12 ΝΟΕΜΒΡΙΟΥ 2022

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΙΑ 1

Συντελεστές εργασίας

Χριστοφορίδης Χαράλαμπος – Π19188

Γεωργιάδης Νικόλαος – Π19032

Καρκάνης Ευστράτιος – Π19064

Περιεχόμενα

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.

2. 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 «στρώματα»: 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.8.0.31
- **Πρωτόκολλο ασφάλειας SSL:** Δεν υπάρχει, η σύνδεση είναι μη ασφαλής!
- **Πλαίσιο υλοποίησης (framework):** Intellij IDEA v. 2022.1.4 με γλώσσα προγραμματισμού Java.
- **Κλειδί εξυπηρετητή:** δεν υπάρχει

3. Δημιουργία μοντέλου αγαθών (asset model)

Στο πληροφορικό σύστημα, το οποίο αναλύουμε, μπορούμε να υποθέσουμε ότι τα υπολογιστικά συστήματα που χρησιμοποιούνται είναι τρία (3), ο web server, ο application server και ο database server .

Αναλυτικότερα, το μοντέλο αγαθών για κάθε ένα από τα παραπάνω υπολογιστικά συστήματα που αναφέρθηκαν περιγράφονται στους ακόλουθους πίνακες:

1. Μοντέλο αγαθών για τον Application Server

Όνομα Υπολογιστικού Συστήματος: Application Server		
HW	Server (μοντέλο, χαρακτηριστικά)	Apache Tomcat 8.5.66 (Server version: 8.5.66.0)
	Τοποθεσία (κτήριο, δωμάτιο)	Το hardware του server είναι ο ίδιος ο υπολογιστής που «τρέχει» η εφαρμογή
SW	Λειτουργικό Σύστημα (πυρήνας, έκδοση)	Το λειτουργικό σύστημα είναι: Windows 10 x64 (έκδοση 10)
	Λογισμικό Εφαρμογών	Intellij IDE (java 1.8.0 _351)
	Άλλο Λογισμικό	Όχι
Network	Περιοχή Δικτύου (network zone)	Ο Apache Tomcat τρέχει στην IP 127.0.0.1:8080 (localhost)
	Σημείο σύνδεσης (Gateway)	Είναι η διεύθυνση localhost
Data	Δεδομένα διαμόρφωσης (Configuration data)	Τα configuration data του server είναι τα αρχεία **server.xml** και **web.xml**
	Δεδομένα λειτουργίας υπηρεσιών (Operation data)	Τα operational data είναι τα δεδομένα που δημιουργεί και επιστρέφει ο web server(αρχεία HTML, JSP).
	Άλλα δεδομένα	όχι

2. Μοντέλο αγαθών για τον Web Server

Όνομα Υπολογιστικού Συστήματος: Web Server		
HW	Server (μοντέλο, χαρακτηριστικά)	Catalina (Server version: 8.5.66.0)
	Τοποθεσία (κτήριο, δωμάτιο)	Το hardware του server είναι ο ίδιος ο υπολογιστής που «τρέχει» η εφαρμογή
SW	Λειτουργικό Σύστημα (πυρήνας, έκδοση)	Το λειτουργικό σύστημα είναι: Windows 10 x64 (έκδοση 10)
	Λογισμικό Εφαρμογών	Ο Catalina Server λειτουργεί πάνω στον Apache Tomcat (8.5.66)
	Άλλο Λογισμικό	όχι
Network	Περιοχή Δικτύου (network zone)	Ο Catalina web server τρέχει στην IP 127.0.0.1:8080 (localhost)
	Σημείο σύνδεσης (Gateway)	Είναι η διεύθυνση localhost, εφόσον όλα τρέχουν τοπικά στο μηχάνημα
Data	Δεδομένα διαμόρφωσης (Configuration data)	Τα configuration data του server είναι τα αρχεία **server.xml** και **web.xml**
	Δεδομένα λειτουργίας υπηρεσιών (Operation data)	Τα operational data είναι τα δεδομένα που δημιουργεί και επιστρέφει ο web server(αρχεία HTML, JSP).
	Άλλα δεδομένα	όχι

Παραδοχή: Θεωρητικά, ο Apache Tomcat λειτουργεί τόσο ως application, όσο και ως web server. Στην προκειμένη περίπτωση, θεωρούμε ότι οι δύο αυτοί ρόλοι του Apache Tomcat αποτελούν δύο διαφορετικά υπολογιστικά συστήματα.

