Πανεπιστήμιο Πατρών

Τμήμα Μηχανικών Η/Υ
& Πληροφορικής

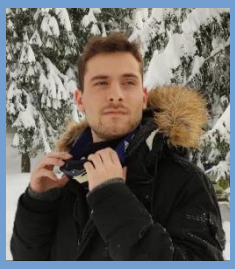
WhatToWear

Risk Assessment v1.0

Table of Contents

Σύνθεση Ομάδας

Μπαράκος Παναγιώτης



Έτος : 6ο

Α.Μ. : 1067514

Email επικοινωνίας : up1067514@upnet.gr

Βαλλάτος Αλέξανδρος

Έτος : 6ο

Α.Μ. : 1067478

Email επικοινωνίας : up1067478@upnet.gr

Βέργης Γρηγόρης

Έτος : 6ο

Α.Μ. : 1067418

Email επικοινωνίας : up1067418@upnet.gr

Μπάτσικας Θεόδωρος

Έτος : 8ο

Α.Μ. : 1058113

Email επικοινωνίας : up1058113@upnet.gr

Περίγραμμα κινδύνων

Λάθος χρονοπρογραμματισμός

Ο προγραμματισμός που έχει γίνει για την ομάδα και το έργο έχει μεγάλη πιθανότητα να είναι λανθασμένος, το οποίο θα είχε αποτέλεσμα την καθυστέρηση του έργου καθώς και αύξηση οικονομικών αναγκών. Κάτι τέτοιο είναι πιθανό να συμβεί λόγω καθυστερήσεων είτε από τα μέλη της ομάδας, είτε από εξωτερικούς παράγοντες (π.χ. νομικά ζητήματα). Για την αντιμετώπιση αυτών έχουμε οργανώσει και μοιράσει τα ζητούμενα του έργου σε μικρά κομμάτια τα οποία είναι δυνατό να εκτελεστούν σε διάστημα μίας εβδομάδας σε συμφωνία με τα Sprints μας, κάτι το οποίο θα βοηθήσει τα μέλη της ομάδας να είναι ενημερωμένα για την πορεία του έργου και να βρίσκονται συνέχεια σε εγρήγορση, καθώς και εβδομαδιαία meetings sprint planning.

Θέματα ασφαλείας

Στην εφαρμογή μας αποθηκεύονται προσωπικά δεδομένα χρηστών και επιχειρήσεων (e-mail, κωδικοί, στοιχεία για την ταυτοποίηση της επιχείρησης κτλ.) τα οποία είναι απαραίτητα για την ομαλή λειτουργία της εφαρμογής. Τα δεδομένα αυτά είναι πιθανό να πέσουν θύμα κάποιου είδους κυβερνοεπιθέσης ή να διαρρεύσουν μέσω μη ελεγχόμενης πρόσβασης. Για την αντιμετώπιση των προβλημάτων αυτών, μπορούμε να χρησιμοποιήσουμε τις παρακάτω μεθόδους:

- Ελαχιστοποίηση των δεδομένων που χρειάζεται να αποθηκεύουμε
- Χρήση εφαρμογών τρίτων που ειδικεύονται πάνω στο τομέα (π.χ. Authentication providers)
- Συχνά τεστ διείσδυσης (penetration tests) με σκοπό την αναγνώριση και αντιμετώπιση θεμάτων ασφαλείας
- Χρήση προχωρημένων πρακτικών ασφαλείας όπως Single Sign-On, Magic Links, κτλ.

