από τις οποίες αντιμετώπιζε συγκεκριμένες ανάγκες και σενάρια χρηστών.

Για το development έγινε χρήση της HTML, CSS, JS και της NodeJS. Επιπλέον χρησιμοποιήθηκε η βιβλιοθήκη Handlebars, η βοήθησε στην δημιουργία ενός δυναμικού και παραμετροποιήσιμου front-end για τις ανάγκες της εφαρμογής.



Μεθοδολογία Εργασίας:

- ☐ Έρευνα σχετικά με τις δυνατότητες του Firebase
- ☐ Δημιουργία ενός User Interface μέσω τεχνολογιών Web

Welcome Guest

Sign-in method: **Anonymous Login**

Logout

Project for "Computer & Network Security" Course

Department of Electrical and Computer Engineering

Developed by: **Alexandros Kanousis** | **up1083813** & **Georgios Stergiopoulos** | **up1083861**

For this project, we explored the secure sign-in options provided by Google's **Firebase Auth** and developed this web application presenting some use cases.

Our application provides the following sign-in methods:

- Email/Password Sign-in
- Google Sign-in
- Anonymous Sign-in
- Phone Sign-in
- Passwordless Sign-in

Find the code in our [GitHub Repo](#)

- Δημιουργία ενός backend server μέσω NodeJS, για προσθήκη λειτουργικότητας στην παραπάνω διεπαφή.
- Δημιουργία ενός Firebase Project, μέσω του Firebase Console. Το project έχει τις δυνατότητες που παρέχει η δωρεάν έκδοση του ονόματι Spark.

FirebaseAuthProjectHmty

cybersecurityhmtly

</>

- Σύνδεση του Firebase Project, με τον backend server μέσω των κατάλληλων NodeJS βιβλιοθηκών και των credentials που μας έδωσε το Firebase.

```
const firebaseConfig = {
  apiKey: "AIza[REDACTED]",
  authDomain: "cybersecurityhmtly.firebaseio.com",
  projectId: "cybersecurityhmtly",
  storageBucket: "cybersecurityhmtly.firebaseio.com",
  messagingSenderId: "[REDACTED]",
  appId: "1:617838396:[REDACTED]",
  measurementId: "G-8B270P5BTQ"
};

const authapp= initializeApp(firebaseConfig);
const auth= getAuth(authapp);

const googleProvider = new GoogleAuthProvider();
```

- Μελέτη του Firebase Auth documentation σχετικά με το πως θα υλοποιήσουμε τις διαφορετικές λειτουργίες.
- Επιλογή του Firebase SDK Authentication αντί για του FirebaseAuth, για να έχουμε πλήρη έλεγχο των επιλογών.
- Υλοποίηση διάφορων case studies που θα παρουσιαστούν στην επόμενη ενότητα.

Σε αυτό το σημείο, είναι ενδιαφέρον να σχολιάσουμε μια ιδιαιτερότητα που συναντήσαμε κατά την ανάπτυξη της εφαρμογής μας. Κάποιες δυνατότητες του FirebaseAuth, υλοποιήθηκαν στο backend της εφαρμογής μας, ωστόσο κάποιες άλλες όπως το Password less και το Phone, με βάση το documentation, υλοποιήθηκαν στο Front-end της ιστοσελίδας.

Email and Password Login

Η πρώτη πρακτική εφαρμογή του Firebase Authentication, έγινε για είσοδο στην ιστοσελίδα με email και password. Για να αποκτήσει ένας χρήστης προσωπικό λογαριασμό με τα στοιχεία του, υπάρχει η επιλογή «Create an account», όπου ο χρήστης μπορεί να πραγματοποιήσει την εγγραφή του στην υπηρεσία. Στην συνέχεια χρησιμοποιώντας τα στοιχεία αυτά, μπορεί να συνεχίσει με επιτυχία την είσοδο του στην ιστοσελίδα.

Καθ' όλη την διάρκεια ο χρήστης λαμβάνει τα κατάλληλα μηνύματα στην οθόνη του σχετικά με της ενέργειες του. (π.χ. “Your account has been created. Please login”, “Password should be at least 6 characters”). Στην εικόνα 1, βλέπουμε την αρχική οθόνη για είσοδο στην υπηρεσία. Σε περίπτωση που ο χρήστης επιλέξει την δημιουργία λογαριασμού, μεταφέρεται στην σελίδα της εικόνας 2 όπου εισάγει τα στοιχεία του.