3. Μοντέλο αγαθών για τον Database Server

Όνομα Υπολογιστικού Συστήματος: Database Server		
HW	Server (μοντέλο, χαρακτηριστικά)	MySQL server (MySQL 8.0.31)
	Τοποθεσία (κτήριο, δωμάτιο)	Το hardware του server είναι ο ίδιος ο υπολογιστής που «τρέχει» η εφαρμογή
SW	Λειτουργικό Σύστημα (πυρήνας, έκδοση)	Το λειτουργικό σύστημα είναι: Windows 10 x64 (έκδοση 10)
	Λογισμικό Εφαρμογών	MySQL workbench 8.0
	Άλλο Λογισμικό	Όχι
Network	Περιοχή Δικτύου (network zone)	Ο database server τρέχει στην διεύθυνση 127.0.0.1:3306
	Σημείο σύνδεσης (Gateway)	Το σημείο σύνδεσης είναι η διεύθυνση Localhost
Data	Δεδομένα διαμόρφωσης (Configuration data)	Είναι το αρχείο /etc/my.cnf, το οποίο ορίζει τη συμπεριφορά και την απόδοση του MySQL server.
	Δεδομένα λειτουργίας υπηρεσιών (Operation data)	Τα operational data είναι τα δεδομένα που «κρατώνται» στην βάση, πάνω στα οποία γίνονται τα διάφορα queries.
	Άλλα δεδομένα	Όχι

4. Αντιστοίχιση υπηρεσιών και υπολογιστικών συστημάτων

Α) Εγγραφή ασθενών: Τα κύρια υπολογιστικά συστήματα που χρησιμοποιούνται για αυτή την υπηρεσία είναι ο **database server** και ο **application server**. Ο ρόλος του πρώτου Υ.Σ. είναι να εισάγει μια νέα εγγραφή χρήστη στη βάση δεδομένων, ενώ του δεύτερου να επεξεργαστεί την δοσμένη πληροφορία και να κάνει τους απαραίτητους ελέγχους (πχ έλεγχος μοναδικότητας ΑΜΚΑ).

Β) Σύνδεση χρηστών: Όλα τα υπολογιστικά συστήματα χρησιμοποιούνται για αυτή την υπηρεσία. Ο **application server** είναι υπεύθυνος για την επαλήθευση των δεδομένων που δίνει ο χρήστης (**username**, **password**) μέσω του **database server**. Μέσω του **web** και του **application server** επιστρέφεται η κατάλληλη σελίδα **HTML** ή **JSP** που αντιστοιχεί στην αποτυχία σύνδεσης ή στα δυναμικά δεδομένα του συνδεδεμένου χρήστη.

Γ) Κλείσιμο ραντεβού από ασθενή Όλα τα υπολογιστικά συστήματα χρησιμοποιούνται για αυτή την υπηρεσία**.** Ο **application server** επεξεργάζεται τα δεδομένα που έδωσε ο ασθενής(χρονικό διάστημα αναζήτησης, κατηγορία αναζήτησης). Μέσω του **database server** γίνεται η αναζήτηση των διαθέσιμων ραντεβού και επιστρέφεται η δυναμική σελίδα **JSP** με τα αποτελέσματα μέσω του **web server** ή/και του **application server**.

Δ) Δήλωση διαθεσιμότητας από ιατρό: Τα κύρια υπολογιστικά συστήματα που χρησιμοποιούνται για αυτή την υπηρεσία είναι ο **database server** και ο **application server,** οι οποίοι είναι υπεύθυνοι για την προσθήκη της ημερομηνίας διαθεσιμότητας στην βάση δεδομένων.

Ε) Εισαγωγή Ιατρών και Διαχειριστών: Τα κύρια υπολογιστικά συστήματα που χρησιμοποιούνται για αυτή την υπηρεσία είναι ο **database server** και ο **application server,** οι οποίοι είναι υπεύθυνοι για την προσθήκη των χρηστών στην βάση δεδομένων. Ο **application server** εκτελεί τον έλεγχο διπλότυπων των στοιχείων του νέου χρήστη προς εισαγωγή με βάση τα δεδομένα του **database server**.

