Μελέτη Ασφάλειας Πληροφοριακού Συστήματος

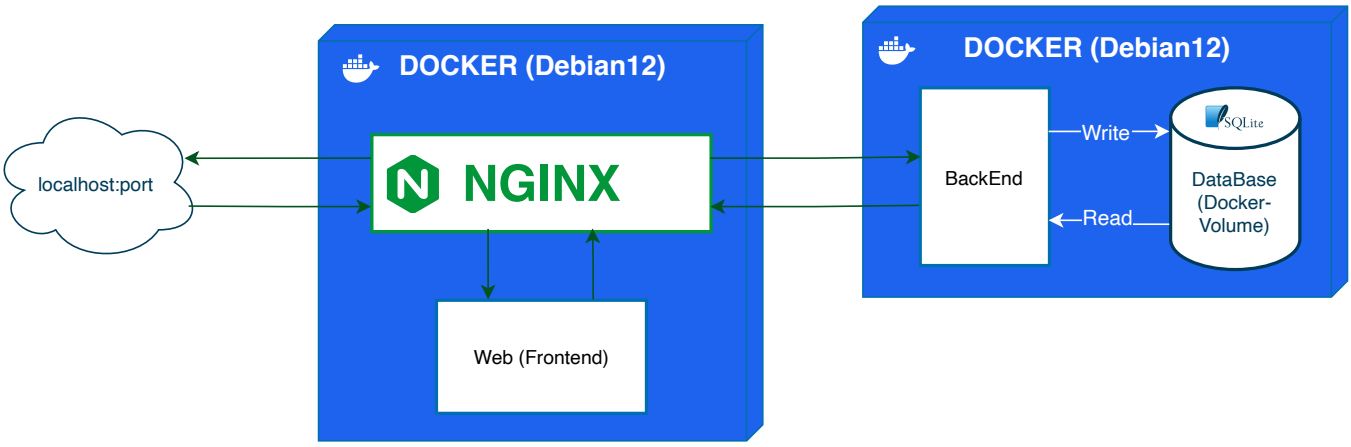
Γιούριϊ Οσιπιάν Π22125
Ιωάννα Ανδριανού Π22010

1. Καταγραφή του υπό μελέτη συστήματος.

Η εφαρμογή προσφέρει τη δυνατότητα καταχώρησης και διαχείρισης ραντεβού μεταξύ ασθενών και ιατρών, που επιτρέπει τη γρήγορη αναζήτηση ειδικών ιατρών βάσει ειδικότητας και περιοχής, την προβολή της διαθεσιμότητάς τους και την πραγματοποίηση ή ακύρωση ραντεβού από πλευράς του ασθενούς. Η εφαρμογή διαθέτει διαφορετικές λειτουργίες ανάλογα με το αν ο χρήστης είναι ιατρός ή ασθενής. Μερικές βασικές λειτουργίες είναι:

1. Εγγραφή και Σύνδεση Χρήστη
2. Κλείσιμο ραντεβού με γιατρούς
3. Οργάνωση μελλοντικών ραντεβού για ασθενείς και γιατρούς
4. Ανώνυμες κριτικές για τους γιατρούς από τους ασθενείς

Η αρχιτεκτονική του δικτύου δίδεται στο παρακάτω σχήμα:



Οι τεχνολογίες πάνω στις οποίες έχει υλοποιηθεί η παραπάνω υπηρεσία είναι οι ακόλουθες:

- Λειτουργικό Σύστημα: `Debian 12 (Docker 28.5.1)`
- Εξυπηρετητής Ιστού: `NGINX v1.28`
- Εξυπηρετητής εφαρμογής: `JDK 21` `Jetty v11.0.25 (embedded via Javalin 6.6.0)`
- Εξυπηρετητής βάσης δεδομένων: `SQLite 3.49.1.0`, `ActiveJDBC 3.5-j11 (ORM)`

2. Δημιουργία μοντέλου αγαθών (asset model).

