Documentation for authentication process

ΠΑΡΑΣΚΕΥΑΣ ΛΟΥΚΑ - ΝΙΚΟΛΑΣ ΒΙΟΛΑΡΗ

TEAM 03

Η λογική υλοποίησης του authentication για τους χρήστες είναι βασισμένη στο $_SESSION του σερβερ όπου αποθηκεύονται κάποια στοιχεία σχετικά με τον κάθε client. Τα στοιχεία αυτά είναι:

1. authenticated, παίρνει την τιμή true αν ο χρήστης είναι authenticated, δηλαδή έχει δώσει username και password και έχουν πιστοποιηθεί ορθά, διαφορετικά το πεδίο αυτό έχει την τιμή false.
2. times, αρχικά για κάθε πελάτη είναι αρχικοποιημένη σε 0 και αυξάνεται κατά 1 κάθε φορά που ο συγκεκριμένος πελάτης προσπαθεί αν συνδεθεί στο σύστημα αποτυχημένα. Ο χρήστης έχει 3 προσπάθειες αποτυχίας, στην 4η προσπάθεια που ο χρήστης θα επιχειρήσει να συνδεθεί στο σύστημα θα του δοθεί μήνυμα ότι ξεπέρασε τις επιτρεπτές προσπάθειες και θα μπορεί να ξαναπροσπαθήσει μετά από 5 λεπτά.
3. last_login_time, σε αυτό το πεδίο καταχωρείται η ακριβής ώρα στην οποία ο χρήστης έκανε την υπέρβαση των επιτρεπτών προσπαθειών για σύνδεση στο σύστημα για να μας βοηθήσει να ξαναδώσουμε προσπάθεια σύνδεσης σε αυτόν μετά από 5 λεπτά.

Περιγραφή διαδικασίας:

Αρχικά ο χρήστης ανακατευθύνεται στην σελίδα σύνδεσης του συστήματος (index.html) και από εκεί έχει την δυνατότητα να δημιουργήσει καινούργιο λογαριασμό. Αφού δημιουργήσει το λογαριασμό του μπορεί να συνδεθεί στο σύστημα καταχωρώντας το username του και τον κωδικό πρόσβασης του. Με το που πατά log in αποστέλλεται αίτημα στο σερβερ με τα προσωπικά στοιχεία του χρήστη, στη πλευρά του σερβερ, ο κωδικός που στέλνει ο client γίνεται σε bcrypt, ανακτάται ο σωστός κωδικός του χρήστη και συγκρίνει τους δύο κωδικούς. Αν τα στοιχεία που έδωσε ο χρήστης είναι σωστά τότε η μεταβλητή authenticated στο session του σερβερ γίνεται true και αποστέλλεται μήνυμα επιτυχίας από το σερβερ στο πελάτη και ο χρήστης ανακατευθύνεται στην σελίδα map.php. Αν τα στοιχεία που έδωσε ο χρήστης είναι λανθασμένα τότε επιστρέφεται μήνυμα λάθους στο πελάτη, αυξάνεται η μεταβλητή times από το session κατά 1 και παραμένει στην σελίδα σύνδεσης. Αν ο χρήστης κάνει 3 αποτυχημένες προσπάθειες σύνδεσης, στην επόμενη προσπάθεια του θα του δοθεί μήνυμα λάθους που αναφέρει πως ξεπέρασε το μέγιστο επιτρεπτό όριο εσφαλμένων προσπαθειών σύνδεσης και

θα παίρνει το ίδιο μήνυμα για τα επόμενα 5 λεπτά μέχρι να του επιτραπεί να ξαναπροσπαθήσει.

Πιστοποίηση χρηστών και βάση δεδομένων:

Η πιστοποίηση των χρηστών γίνεται με την χρήση της βάσης δεδομένων όπου υπάρχουν καταχωρημένα το username κάθε χρήστη και ο κωδικός του που είναι σε bcrypt.

Περιορισμός πρόσβασης σε σελίδες και API χωρίς σύνδεση:

Οι χρήστες οι οποίοι δεν είναι authenticated δεν έχουν πρόσβαση σε καμία σελίδα του συστήματος εκτός από αυτή της σύνδεσης καθώς επίσης ούτε και στις λειτουργίες του API. Αυτό επιτυγχάνεται ελέγχοντας στην αρχή κάθε αρχείου του οποίου δεν θέλουμε να έχουν πρόσβαση μη συνδεδεμένοι χρήστες τον εξής κώδικα:

```php
<?php
session_start();
if(empty($_SESSION["authenticated"]) || $_SESSION["authenticated"] != 'true') {
    header('Location: ../front_end/index.html');
    exit();
}
?>
```

Στο πιο πάνω κομμάτι κώδικα αρχικά ξεκινούμε το session και στην συνέχεια αν η μεταβλητή authenticated, που είναι καταχωρημένη σε αυτό δεν είναι true ή είναι κενή τότε κάνει redirect (response code 302) το χρήστη στη σελίδα της σύνδεσης που είναι το index.html

Περιορισμός στις 3 προσπάθειες και μπλοκάρισμα για 5 λεπτά:

Το σύστημα μετρά τις αποτυχημένες προσπάθειες που κάνει κάποιος συγκεκριμένος χρήστης για σύνδεση σε αυτό καταχωρώντας τις στο session του σερβερ. Όταν ο χρήστης κάνει 3 αποτυχημένες προσπάθειες τότε το σύστημα τον μπλοκάρει από το να συνδεθεί για τα επόμενα 5 λεπτά παρουσιάζοντας του μήνυμα ότι ξεπέρασε το μέγιστο επιτρεπτό όριο αποτυχημένων προσπαθειών. Αυτό γίνεται καταχωρώντας στο session του σερβερ την ώρα που έκανε την 4η προσπάθεια στην οποία του ανακοινώθηκε πώς δεν μπορεί να συνδεθεί για τα επόμενα 5 λεπτά. Ο έλεγχος για το χρόνο γίνεται ελέγχοντας κάθε φορά πόση ώρα πέρασε από την ώρα που του απαγορεύτηκε η πρόσβαση η οποία είναι καταχωρημένη στο session.

Backspace και Log Out:

Αφού κάποιος χρήστης συνδεθεί στο σύστημα και μετά πατήσει backspace ή Log Out το σύστημα τον ανακατευθύνει στην σελίδα σύνδεσης και τον αποσυνδέει από το σύστημα (κάνει το authenticated = false) με αποτέλεσμα ο χρήστης να χάνει αυτόματα κάθε πρόσβαση στο σύστημα όπως το API και σελίδα και για να ξανά αποκτήσει πρόσβαση στο σύστημα θα πρέπει να συνδεθεί.