Βασική οθόνη εισόδου

Δημιουργία λογαριασμού

Για να παρουσιάσουμε την λειτουργία αυτή, δημιουργήσαμε έναν λογαριασμό με email: login_password@test.gr. Αφού πραγματοποιήσουμε την εγγραφή αυτή, βλέπουμε στο Firebase console την εγγραφή αυτή να καταγράφεται στην βάση δεδομένων με τις απαραίτητες πληροφορίες για τον χρήστη όπως τον τρόπο εγγραφής του (provider) και την ημερομηνία δημιουργίας του λογαριασμού.

| Identifier | Providers | Created ↓ | Signed in | User UID |
|------------------------|-----------|-------------|-------------|-----------------------------|
| login_password@test.gr | 📧 | 24 Dec 2024 | 24 Dec 2024 | ukRcaiO7uNeJLvNpEuldqQLN... |

Firebase console, δεδομένα χρήστη

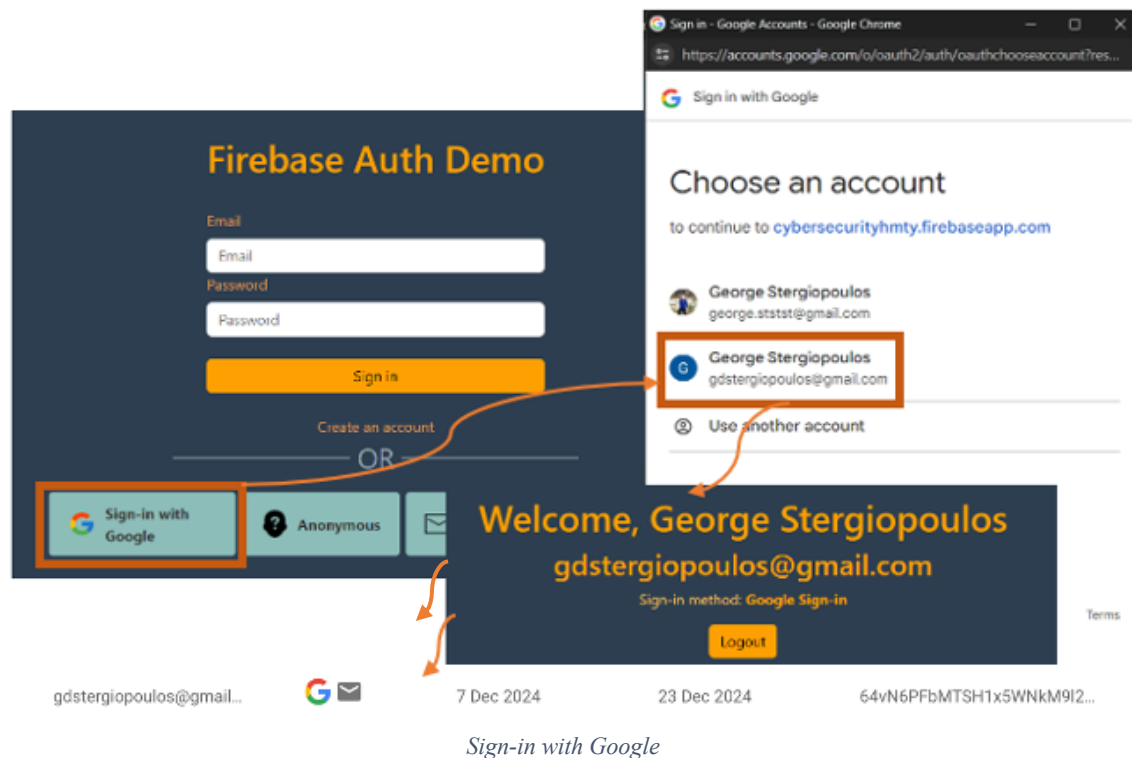
Ο χρήστης αυτός στην συνέχεια εισάγοντας το email και το password του στην αρχική σελίδα, αποκτά ταυτοποιημένη πρόσβαση στην ιστοσελίδα όπως φαίνεται στην εικόνα δεξιά. Με το κουμπί “Logout”, μπορεί στην συνέχεια να αποσυνδεθεί.

Επιτυχημένη είσοδος

Σε αυτό το σημείο θα ήταν ενδιαφέρον να σχολιάσουμε ότι σε περίπτωση που θα θέλαμε να συνδέσουμε τον χρήστη με κάποια έξτρα στοιχεία όπως όνομα κλπ, θα έπρεπε να κάνουμε χρήση του Firestore ή κάποιας δικιάς μας βάσης. Η απλή εκδοχή sign-in με email και password δεν κρατάει παραπάνω στοιχεία από αυτά τα δύο.

