ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ  
ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΙΑ 1

**Συντελεστές εργασίας**

Χριστοφορίδης Χαράλαμπος – Π19188

Γεωργιάδης Νικόλαος – π19032

Καρκάνης Ευστράτιος – Π19064

31 Οκτωβρίου 2022

**Περιεχόμενα**

[1. Εισαγωγή 2](#_Toc118131581)

[2. Καταγραφή του υπό μελέτη συστήματος 2](#_Toc118131582)

[3. Δημιουργία μοντέλου αγαθών (asset model) 2](#_Toc118131583)

[4. Αντιστοίχιση υπηρεσιών και υπολογιστικών συστημάτων 2](#_Toc118131584)

[5. Αποτίμηση συνεπειών ή επιπτώσεων ασφαλείας (impact assessment) 2](#_Toc118131585)

[6. Αποτίμηση απειλών (threat assessment) 2](#_Toc118131586)

[7. Αποτίμηση αδυναμιών (vulnerability assessment) 2](#_Toc118131587)

1. **Εισαγωγή**

Στην συγκεκριμένη εργασία του μαθήματος, το πληροφοριακό σύστημα (ΠΣ) που χρησιμοποιούμε είναι μία εφαρμογή εξυπηρέτησης ιατρών, ασθενών και διαχειριστών που είχαμε αναπτύξει σε προηγούμενο μάθημα. Περισσότερες λεπτομέρειες για το εν λόγω πληροφοριακό σύστημα αναφέρονται στο επόμενο κεφάλαιο.

1. **Καταγραφή του υπό μελέτη συστήματος**

Το πληροφοριακό σύστημα, στο οποίο βασιζόμαστε, μπορεί να υποστηρίξει χρήστες με διαφορετικά δικαιώματα πρόσβασης στο σύστημα. Οι τρεις κατηγορίες χρηστών είναι οι Ιατροί, οι Ασθενείς και οι Διαχειριστές. Ορισμένες βασικές υπηρεσίες που υποστηρίζει η εφαρμογή είναι οι ακόλουθες:

**Α) Εγγραφή ασθενών:** οι μόνοι χρήστες που μπορούν να εγγραφούν στο σύστημα μόνοι τους είναι οι ασθενείς. Οι τελευταίοι μπορούν να χρησιμοποιήσουν μία Web φόρμα εγγραφής παρέχοντας στοιχεία όπως: First Name, Last Name, Username, Password, Age και ΑΜΚΑ. Ο νέος χρήστης εισάγεται σε μία βάση δεδομένων.

**Β) Σύνδεση χρηστών:** όλοι οι χρήστες της εφαρμογής (κάθε κατηγορίας) μπορούν να χρησιμοποιήσουν μία Login φόρμα, για να συνδεθούν στο σύστημα. Προκειμένου να γίνει αυτό, θα πρέπει να πληκτρολογήσουν το Username, το Password και την κατηγορία, στην οποία ανήκουν (Ασθενείς, Ιατροί ή Διαχειριστές). Εφόσον υπάρχει όντως χρήστης με αυτά τα στοιχεία, έπειτα από αναζήτηση σε μία βάση δεδομένων, η σύνδεση του χρήστη στην εφαρμογή είναι επιτυχής.

**Γ) Κλείσιμο ραντεβού από ασθενή:** μία από τις βασικές λειτουργίες του ασθενούς είναι να ψάχνει, μέσα σε ένα συγκεκριμένο διάστημα που θα ορίζει αυτός, διαθέσιμους ιατρούς, ώστε να κλείσει ένα ραντεβού. Ο ασθενής δεν έχει τόσο μεγάλο έλεγχο σε αυτό, καθώς, για να κρατηθεί ένα ραντεβού, θα πρέπει, πρωτίστως, να είναι ο ιατρός διαθέσιμος. Μάλιστα, ο ασθενής δεν μπορεί να κλείσει όποια ημέρα επιθυμεί αυτός, αλλά αυτές που έχει ορίσει ο ιατρός ως «διαθέσιμες».

**Δ) Δήλωση διαθεσιμότητας από ιατρό:** μέσα στο σύστημα, ένας ιατρός μπορεί να δηλώσει πότε είναι διαθέσιμος να δεχτεί έναν οποιονδήποτε ασθενή σε ραντεβού.

**Ε) Εισαγωγή Ιατρών και Διαχειριστών:** ένας διαχειριστής έχει τη δυνατότητα να εισάγει μέσα στο σύστημα καινούριους ιατρούς και διαχειριστές. Σε κάθε περίπτωση, πάντα στο σύστημα πρέπει να υπάρχει τουλάχιστον ένας Διαχειριστής. Οι νέοι χρήστες εισάγονται σε μία βάση δεδομένων.

**Ζ)** **Διαγραφή χρηστών από το σύστημα:** ένας διαχειριστής μπορεί να διαγράψει έναν οποιονδήποτε χρήστη κάθε κατηγορίας, εκτός από τον εαυτό του.

**Η)** **Ακύρωση ραντεβού:** ένας ασθενής μπορεί να ακυρώσει ένα μελλοντικό ραντεβού που έχει κλείσει με ένα γιατρό. Ταυτόχρονα, ένας ιατρός μπορεί να ακυρώσει ένα μελλοντικό ραντεβού που έχει κλειστεί με έναν ασθενή.

Όσον αφορά την αρχιτεκτονική του συστήματος, πρόκειται για μία 3-tier εφαρμογή, η οποία αποτελείται από τρία layers: application layer, web-server layer και database layer. Αναλυτικότερα έχουμε τα εξής:

* Λειτουργικό Σύστημα: Windows 10 x64 (intel core i5)
* Εξυπηρετητής Ιστού και εφαρμογής: Apache Tomcat v. 8.5.66
* Εξυπηρετητής βάσης δεδομένων: MySQL v. ?
* Πρωτόκολλο ασφάλειας SSL: Δεν υπάρχει, η σύνδεση είναι μη ασφαλής
* Κλειδί εξυπηρετητή: δεν υπάρχει

1. **Δημιουργία μοντέλου αγαθών (asset model)**
2. **Αντιστοίχιση υπηρεσιών και υπολογιστικών συστημάτων**
3. **Αποτίμηση συνεπειών ή επιπτώσεων ασφαλείας (impact assessment)**
4. **Αποτίμηση απειλών (threat assessment)**
5. **Αποτίμηση αδυναμιών (vulnerability assessment)**

Το σύστημα αυτό αποτελεί μία εφαρμογή εξυπηρέτησης Ιατρών (doctors), Ασθενών (patients) και Διαχειριστών (administrators).

Πιο συγκεκριμένα, στην εφαρμογή συνδέονται και αποσυνδέονται Ιατροί, για να παρακολουθήσουν τα ραντεβού που έχουν με ασθενείς, να