Υπολογιστικό Σύστημα: Web Server

HW	**Server** (μοντέλο, χαρακτηριστικά) **Τοποθεσία** (κτήριο, δωμάτιο)	Docker Greece
SW	**Λειτουργικό Σύστημα** (πυρήνας, έκδοση) **Λογισμικό Εφαρμογών** **Άλλο Λογισμικό**	Debian 12 x86-64 Docker Container 28.5.1 NGINX
Network	**Περιοχή Δικτύου** (network zone) **Σημείο σύνδεσης** (Gateway)	localhost 9191
Data	**Δεδομένα διαμόρφωσης** (Configuration data) **Δεδομένα λειτουργίας υπηρεσιών** (Operation data) **Άλλα δεδομένα**	NGINX-config Docker-config versions-info connections-info certificates private-key web-structure images

Υπολογιστικό Σύστημα: Backend Server (Application)

HW	**Server** (μοντέλο, χαρακτηριστικά) **Τοποθεσία** (κτήριο, δωμάτιο)	Docker Greece
SW	**Λειτουργικό Σύστημα** (πυρήνας, έκδοση) **Λογισμικό Εφαρμογών** **Άλλο Λογισμικό**	Debian 12 x86-64 Docker Container 28.5.1 JDK-21 Jetty v11.0.25 Javalin 6.6.0 (web framework), ActiveJDBC 3.5-j11 (ORM)
Network	**Περιοχή Δικτύου** (network zone) **Σημείο σύνδεσης** (Gateway)	localhost 7070
Data	**Δεδομένα διαμόρφωσης** (Configuration data) **Δεδομένα λειτουργίας υπηρεσιών** (Operation data) **Άλλα δεδομένα**	git Docker-config maven-config application-code(bru sql java json) backend-structure documentations, diagrams

Υπολογιστικό Σύστημα: Backend Server (Database)

HW	**Server** (μοντέλο, χαρακτηριστικά) **Τοποθεσία** (κτήριο, δωμάτιο)	Docker Greece

SW	**Λειτουργικό Σύστημα** (πυρήνας, έκδοση) **Λογισμικό Εφαρμογών** **Άλλο Λογισμικό**	Debian 12 x86-64 Docker Container 28.5.1 SQLite 3.49.1.0
Network	**Περιοχή Δικτύου** (network zone) **Σημείο σύνδεσης** (Gateway)	localhost 7070
Data	**Δεδομένα διαμόρφωσης** (Configuration data) **Δεδομένα λειτουργίας υπηρεσιών** (Operation data) **Άλλα δεδομένα**	SQLite calls database -

3. Αντιστοίχιση υπηρεσιών και υπολογιστικών συστημάτων.

Και οι τέσσερις υπηρεσίες που παρέχονται από το συγκεκριμένο σύστημα χρησιμοποιούν τον web server, τον application server και τη βάση δεδομένων.

	Web Server	**Application server**	**Database**
Εγγραφή και Σύνδεση Χρήστη	O	O	O
Κλείσιμο ραντεβού με γιατρούς	O	O	O
Οργάνωση μελλοντικών ραντεβού για ασθενείς και γιατρούς	O	O	O
Ανώνυμες κριτικές για τους γιατρούς από τους ασθενείς	O	O	O

- Αρχικά, για την εγγραφή και τη σύνδεση χρήστη πρέπει να χρησιμοποιηθούν τα login credentials του χρήστη που είναι αποθηκευμένα στη βάση δεδομένων ή να αποθηκευτούν νέα. Για αυτό, από τη σελίδα login ή sign up στο web, τα στοιχεία στέλνονται στο backend που ελέγχει τη βάση δεδομένων (στη σύνδεση) ή αποθηκεύει τα στοιχεία του νέου χρήστη (στην εγγραφή).
- Για το κλείσιμο ραντεβού χρειάζεται να γίνει retrieve από το backend τα στοιχεία των γιατρών από τη βάση καθώς και οι διαθέσιμες ώρες τους.
- Για την οργάνωση των μελλοντικών ραντεβού σε calendar ζητάμε από τη βάση τα ραντεβού του συγκεκριμένου χρήστη.
- Για να αφήσει κριτική ο χρήστης θα πρέπει να την αποθηκεύσουμε στη βάση και για να τη δει ο γιατρός θα την κάνουμε retrieve από τη βάση.

4. Αποτίμηση συνεπειών ή επιπτώσεων ασφάλειας (impact assessment).