Θέματα απόδοσης

Λόγω της φύσης της εφαρμογής που μοιάζει αρκετά με ένα ηλεκτρονικό κατάστημα αναμένεται να υπάρχει υψηλός αριθμός χρηστών ανά πάσα στιγμή. Αυτό θα έχει το αποτέλεσμα αύξησης του χρόνου ανταπόκρισης των server μας, μειώνοντας έτσι την εμπειρία των χρηστών. Για την αντιμετώπιση αυτών των προβλημάτων θα χρησιμοποιήσουμε τα εξής:

- CDNs έτσι ώστε η εφαρμογή να σερβίρεται από πολλά σημεία ανά πάσα στιγμή
- Cross-region λογαριασμούς, έτσι ώστε να εξυπηρετούμε χρήστες από όλες τις χώρες χωρίς καθυστερήσεις
- Caching layer (π.χ. Redis) για τα requests των καθημερινών χρηστών η οποία γίνεται invalidate όταν οι πωλητές αλλάζουν τα προϊόντα τους.

Νομικά ζητήματα

Η εφαρμογή κάνει χρήση προσωπικών δεδομένων πραγματικών προσώπων οπότε υπόκειται σε διάφορους νόμους που αφορούν την προστασία και ασφάλεια αυτών. Οι διαδικασίες και τα συστήματα που χρειάζεται να υλοποιηθούν για να διασφαλιστούν τα παραπάνω είναι αδύνατο να γνωρίζονται από τα βασικά μέλη της ομάδας καθώς κανείς δεν είναι ειδικός σε νομικά θέματα, οπότε θα χρειαστεί να γίνει πρόσληψη μίας νομικής ομάδας.

Αδυναμία επιτυχίας της εφαρμογής

Ο τομέας της μόδας και της ενδυμασίας με τον οποίο ασχολείται η εφαρμογή μας έχει την ιδιαιτερότητα να μεταβάλλεται συνεχώς και σε καθημερινή βάση, κάτι το όποιο θα δυσκολέψει την δουλεία μας να συνδυάζουμε επιλογές για τους χρήστες. Για αυτό το λόγο είναι πιθανό να υπάρχουν χρήστες οι οποίοι δεν είναι ικανοποιημένοι με τις επιλογές που προσφέρουμε. Είναι λοιπόν σημαντικό να υπάρχει ομάδα οι οποία θα ασχολείται καθημερινά με την ανανέωση και την εύρεση συνδυασμών για τους χρήστες μας.

Φόρμες ρίσκων

Λάθος χρονοπρογραμματισμός

ΛΑΘΟΣ ΧΡΟΝΟΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ			
Α/Α: 1	**Υπεύθυνος αντιμετώπισης:**	**Ημερομηνία:**	**Προτεραιότητα:**
Συνδεόμενη δραστηριότητα:		23-03-2024	☒ 1 ☐ 2 ☐ 3

Περιγραφή κινδύνου:

Ο προγραμματισμός που έχει γίνει για την ομάδα και το έργο έχει μεγάλη πιθανότητα να είναι λανθασμένος, το οποίο θα είχε αποτέλεσμα την καθυστέρηση του έργου καθώς και αύξηση οικονομικών αναγκών.

Τύπος: ☐ Σχέδιο ☐ Ποιότητα ☒ Κόστος

Επεξήγηση: Λόγω της καθυστέρησης του έργου, αυξάνεται το συνολικό κόστος διότι χρειάζεται παραπάνω χρόνο για να ολοκληρωθούν οι επιμέρους εργασίες.

Επίπεδο σοβαρότητας συνεπειών:	**Πιθανότητα:**
☒ Υψηλό ☐ Μεσαίο ☐ Χαμηλό	☒ Μεγάλη ☐ Μεσαία ☐ Μικρή

Πρώτο γεγονός ενεργοποίησης κινδύνου:

Μεγάλη χρονική διαφορά μεταξύ χρονουπολογισμού και πραγματικού χρόνου για κάποιο υπό-έργο.

Στρατηγική μετριασμού:

Χρήση sprint cycles μικρού χρονικού διαστήματος με σκοπό τη συνεχή ενημέρωση και συμμετοχή όλων των μελών της ομάδας, καθώς και εβδομαδιαία meetings sprint planning.