Social Login (Google)

Η επόμενη υπηρεσία που υλοποιήσαμε είναι το Social Login. Συγκεκριμένα επιλέξαμε να ενσωματώσουμε την επιλογή εισόδου στην ιστοσελίδα με λογαριασμό της Google. Με αντίστοιχο τρόπο όμως λειτουργεί και το Social Login με άλλες εταιρείες παροχής ταυτοποίησης χρηστών. Στην κεντρική οθόνη λοιπόν, ο χρήστης έχει την δυνατότητα να επιλέξει “Sign-in with Google” και όπως φαίνεται στην παρακάτω εικόνα, να πραγματοποιήσει την είσοδο του με όποιον λογαριασμό



Anonymous Login

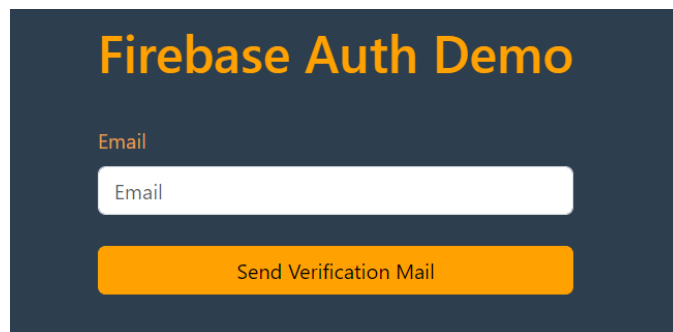
Μια ακόμα επιλογή εισόδου που υλοποιήθηκε είναι το Anonymous Login όπου ο χρήστης μπορεί να έχει πρόσβαση στην ιστοσελίδα χωρίς να δημιουργεί κάποιον λογαριασμό. Σε πραγματικές εφαρμογές τις περισσότερες φορές η είσοδος στις ιστοσελίδες γίνεται πάντα ως ανώνυμη και στην συνέχεια ο κάθε χρήστης μπορεί να συνδεθεί με έναν από τους υπόλοιπους τρόπους για να προχωρήσει σε προσωποποιημένες ενέργειες που απαιτούν ταυτοποίηση. Εμείς επιλέξαμε να το προσθέσουμε σαν επιλογή στην αρχική σελίδα εισόδου ώστε να διαχωρίσουμε όλες τις δυνατές επιλογές εισόδου για τους χρήστες που υλοποιήσαμε.



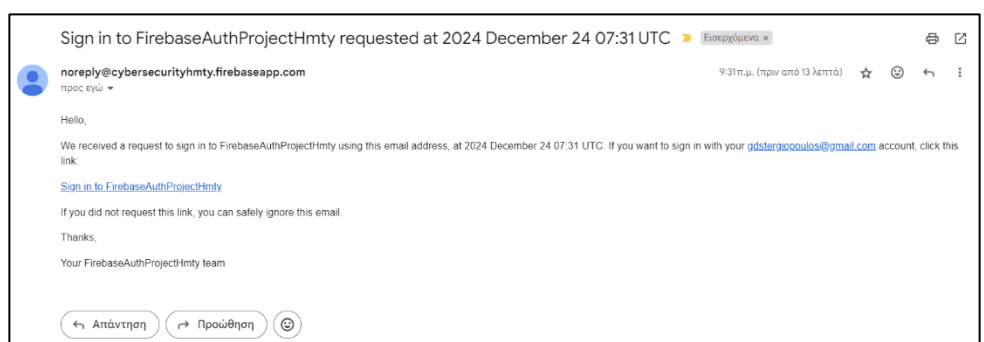
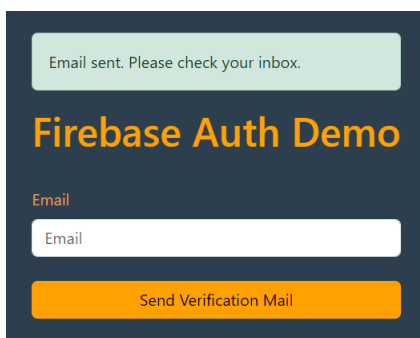
Password-less Login (via Email)

Για την σύνδεση χωρίς κωδικό, η διαδικασία έχει ως εξής:

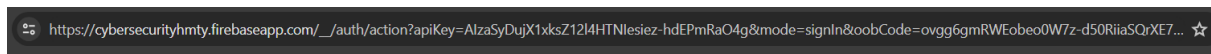
Ο χρήστης δίνει ένα έγκυρο Mail στο οποίο έχει πρόσβαση, και πατάει να λάβει ένα Verification Mail.