Υπηρεσία: Εγγραφή και Σύνδεση Χρήστη

Συνέπειες για:	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση**
Μη διαθεσιμότητα (unavailability)	Παρεμπόδιση λειτουργιών Άμεσες οικονομικές απώλειες Δυσφήμιση	Υψηλή	Η αδυναμία σύνδεσης των χρηστών μπορεί να οδηγήσει σε απώλεια εσόδων λόγω αδυναμίας κλεισίματος ραντεβού καθώς και σε δυσφήμιση της εταιρίας.
Αποκάλυψη δεδομένων (disclosure)	Δυσφήμιση Νομικές κυρώσεις	Υψηλή	Η αποκάλυψη login credentials ή ιατρικών δεδομένων μπορεί να οδηγήσει σε σοβαρές νομικές συνέπειες.
Τροποποίηση δεδομένων (modification)	Παρεμπόδιση λειτουργιών Δυσφήμιση	Μέτρια	Η τροποποίηση των στοιχείων σύνδεσης των χρηστών μπορεί να προκαλέσει προβλήματα στη χρήση της εφαρμογής και απώλεια εμπιστοσύνης.

Υπηρεσία: Κλείσιμο ραντεβού με γιατρούς

Συνέπειες για:	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση**
Μη διαθεσιμότητα (unavailability)	Άμεσες οικονομικές απώλειες Παρεμπόδιση λειτουργιών Δυσφήμιση	Υψηλή	Ως βασική λειτουργία της εφαρμογής, η μη διαθεσιμότητά της θα οδηγήσει σε απώλεια εσόδων λόγω της αδυναμίας κλεισίματος ραντεβού.
Αποκάλυψη δεδομένων (disclosure)	Δυσφήμιση Νομικές κυρώσεις	Μέτρια	Λόγω ιατρικού απορρήτου, η αποκάλυψη στοιχείων των ραντεβού μπορεί να οδηγήσει σε νομικά προβλήματα.
Τροποποίηση δεδομένων (modification)	Δυσφήμιση Παρεμπόδιση λειτουργιών	Μέτρια	Η τροποποίηση των στοιχείων ενός ραντεβού μπορεί να προκαλέσει ασυνεννοησία μεταξύ γιατρού και ασθενούς.

Υπηρεσία: Οργάνωση μελλοντικών ραντεβού

Συνέπειες για:	Τύπος Συνέπειας	Βαθμός Συνέπειας	Σύντομη αιτιολόγηση
Μη διαθεσιμότητα (unavailability)	Δυσφήμιση Παρεμπόδιση λειτουργιών	Μέτρια	Οι χρήστες δεν θα μπορούν να οργανώσουν τα μελλοντικά τους ραντεβού, κάτι που μπορεί να οδηγήσει σε ασυνεννοησία μεταξύ γιατρών και ασθενών.
Αποκάλυψη δεδομένων (disclosure)	Δυσφήμιση Νομικές κυρώσεις	Υψηλή	Η αποκάλυψη μελλοντικών ραντεβού μπορεί να οδηγήσει σε νομικές κυρώσεις λόγω ιατρικού απορρήτου.
Τροποποίηση δεδομένων (modification)	Δυσφήμιση Παρεμπόδιση λειτουργιών	Μέτρια	Η τροποποίηση των στοιχείων ενός ραντεβού μπορεί να προκαλέσει ασυνεννοησία μεταξύ γιατρών και ασθενών.

Υπηρεσία: Ανώνυμες κριτικές για τους γιατρούς

Συνέπειες για:	Τύπος Συνέπειας	Βαθμός Συνέπειας	Σύντομη αιτιολόγηση
Μη διαθεσιμότητα (unavailability)	Δυσφήμιση	Χαμηλή	Μπορεί να οδηγήσει σε λιγότερα ραντεβού για τους γιατρούς και σε δυσφήμηση για την εταιρία.
Αποκάλυψη δεδομένων (disclosure)	Δυσφήμιση	Χαμηλή	Η αποκάλυψη της ταυτότητας των σχολιαστών που υποτίθεται ότι είναι ανώνυμοι μπορεί να προκαλέσει δυσφήμιση.
Τροποποίηση δεδομένων (modification)	Δυσφήμιση Νομικές κυρώσεις	Μέτρια	Η τροποποίηση κριτικών μπορεί να οδηγήσει σε εσφαλμένη δυσφήμιση κάποιου γιατρού και πιθανές νομικές συνέπειες.