Γεγονός έναρξης της επιβολής της στρατηγικής αντιμετώπισης:

Συνεχή αύξηση στις διαφορές μεταξύ χρονουπολογισμού και πραγματικού χρόνου για υπό-έργα.

Στρατηγική αντιμετώπισης:

Επανάληψη κατασκευής του Project Plan με βάση τα νέα δεδομένα του έργου και του τελικού στόχου, με πιθανόν αλλαγές στη διαδικασία, το τελικό στόχο καθώς και τις διαδικασίες της ομάδας.

Παρακολούθηση κινδύνου

Ημερομηνία	Δράση	Κατάσταση

Κριτήρια απενεργοποίησης κινδύνου:	**Τρέχουσα κατάσταση:**
Εκτέλεση των υπό-έργων με βάση τον χρονουπολογισμό.	☐ Ενεργός ☒ Ανενεργός
Τελική ημερομηνία παρακολούθησης κινδύνου:	

Θέματα ασφαλείας

ΘΕΜΑΤΑ ΑΣΦΑΛΕΊΑΣ			
Α/Α: 2 **Συνδεόμενη δραστηριότητα:**	**Υπεύθυνος αντιμετώπισης:**	**Ημερομηνία:** 24-03-2024	**Προτεραιότητα:** ☒ 1 ☐ 2 ☐ 3
Περιγραφή κινδύνου: Στην εφαρμογή μας αποθηκεύονται προσωπικά δεδομένα χρηστών και επιχειρήσεων (e-mail, κωδικοί, στοιχεία για την ταυτοποίηση της επιχείρησης κτλ.) τα οποία είναι απαραίτητα για την ομαλή λειτουργία της εφαρμογής. Τα δεδομένα αυτά είναι πιθανό να πέσουν θύμα κάποιου είδους κυβερνοεπιθέσης ή να διαρρεύσουν μέσω μη ελεγχόμενης πρόσβασης.			
Τύπος: ☐ Σχέδιο ☒ Ποιότητα ☐ Κόστος **Επεξήγηση:** Η διαρροή προσωπικών δεδομένων ενός χρήστη, δημιουργεί πολύ κακή φήμη για την ασφάλεια της εφαρμογής και την ποιότητα της.			
Επίπεδο σοβαρότητας συνεπειών: ☒ Υψηλό ☐ Μεσαίο ☐ Χαμηλό		**Πιθανότητα:** ☒ Μεγάλη ☐ Μεσαία ☒ Μικρή	
Πρώτο γεγονός ενεργοποίησης κινδύνου: Μη φυσιολογική κίνηση στα συστήματα μας (logs, graphs).			
Στρατηγική μετριασμού: Χρήση 3rd party εφαρμογών που ειδικεύονται σε τομείς ασφαλείας, καθώς και συχνά penetration tests, ιδιαίτερα όταν συμβαίνουν αλλαγές σε συστήματα που αφορούν τα δεδομένα χρηστών.			
Γεγονός έναρξης της επιβολής της στρατηγικής αντιμετώπισης: Οποιοδήποτε δείγμα κυβερνοεπίθεσης ή διαρροής δεδομένων.			
Στρατηγική αντιμετώπισης: Άμεση ανάκληση στοιχείων πρόσβασης στα συστήματα (π.χ. access tokens) και διερεύνηση της διαρροής για αναγνώριση της πηγής της, καθώς και αλλαγές που μπορούν να γίνουν για την αντιμετώπιση της.			
Παρακολούθηση κινδύνου			
Ημερομηνία	Δράση		Κατάσταση
Κριτήρια απενεργοποίησης κινδύνου: Επιτυχία σε penetration test με το είδος επίθεσης που δέχτηκαν τα συστήματα πριν.		**Τρέχουσα κατάσταση:** ☐ Ενεργός ☒ Ανενεργός	
Τελική ημερομηνία παρακολούθησης κινδύνου:			