Ζ) Διαγραφή χρηστών από το σύστημα: Τα κύρια υπολογιστικά συστήματα που χρησιμοποιούνται για αυτή την υπηρεσία είναι ο **database server** και ο **application server,** οι οποίοι είναι υπεύθυνοι για την διαγραφή των χρηστών από την βάση δεδομένων. Ο **application server** εκτελεί τον έλεγχο ύπαρξης των στοιχείων του χρήστη προς διαγραφή με βάση τα δεδομένα του **database server**.

Η) Ακύρωση ραντεβού: Τα κύρια υπολογιστικά συστήματα που χρησιμοποιούνται για αυτή την υπηρεσία είναι ο **database server** και ο **application server.** Αφού ο ασθενής πατήσει το κουμπί της ακύρωσης του ραντεβού ο **application server** αντλεί τα δεδομένα εκείνου του ραντεβού και το αφαιρεί από τα δεδομένα του **database server**.

5. Αποτίμηση συνεπειών ή επιπτώσεων ασφαλείας (impact assessment)

Όνομα Υπηρεσίας:	**…**		
Εγγραφή ασθενών	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση** *(ποιο υπολογιστικό σύστημα που χρησιμοποιείται για την παροχή της υπηρεσίας και συγκεκριμένο αγαθό αυτού οφείλεται για τη μεγαλύτερη δυνατή συνέπεια)*
Συνέπειες για:			
(1) Μη διαθεσιμότητα (unavailability)	Άμεσες οικονομικές απώλειες, Παρεμπόδιση λειτουργιών, Δυσφήμιση	Μέτριος	Υλικό(hardware) του Application Server
(2) Αποκάλυψη δεδομένων* **(disclosure)** *Δεδομένων λογαριασμών ασθενών	Άμεσες οικονομικές απώλειες, Νομικές Κυρώσεις, Δυσφήμιση	Υψηλός	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Database Server
(3) Τροποποίηση δεδομένων* **(modification)** *Δεδομένων λογαριασμών ασθενών	Άμεσες οικονομικές απώλειες, Δυσφήμιση, Παρεμπόδιση λειτουργιών	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Database Server

Όνομα Υπηρεσίας:	**…**		
Σύνδεση χρηστών	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση** *(ποιο υπολογιστικό σύστημα που χρησιμοποιείται για την παροχή της υπηρεσίας και συγκεκριμένο αγαθό αυτού οφείλεται για τη μεγαλύτερη δυνατή συνέπεια)*
Συνέπειες για:			
(1) Μη διαθεσιμότητα (unavailability)	Άμεσες οικονομικές απώλειες, Παρεμπόδιση λειτουργιών, Δυσφήμιση	Υψηλός	Υλικό(hardware) του Application Server
(2) Αποκάλυψη δεδομένων* **(disclosure)** *Δεδομένων λογαριασμών χρηστών	Άμεσες οικονομικές απώλειες, Νομικές Κυρώσεις, Δυσφήμιση	Υψηλός	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Database Server
(3) Τροποποίηση δεδομένων* **(modification)** *Δεδομένων λογαριασμών χρηστών	Άμεσες οικονομικές απώλειες, Δυσφήμιση, Παρεμπόδιση λειτουργιών	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Database Server

Όνομα Υπηρεσίας:	**…**		
Κλείσιμο ραντεβού από ασθενή	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση** *(ποιο υπολογιστικό σύστημα που χρησιμοποιείται για την παροχή της υπηρεσίας και συγκεκριμένο αγαθό αυτού οφείλεται για τη μεγαλύτερη δυνατή συνέπεια)*
Συνέπειες για:			
(1) Μη διαθεσιμότητα (unavailability)	Άμεσες οικονομικές απώλειες, Δυσφήμιση	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Application Server
(2) Αποκάλυψη δεδομένων* **(disclosure)** *Δεδομένων ραντεβού ασθενών	Νομικές Κυρώσεις, Δυσφήμιση, Άμεσες οικονομικές απώλειες	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server
(3) Τροποποίηση δεδομένων* **(modification)** *Δεδομένων ραντεβού ασθενών	Δυσφήμιση, Παρεμπόδιση λειτουργιών	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server