5. Αποτίμηση απειλών (threat assessment).

Απειλή:	Web Server:	Application Server	Database
Unauthorized Access	Medium	Medium	Low
Ransomware	Low	Medium	Medium
Web Defacement	High	Low	Low
Code Injection	High	Medium	Low
Denial of Service	High	Medium	Low

Σχόλια: Ο πίνακας έχει γίνει με βάση την πιθανότητα που υπάρχει κάποια απειλή να εκδηλωθεί σε κάποιον από τους server. Γενικά το database βρίσκεται πίσω από το backend οπότε είναι πιο δύσκολο να γίνει επίθεση προς αυτόν ενώ ο web server και το backend είναι πολύ πιο ευάλωτοι. Επιπλέον το web defacement και το code injection γίνονται συνήθως μέσω του frontend για αυτό και έχουν μεγαλύτερη πιθανότητα να εκδηλωθεί εκεί. Τέλος τα περισσότερα DoS attacks γίνονται με επίθεση στο frontend.

6. Αποτίμηση αδυναμιών (vulnerability assessment).

Με την βάση αδυναμιών ασφάλειας του NIST και υπολογίζοντας το CVSS 3 score κάθε vulnerability έχουμε τον παρακάτω πίνακα:

Λογισμικό	Αδυναμία	CVSS 3.1 Score
Debian 12 sudo 1.9.13p3	**CVE-2025-32463** Χρησιμοποιώντας sudo --chroot ο χρήστης μπορεί να πειράξει το αρχείο nsswitch.conf και να αποκτήσει πρόσβαση root	7.8 (High)
Docker Compose 2.40.0	**CVE-2025-62725** Το Docker Compose εμπιστεύεται τις πληροφορίες διαδρομής που είναι ενσωματωμένες σε απομακρυσμένα αντικείμενα σύνθεσης OCI	8.9 (High)
JDK 21	**CVE-2024-20952** Αποφυγή ελέγχου πιστοποιητικού και μη εξουσιοδοτημένη πρόσβαση (JSSE)	7.4 (High)
Eclipse Jetty 11.0.5	**CVE-2025-5115** CVE-2025-5115 Στέλνοντας πολλαπλά RST_STREAM frames στον server ο χρήστης μπορεί να φορτώσει χωρίς λόγο τους πόρους του server	7.7 (High)
Eclipse Jetty 11.0.5	**CVE-2021-34429** Με ειδικό τρόπο αποστολής URIs υπάρχει δυνατότητα σύνδεσης στο WEB-INF φάκελο	5.3 (Medium)

Σημείωση: Για NGINX 1.28, SQLite 3.49.1 και ActiveJDBC 3.5-j11 δεν βρέθηκαν αδυναμίες.

7. Αποτίμηση κινδύνων (risk assessment).

α) Αποτίμηση Απειλών

Παρατηρούμε ότι παρόλλο που ο αριθμός των απειλών που βρήκαμε στο vulnerability assessment ειναι χαμηλός, στο σύστημα μας υπάρχουν κάποια σοβαρά vulnerabilities (severity: High), τα οποία αυξάνουν την αποτίμηση των απειλών. Για το cvss για κάθε απειλή χρησιμοποιήσαμε τον μέσο όρο των απειλών καθώς στην πιθανότητα απειλής βάλαμε το υψηλότερο που υπήρχε σε κάθε απειλή στο threat assessment. Ο πίνακας για την αποτίμηση επιπέδου απειλής είναι ο παρακάτω:

Επίπεδο Αδυναμίας (βάσει CVSS score):	**None**	**Low**	**Medium**	**High**	**Critical**
Πιθανότητα Απειλής:					
0 (Low Prob)	0	0	0	1	1
1 (Med. Prob)	0	1	2	2	3
2 (High Prob)	0	1	2	3	4

Οπότε με βάση τον πίνακα έχουμε τις παρακάτω αποτιμήσεις:

Απειλή	**Αδυναμίες**	**Μέσος όρος CVSS Score**	**Πιθανότητα Απειλής**	**Αποτίμηση Επιπέδου Απειλής**
Unauthorized Access	CVE-2025-32463 CVE-2024-20952 CVE-2021-34429	7.5 (High)	Medium	2
Ransomware	CVE-2025-62725	8.9 (High)	Medium	2
Web Defacement	CVE-2021-34429	5.3 (Medium)	High	2
Code Injection	CVE-2025-62725	8.9 (High)	High	3
Denial of Service	CVE-2025-5115	7.7 (High)	High	3