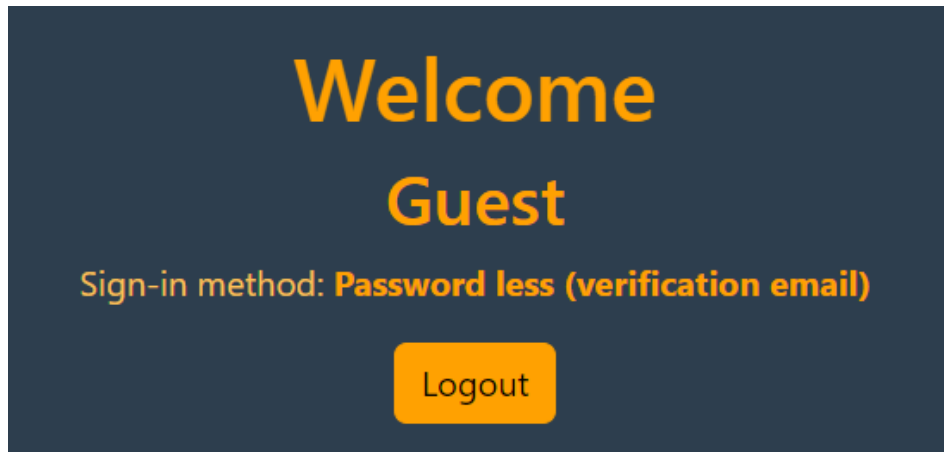
Άμα το Mail, είναι έγκυρο στον χρήστη στέλνετε ένα Mail, το κείμενο του οποίου μπορεί να το ορίσει ο διαχειριστής, ωστόσο αυτό θα περιέχει αναγκαστικά ένα verification link.



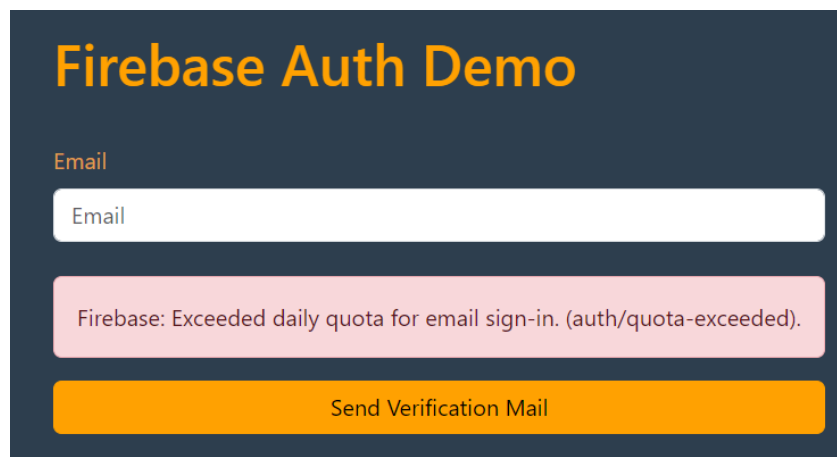
Μόλις πατήσει ο χρήστης στο link μεταβαίνει σε αυτή την σελίδα:



Και μόλις γίνει ο απαραίτητος έλεγχος, αν γίνει επιτυχώς η διαδικασία γίνεται sign-in και redirect στο Home page.