Όνομα Υπηρεσίας:	**…**		
Δήλωση διαθεσιμότητας από ιατρό	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση** *(ποιο υπολογιστικό σύστημα που χρησιμοποιείται για την παροχή της υπηρεσίας και συγκεκριμένο αγαθό αυτού οφείλεται για τη μεγαλύτερη δυνατή συνέπεια)*
Συνέπειες για:			
(1) Μη διαθεσιμότητα (unavailability)	Άμεσες οικονομικές απώλειες, Δυσφήμιση, Παρεμπόδιση λειτουργιών	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Application Server
(2) Αποκάλυψη δεδομένων (disclosure)	Τα δεδομένα διαθεσιμότητας του ιατρού είναι δημόσια, άρα δεν υπάρχουν συνέπειες.	-	-
(3) Τροποποίηση δεδομένων (modification)	Δυσφήμιση, Παρεμπόδιση λειτουργιών	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server

Όνομα Υπηρεσίας:	**…**		
Εισαγωγή Ιατρών και Διαχειριστών	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση** *(ποιο υπολογιστικό σύστημα που χρησιμοποιείται για την παροχή της υπηρεσίας και συγκεκριμένο αγαθό αυτού οφείλεται για τη μεγαλύτερη δυνατή συνέπεια)*
Συνέπειες για:			
(1) Μη διαθεσιμότητα (unavailability)	Δυσφήμιση	Χαμηλός	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Application Server
(2) Αποκάλυψη δεδομένων* **(disclosure)** *Δεδομένων λογαριασμών Ιατρών και Διαχειριστών	Άμεσες οικονομικές απώλειες, Δυσφήμιση, Νομικές Κυρώσεις	Υψηλός	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server
(3) Τροποποίηση δεδομένων* **(modification)** *Δεδομένων λογαριασμών Ιατρών και Διαχειριστών(Μόνο εισαγωγή)	Δυσφήμιση	Χαμηλός	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server

Όνομα Υπηρεσίας:	**…**		
Διαγραφή χρηστών από το σύστημα	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση** *(ποιο υπολογιστικό σύστημα που χρησιμοποιείται για την παροχή της υπηρεσίας και συγκεκριμένο αγαθό αυτού οφείλεται για τη μεγαλύτερη δυνατή συνέπεια)*
Συνέπειες για:			
(1) Μη διαθεσιμότητα (unavailability)	Δυσφήμιση, Παρεμπόδιση λειτουργιών	Χαμηλός	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Application Server
(2) Αποκάλυψη δεδομένων* **(disclosure)** *Δεδομένων λογαριασμών Ιατρών, Διαχειριστών και ασθενών	Άμεσες οικονομικές απώλειες, Δυσφήμιση, Νομικές Κυρώσεις	Υψηλός	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server
(3) Τροποποίηση δεδομένων* **(modification)** *Δεδομένων λογαριασμών Ιατρών, Διαχειριστών και ασθενών (Μόνο διαγραφή)	Δυσφήμιση, Άμεσες οικονομικές απώλειες, Παρεμπόδιση λειτουργιών	Υψηλός	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server

Όνομα Υπηρεσίας:	**…**		
Ακύρωση ραντεβού	**Τύπος Συνέπειας**	**Βαθμός Συνέπειας**	**Σύντομη αιτιολόγηση** *(ποιο υπολογιστικό σύστημα που χρησιμοποιείται για την παροχή της υπηρεσίας και συγκεκριμένο αγαθό αυτού οφείλεται για τη μεγαλύτερη δυνατή συνέπεια)*
Συνέπειες για:			
(1) Μη διαθεσιμότητα (unavailability)	Δυσφήμιση, Παρεμπόδιση λειτουργιών	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) του Application Server
(2) Αποκάλυψη δεδομένων* **(disclosure)** *Δεδομένων ραντεβού ασθενών	Άμεσες οικονομικές απώλειες, Δυσφήμιση, Νομικές Κυρώσεις	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server
(3) Τροποποίηση δεδομένων* **(modification)** * Δεδομένων ραντεβού ασθενών (μόνο ακύρωση)	Δυσφήμιση, Άμεσες οικονομικές απώλειες	Μέτριος	Δεδομένα λειτουργίας υπηρεσιών(Operational data) Database Server

