ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ  
ΣΥΣΤΗΜΑΤΩΝ

Τελικη ΕΡΓΑΣΙΑ

**Συντελεστές εργασίας**

Χριστοφορίδης Χαράλαμπος – Π19188

Γεωργιάδης Νικόλαος – π19032

Καρκάνης Ευστράτιος – Π19064

20 ιανουαριου 2023

**Περιεχόμενα**

[**0.** **Εισαγωγή** 2](#_Toc125133869)

[**1.** **Μελέτη ασφάλειας ΠΣ** 2](#_Toc125133870)

[**2.** **Κρυπτογράφηση ssl στον server της εφαρμογης** 2](#_Toc125133871)

[**3.** **Μηχανισμός αυθεντικοποίησης και ελέγχου πρόσβασης** 2](#_Toc125133872)

[**4.** **Input filtering και validation** 2](#_Toc125133873)

[**5.** **Αυτοματοποιημένος έλεγχος για την εύρεση επαθειών ασφάλειας** 2](#_Toc125133874)

# **Εισαγωγή**

Η διαδικτυακή εφαρμογή που έχουμε αναπτύξει, αποτελεί ένα σύστημα διαχείρισης ραντεβού ασθενών και ιατρών. Στο σύστημα υπάρχουν και οι διαχειριστές, οι οποίοι μπορούν να προσθέτουν και να αφαιρούν κάθε κατηγορία χρήστη από την στιγμή που θα συνδεθούν στο σύστημα. Αναλυτικές πληροφορίες για τις λειτουργίες και για το περιεχόμενο της εφαρμογής μπορούν να βρεθούν στο αρχείο “**Παρουσίαση παλιάς εργασίας.pdf**” το οποίο αποτελεί την παρουσίαση της εφαρμογής που αναπτύχθηκε στο 4o εξάμηνο κατά τη διάρκεια του μαθήματος “**Προγραμματισμός στο διαδίκτυο και στον παγκόσμιο ιστό**”.

Η εφαρμογή έχει αναπτυχθεί μέσω του **IDE** **Intellij IDEA v.2021.2.2** σε **Java**, χρησιμοποιώντας **servlets, HTML και JSP σελίδες**. Ο Application-Web server που χρησιμοποιήθηκε είναι ο **Tomcat v.8.5.6.** Η ανάπτυξη της βάσης δεδομένων έγινε μέσω του εργαλείου **MySQL WorkBench v.8.0.**

Στον φάκελο “**Web App**” βρίσκεται ο αναλυτικός κώδικας σε μορφή **Intellij IDEA** project(**Ergasia 3**), το μοντέλο της βάσης δεδομένων(**app\_db.mwb**), ο φάκελος “**sql\_statements**” που περιέχει τα queries τα οποία εισάγουν τα δεδομένα στη βάση και ένα αρχείο “**passwords memo.txt**” για να μπορούμε να έχουμε πρόσβαση σε κάποια passwords χρηστών προκειμένου να γίνει δοκιμή της εφαρμογής(τα **passwords** βρίσκονται σε **hashed + salted** μορφή στη βάση δεδομένων οπότε **δεν μπορούμε να τα ανακτήσουμε**).

# **Μελέτη ασφάλειας ΠΣ**

# **Κρυπτογράφηση ssl στον server της εφαρμογης**

Text, letter

Description automatically generated

# **Μηχανισμός αυθεντικοποίησης και ελέγχου πρόσβασης**

# **Input filtering και validation**

# **Αυτοματοποιημένος έλεγχος για την εύρεση ευπαθειών ασφάλειας**