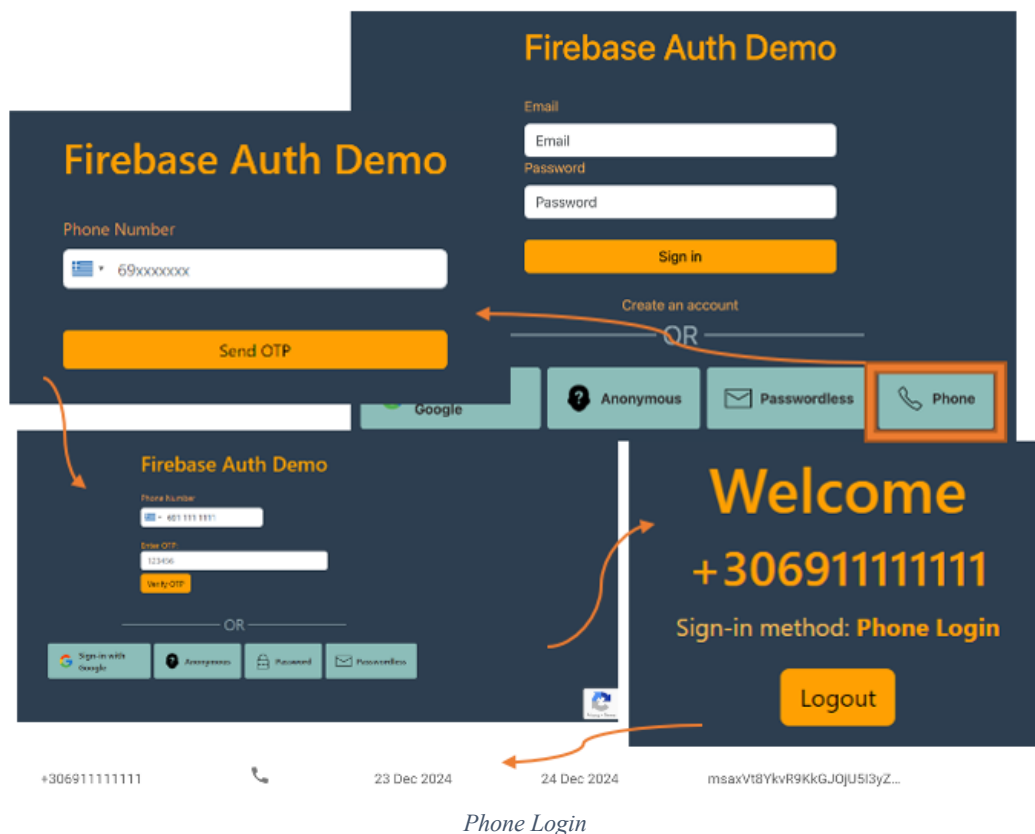


Δυστυχώς, αυτή η δυνατότητα έχει αυστηρούς περιορισμούς καθώς το δωρεάν πλάνο Spark του Firebase, μπορεί να στέλνει μέχρι 5 verification mail ανά μέρα με αποτέλεσμα συχνά να λαμβάνουμε το παρακάτω μήνυμα.



Phone Login

Η τελευταία μέθοδος που υλοποιήσαμε είναι το Phone Login. Η χρήστης έχει τη δυνατότητα να επιλέξει το τηλέφωνο με το οποίο επιθυμεί να γίνει η ταυτοποίηση. Στην συνέχεια λαμβάνει σε αυτό, τον μοναδικό κωδικό OTP που πληκτρολογεί στο αντίστοιχο πεδίο και αποκτά την πρόσβαση στην ιστοσελίδα. Λόγω του προγράμματος Spark του Firebase που διαθέτουμε, το οποίο είναι δωρεάν, δεν υπάρχει η δυνατότητα να αποστέλλουμε τον απαραίτητο κωδικό σε οποιοδήποτε κινητό επιθυμούμε. Σε περίπτωση που γίνει συνδρομή επι πληρωμή το σύστημα είναι έτοιμο να λειτουργήσει κανονικά. Για τις ανάγκες αυτής της εργασίας δημιουργήθηκε ένας demo αριθμός τηλεφώνου 691111111 με κωδικό OTP: 402026



Παράρτημα

Κώδικας

Ο κώδικας που γράφτηκε για τις ανάγκες των παραπάνω Case Study βρίσκεται στο παρακάτω [GitHub](#).

Οδηγίες Εγκατάστασης

- 1) Βεβαιωθείτε ότι ο υπολογιστής σας έχει εγκατεστημένη την NodeJS ή εγκαταστήστε την από [εδώ](#).
- 2) Κατεβάστε τον κώδικα από το Github ή εκτελέστε την εντολή `git clone http://github.com/gdstergiopoulos/FirebaseAuthProject`
- 3) Εκτελέστε (έχοντας βεβαιωθεί ότι το terminal σας βρίσκεται στο path όπου βρίσκεται ο κώδικας), τις παρακάτω εντολές
`npm install`
`npm start`
- 4) Δοκιμάστε την εφαρμογή μας στο <http://localhost:3000/>

Demo Video

Δείτε (πατώντας την εικόνα) το demo video που ετοιμάσαμε σε περίπτωση που δεν επιθυμείτε να ακολουθήσετε την παραπάνω διαδικασία ή δεν λειτούργησε στο σύστημα σας.