6. Αποτίμηση απειλών(Threat Assessment)

Σε αυτό το ερώτημα καλούμαστε να αξιολογήσουμε κάθε μία από τις παρακάτω απειλές για κάθε ένα από τα 3 υπολογιστικά συστήματα που καταγράψαμε στο βήμα 2(Application Server, Web Server, Database Server). Η αξιολόγηση αυτή θα γίνει με τη χρήση του παρακάτω πίνακα στον οποίο αξιολογούμε τις απειλές για κάθε υπολογιστικό σύστημα και κάνουμε και ένα μικρό σχόλιο για το λόγο που θεωρούμε ότι ανήκει σε αυτή τη κατηγορία πιθανότητας επικινδυνότητας. Οι βαθμίδες πιθανότητας επικινδυνότητας σύμφωνα με την εκφώνηση είναι οι εξής:

- **0** → Δεν εφαρμόζεται **(Not Applicable)**: Η απειλή δεν εφαρμόζεται/ δεν επηρεάζει το εν λόγω σύστημα.
- **1** → Χαμηλή πιθανότητα **(Low Likelihood)**: Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι το πολύ 10%.
- **2** → Μέτρια πιθανότητα **(Medium Likelihood**): Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 30%.
- **3** → Υψηλή πιθανότητα **(High likelihood)**: Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι μέχρι 60%.
- **4** → Πολύ υψηλή πιθανότητα **(Very High Likelihood)**: Η εκτιμώμενη πιθανότητα να εκδηλωθεί η απειλή στο υπό μελέτη σύστημα είναι πάνω από 60%.

Αναλυτικά για το κάθε υπολογιστικό σύστημα έχουμε:

Πιθανές Απειλές	Application Server	Web Server	Database Server
(1) Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access)	**2** Αν και υπάρχουν τα απαραίτητα πρότυπα ασφαλείας δεν είναι και αδύνατο κάποιος κακόβουλος να αποκτήσει πρόσβαση χωρίς να έχει το δικαίωμα.	**2** Αν και υπάρχουν τα απαραίτητα πρότυπα ασφαλείας δεν είναι και αδύνατο κάποιος κακόβουλος να αποκτήσει πρόσβαση χωρίς να έχει το δικαίωμα.	**2** Αν και υπάρχουν τα απαραίτητα πρότυπα ασφαλείας δεν είναι και αδύνατο κάποιος κακόβουλος να αποκτήσει πρόσβαση χωρίς να έχει το δικαίωμα.
(2) Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει/ ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware)	**0** Δεν υπάρχει τέτοια πιθανότητα, καθώς τα δεδομένα στην δικιά μας εφαρμογή δεν είναι ευαίσθητης φύσης και κατά συνέπεια δεν έχουν κάποια ιδιαίτερη χρηματική αξία.	**0** Δεν υπάρχει τέτοια πιθανότητα, καθώς τα δεδομένα στην δικιά μας εφαρμογή δεν είναι ευαίσθητης φύσης και κατά συνέπεια δεν έχουν κάποια ιδιαίτερη χρηματική αξία.	**0** Δεν υπάρχει τέτοια πιθανότητα, καθώς τα δεδομένα στην δικιά μας εφαρμογή δεν είναι ευαίσθητης φύσης και κατά συνέπεια δεν έχουν κάποια ιδιαίτερη χρηματική αξία.
(3) Παραποίηση ιστοσελίδας (Web Defacement)	**3** Υψηλή πιθανότητα τέτοιου συμβάντος, καθώς μία τέτοια επίθεση θα έβλαπτε αρκετά το κύρος της επιχείρησης που εξυπηρετεί η εφαρμογή.	**1** Αν και είναι δυνατό να παραποιηθεί η ιστοσελίδα όσο βρίσκεται στον Web Server πριν πάει στον End-User, συνήθως τέτοιου είδους επίθεση γίνεται στον Application Server.	**0** Μιλάμε για έναν Database Server, ο οποίος δεν διαθέτει ιστοσελίδα για να παραποιηθεί.
(4) Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection)	**2** Συχνό φαινόμενο σε αυτού του είδους τα υπολογιστικά συστήματα. Αν και στην περίπτωση μας δεν θα είναι και ιδιαίτερα πιθανό λόγο της του Application server μας.	**3** Πολύ συχνό φαινόμενο σε αυτού του είδους τα υπολογιστικά συστήματα. Στην περίπτωση του Web Server μας θα άξιζε να προσπαθήσει κάποιο κάτι τέτοιο.	**4** Εξαιρετικά πιθανό σενάριο να συμβεί καθώς με αυτό το τρόπο θα μπορούσε κάποιος επιτιθέμενος να παραποιήσει τα δεδομένα όλων των χρηστών της εφαρμογής.