Παρατηρούμε ότι οι περισσότερες αδυναμίες του συστήματός μας είναι στην απειλή Unauthorized Access. Υπό άλλες συνθήκες, ενώ η συγκεκριμένη απειλή είναι πιο δύσκολη να εκδηλωθεί, παρατηρούμε ότι

αυξάνεται η πιθανότητα λόγω του πλήθους των αδυναμιών. Στην συγκεκριμένη περίπτωση όμως, μιας και η πιθανότητα απειλής είχε υπολογιστεί ανεξάρτητα των vulnerabilities, παραμένει Medium.

β) Αποτίμηση Κινδύνου

Στην αποτίμηση κινδύνου είναι σημαντικό να αναφερθεί ότι το συγκεκριμένο σύστημα χρησιμοποιεί σημαντικά προσωπικά δεδομένα και για αυτό είναι πολύ σημαντική η ασφαλής και σωστή λειτουργία του συστήματος. Για αυτό το λόγο, το επίπεδο συνέπειας παραμένει γενικά υψηλό. Όπως αναφέρθηκε και νωρίτερα στο impact assessment, λόγω ιατρικού απορρήτου που μπορεί να οδηγήσει σε νομικές κυρώσεις η συνέπειες μπορούν να είναι αρκετά μεγάλες.

Οπότε χρησιμοποιώντας τον παρακάτω πίνακα:

Αποτίμηση Απειλής:	**0**	**1**	**2**	**3**	**4**
Αποτίμηση Συνέπειας:					
1 (Χαμηλή)	0	1	2	3	4
2 (Μέτρια)	0	2	4	6	8
3 (Υψηλή)	0	3	6	9	12

Έχουμε τον παρακάτω πίνακα αποτίμησης κινδύνου:

Απειλή	**Επίπεδο συνέπειας**	**Αποτίμηση Απειλής**	**Αποτίμηση επιπέδου κινδύνου**
Unauthorized Access	High (Πληροφορίες χρηστών, ιατρικό απόρρητο)	2	6
Ransomware	High (Καταστροφή δεδομένων, μη λειτουργικότητα συστήματος)	2	6
Web Defacement	Medium (Δυσφήμιση εταιρίας)	2	3
Code Injection	High (Καταστροφή δεδομένων, unauthorized access)	3	6
Denial of Service	High (Μη λειτουργικότητα του συστήματος)	3	6

Κατώφλι Κινδύνου (Risk threshold)

Με κατώφλι κινδύνου να είναι 2 παρατηρούμε ότι όλες οι απειλές είναι πάνω από το κατώφλι κινδύνου. Γενικά παρατηρούμε ότι το σύστημα έχει αποτίμηση κινδύνου επίπεδο ~6 . Αυτό θεωρείται υψηλό αλλά είναι λογικό λόγω των ευαίσθητων στοιχείων και λόγω των vulnerabilities που βρήκαμε. Αυτό σημαίνει ότι

για να μειωθεί ο κίνδυνος θα πρέπει μελλοντικά να μειώσουμε, όσο το δυνατόν, τα vulnerabilities που υπάρχουν ώστε η αποτίμηση της απειλής να είναι όσο χαμηλά γίνεται.

Τελικά Σχόλια

Μέσω του security assessment παρατηρούμε ότι λόγω της φύσης του συστήματος υπάρχει μεγάλη προτεραιότητα στην ασφάλεια λόγω των δεδομένων. Πιο συγκεκριμένα πρέπει να υπάρχει προτεραιότητα στην εμπιστευτικότητα και ακεραιότητα των δεδομένων ώστε η εταιρία να προστατευθεί από νομικές κυρώσεις. Στην συνέχεια θα πρέπει να προστατευτεί και η διαθεσιμότητα της υπηρεσίας καθώς από εκεί έρχονται τα κύρια έσοδα της εταιρίας. Για αυτό το λόγο θα πρέπει να γίνει διασφάλιση όλων των υπολογιστικών συστημάτων και να εφαρμοστεί κάθε μέτρο που ορίζει ο νόμος.