(5) Άρνηση υπηρεσίες (Denial of Service)	**4** Κάτι τέτοιο είναι πολύ πιθανό να συμβεί, καθώς κάποιο με κάποια σειρά ενεργειών μπορούν να κάνουν τον Server να σταματήσει να ανταποκρίνεται. Παράδειγμα = https://tomcat.apache.org/security-8.html#Fixed_in_Apache_Tomcat_8.5.66).	**4** Κάτι τέτοιο είναι πολύ πιθανό να συμβεί, καθώς κάποιο με κάποια σειρά ενεργειών μπορούν να κάνουν τον Server να σταματήσει να ανταποκρίνεται.	**1** Μία τέτοια επίθεση θα ήταν αρκετά δύσκολο να συμβεί, καθώς δεν υπάρχει κάποια άμεση αλληλεπίδραση του χρήστη με τη βάση και συνεπώς καμία ενέργεια που να οδηγεί σε άρνηση υπηρεσιών στον Database Server.

7. Αποτίμηση αδυναμιών (vulnerability assessment)

Σε αυτό το ερώτημα καλούμαστε να κάνουμε αποτίμηση αδυναμιών για όλα τα αγαθά λογισμικού των τριών υπό μελέτη υπολογιστικών συστημάτων. Συγκεκριμένα τα αγαθά μας είναι τα παρακάτω:

- Λειτουργικό Σύστημα: Windows 10 x64
- Εξυπηρετητής Ιστού και εφαρμογής: Apache Tomcat/Catalina v. 8.5.66
- Εξυπηρετητής βάσης δεδομένων: Mysql v.8.0.31

Για το καθένα από τα παραπάνω αγαθά θα γίνει μία αναφορά στις κυριότερες αδυναμίες τους καθώς και μία περιγραφή αυτών των αδυναμιών. Για την εύρεση αυτών χρησιμοποιήσαμε την βάση αδυναμιών ασφάλειας του NIST (http://nvd.nist.gov/). Ως βασικότερες απειλές θεωρήσαμε αυτές που είχαν βαθμολογία από 7 και πάνω, δηλαδή αυτές που ήταν βαθμολογημένες, από την κλίμακα της NIST, ως High(7-8.9) ή Critical (>9) (Η κλίμακα είναι έχει εύρος τιμών από1 έως 10 και οι αντίστοιχες βαθμολογίες είναι Low,Medium,High,Critical). Για κάθε μία αδυναμία θα υπάρχει ο ανάλογος σύνδεσμος, η αναλυτική βαθμολογία επικινδυνότητάς της καθώς και μία περιγραφή της φύσης της. Αναλυτικότερα:

- Λειτουργικό Σύστημα: Windows 10 x64

1. **Windows TCP/IP Remote Code Execution Vulnerability**. Ο σύνδεσμος για αυτήν είναι (‘’https://nvd.nist.gov/vuln/detail/CVE-2022-34718‘’). Η βαθμολογία αυτής της αδυναμίας είναι 9.8 και κατατάσσεται στην κατηγορία Critical. Επρόκειτο για μια αδυναμία που θα μπορούσε να επιτρέψει σε έναν μη επαληθευμένο, απομακρυσμένο εισβολέα να εκτελέσει κώδικα με αυξημένα προνόμια στα επηρεαζόμενα συστήματα χωρίς αλληλεπίδραση με τον χρήστη. Ουσιαστικά, λόγω αυτού του κενού ασφαλείας, θα μπορούσε κάποιος χρήστης να στέλνει ειδικά δημιουργημένα πακέτα IPv6 σε έναν κόμβο/μηχάνημα των Windows, όπου είναι ενεργοποιημένο το IPSec, το οποίο θα μπορούσε να ενεργοποιήσει μια απομακρυσμένη εκτέλεση κώδικα σε αυτό το μηχάνημα.

2. **Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability.** Ο σύνδεσμος για αυτήν είναι (‘’ https://nvd.nist.gov/vuln/detail/CVE-2022-34721‘’). Η βαθμολογία αυτής της αδυναμίας είναι 9.8 και κατατάσσεται στην κατηγορία Critical. Σε αυτήν την αδυναμία θα μπορούσε ένας εισβολέας, χωρίς έλεγχο ταυτότητας, να στείλει ένα ειδικά κατασκευασμένο πακέτο IP σε ένα μηχάνημα-στόχο που εκτελεί Windows και έχει ενεργοποιημένο το IPSec, το οποίο θα μπορούσε να ενεργοποιήσει μια απομακρυσμένη εκμετάλλευση της εκτέλεσης κώδικα. Αυτή η ευπάθεια επηρεάζει μόνο το κλειδί τύπου IKEv1. Το IKEv2 δεν επηρεάζεται. Ωστόσο, όλοι οι διακομιστές Windows επηρεάζονται επειδή δέχονται πακέτα V1 και V2.

3. **Server Service Remote Protocol Elevation of Privilege Vulnerability.** Ο σύνδεσμος για αυτήν είναι (‘’ https://nvd.nist.gov/vuln/detail/CVE-2022-38045‘’). Η βαθμολογία αυτής της αδυναμίας είναι 9.8 και κατατάσσεται στην κατηγορία Critical. Μέσω της συγκεκριμένης αδυναμίας ένας εισβολέας θα μπορούσε να διαγράψει μόνο στοχευμένα αρχεία σε ένα σύστημα που τρέχει Windows. Δεν θα αποκτούσε όμως δικαιώματα προβολής ή τροποποίησης του περιεχομένου του εκάστοτε αρχείου.

- Εξυπηρετητής Ιστού και εφαρμογής: Apache Tomcat v. 8.5.66

1. **Application Continues Using Socket After It Has Been Closed.** Ο σύνδεσμος για αυτήν είναι (‘’ https://nvd.nist.gov/vuln/detail/CVE-2022-25762‘’). Η βαθμολογία αυτής της αδυναμίας είναι 8.6 και κατατάσσετε στην κατηγορία High. Το πρόβλημα είναι πως εάν μια εφαρμογή ιστού στέλνει ένα μήνυμα WebSocket ταυτόχρονα με το κλείσιμο της σύνδεσης WebSocket όταν αυτά εκτελούνται σε Apache Tomcat 8.5.0 έως 8.5.75 ή Apache Tomcat 9.0.0.M1 έως 9.0.20, είναι πιθανό η εφαρμογή να συνεχίσει να χρησιμοποιεί την υποδοχή(Socket) αφού έχει κλείσει. Ο χειρισμός σφαλμάτων που ενεργοποιείται σε αυτήν την περίπτωση θα μπορούσε να προκαλέσει την τοποθέτηση ενός συγκεκριμένου/’’χρησιμοποιημένου’’ αντικειμένου στο pool δύο φορές. Αυτό θα μπορούσε να οδηγήσει σε επακόλουθες συνδέσεις που χρησιμοποιούν ταυτόχρονα το ίδιο αντικείμενο, κάτι που θα μπορούσε να έχει ως αποτέλεσμα την επιστροφή δεδομένων σε λάθος ενέργεια ή/και άλλα σφάλματα.

2. **An Incorrect Default Permissions Vulnerability In The Packaging Of Tomcat.** Ο σύνδεσμος για αυτήν είναι (‘’ https://nvd.nist.gov/vuln/detail/CVE-2020-8022‘’). Η βαθμολογία αυτής της αδυναμίας είναι 7.8 και κατατάσσεται στην κατηγορία High. Η συγκεκριμένη

αδυναμία δημιουργεί προβλήματα στα πακέτα των αντίστοιχων εκδόσεων του Tomcat καθώς θα μπορούσε κάποιος χρήστης να έχει δικαιώματα διαχειριστή by-default χωρίς αυτά να προορίζονται γι' αυτόν.

3. **Bug_63362 Introduced A Memory Leak.** Ο σύνδεσμος για αυτήν είναι (" https://nvd.nist.gov/vuln/detail/CVE-2021-42340"). Η βαθμολογία αυτής της αδυναμίας είναι 7.5 και κατατάσσεται στην κατηγορία High. Μέσω του συγκεκριμένου Bug/Αδυναμίας, ένα αντικείμενο που εισήχθη για τη συλλογή μετρήσεων για συνδέσεις αναβάθμισης HTTP δεν κυκλοφόρησε για συνδέσεις WebSocket μόλις έκλεισε η σύνδεση. Αυτό θα δημιουργήσει μια διαρροή μνήμης που, με την πάροδο του χρόνου, θα μπορούσε να οδηγήσει σε άρνηση υπηρεσίας μέσω ενός OutOfMemoryError.

- Εξυπηρετητής βάσης δεδομένων: MySQL v 8.0.31

1. **Vulnerability in the MySQL Server product of Oracle MySQL**. Ο σύνδεσμος για αυτήν είναι (" https://nvd.nist.gov/vuln/detail/CVE-2021-2144"). Η βαθμολογία αυτής της αδυναμίας είναι 7.2 και κατατάσσεται στην κατηγορία High. Η αδυναμία αυτή είναι εύκολα εκμεταλλεύσιμη και επιτρέπει στον εισβολέα με υψηλά προνόμια και πρόσβαση στο δίκτυο μέσω πολλαπλών πρωτοκόλλων να υπονομεύσει τον MySQL Server. Οι επιτυχείς επιθέσεις αυτής της ευπάθειας μπορούν να οδηγήσουν στην εξαγορά του MySQL Server. (Επιπτώσεις στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα κ.ά.)

2. **Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer)**. Ο σύνδεσμος για αυτήν είναι ("https://nvd.nist.gov/vuln/detail/CVE-2021-35610").

Η βαθμολογία αυτής της αδυναμίας είναι 7.2 και κατατάσσεται στην κατηγορία High. Η αδυναμία αυτή είναι εύκολα εκμεταλλεύσιμη και επιτρέπει στον εισβολέα ακόμα και με χαμηλά προνόμια και πρόσβαση στο δίκτυο μέσω πολλαπλών πρωτοκόλλων να υπονομεύσει τον MySQL Server. Οι επιτυχείς επιθέσεις αυτής της ευπάθειας μπορούν να οδηγήσουν σε μη εξουσιοδοτημένη δυνατότητα πρόκλησης διακοπής λειτουργίας ή συχνά επαναλαμβανόμενης διακοπής λειτουργίας (πλήρες DOS) του MySQL Server καθώς και μη εξουσιοδοτημένης ενημέρωσης, εισαγωγής ή διαγραφής πρόσβασης σε ορισμένα από τα προσβάσιμα ως τότε δεδομένα του MySQL Server. (Επιπτώσεις ακεραιότητας και διαθεσιμότητας)

Σχόλια:

- Σε κάθε σύνδεσμο υπάρχει μέσα και ο κωδικός που έχει δοθεί στην κάθε αδυναμία της μορφής (CVE-…-…)
- Προφανώς υπάρχουν και άλλες βάσεις με τις δικές τους αξιολογήσεις (π.χ. η CNA: Microsoft Corporation) αλλά εμείς επιλέξαμε την NVD.
- Υπάρχουν και άλλες αδυναμίες για κάθε ένα αγαθό παρ’ όλα αυτά η σημαντικότητά τους δεν είναι αρκετά υψηλή ώστε να συμπεριληφθούν ως βασικότερες.
- Προτεραιότητα στις αδυναμίες , εκτός από την σοβαρότητά τους, δώσαμε και με βάση την ημερομηνία έκδοσης τους αντίστοιχου άρθρου γι’ αυτές.