Θέματα απόδοσης

ΘΕΜΑΤΑ ΑΠΟΔΟΣΗΣ			
Α/Α: 3 **Συνδεόμενη δραστηριότητα:**	**Υπεύθυνος αντιμετώπισης:**	**Ημερομηνία:** 24-03-2024	**Προτεραιότητα:** ☐ 1 ☐ 2 ☒ 3
Περιγραφή κινδύνου: Λόγω της φύσης της εφαρμογής που μοιάζει αρκετά με ένα ηλεκτρονικό κατάστημα αναμένεται να υπάρχει υψηλός αριθμός χρηστών ανά πάσα στιγμή. Αυτό θα έχει το αποτέλεσμα αύξησης του χρόνου ανταπόκρισης των server μας, μειώνοντας έτσι την εμπειρία των χρηστών.			
Τύπος: ☒ Σχέδιο ☒ Ποιότητα ☐ Κόστος **Επεξήγηση:** Η καθυστέρηση εξυπηρέτησης requests χρηστών, καθώς και downtimes της εφαρμογής, δείχνουν πως ο σχεδιασμός καθώς και η ποιότητα της εφαρμογής δεν είναι αρκετά καλοί.			
Επίπεδο σοβαρότητας συνεπειών: ☐ Υψηλό ☐ Μεσαίο ☒ Χαμηλό		**Πιθανότητα:** ☐ Μεγάλη ☐ Μεσαία ☒ Μικρή	
Πρώτο γεγονός ενεργοποίησης κινδύνου: Μεγάλος αριθμός παραπόνων χρηστών.			
Στρατηγική μετριασμού: Χρήσης caching layer (π.χ. Redis) για τα requests των καθημερινών χρηστών η οποία γίνεται invalidate όταν οι πωλητές αλλάζουν τα προϊόντα τους.			
Γεγονός έναρξης της επιβολής της στρατηγικής αντιμετώπισης: Συνεχόμενη αύξηση παραπόνων χρηστών, καθώς και παρακολούθηση αύξησης χρόνου εξυπηρέτησης χρηστών σε logs.			
Στρατηγική αντιμετώπισης: Χρήση CDNs και cross-region accounts για γρηγορότερη εξυπηρέτηση αιτημάτων χρηστών, καθώς και σχεδιασμός της εφαρμογής για υποστήριξη μεγάλου αριθμού χρηστών.			
Παρακολούθηση κινδύνου			
Ημερομηνία	Δράση		Κατάσταση
Κριτήρια απενεργοποίησης κινδύνου: Ομαλή λειτουργία εφαρμογής, χωρίς μεγάλο αριθμό παραπόνων χρηστών.		**Τρέχουσα κατάσταση:** ☐ Ενεργός ☒ Ανενεργός	
Τελική ημερομηνία παρακολούθησης κινδύνου:			

Νομικά ζητήματα

ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ			
Α/Α: 4 **Συνδεόμενη δραστηριότητα:**	**Υπεύθυνος αντιμετώπισης:**	**Ημερομηνία:** 24-03-2024	**Προτεραιότητα:** ☒ 1 ☐ 2 ☐ 3
Περιγραφή κινδύνου: Η εφαρμογή κάνει χρήση προσωπικών δεδομένων πραγματικών προσώπων οπότε υπόκειται σε διάφορους νόμους που αφορούν την προστασία και ασφάλεια αυτών.			
Τύπος: ☐ Σχέδιο ☒ Ποιότητα ☒ Κόστος **Επεξήγηση:** Το κόστος που μπορεί να υπάρξει από τα πρόστιμα και δικαστικά έξοδα σε περίπτωση μη συμμόρφωσης με νομικά θέματα μπορεί να είναι πάρα πολύ μεγάλο, κάτι το οποίο θα δημιουργήσει πρόβλημα στα οικονομικά του έργου. Συγχρόνως, μη τήρηση αυτών μπορεί να εμφανιστεί ως κακή ποιότητα της εφαρμογής στους χρήστες, λόγω της μη τήρησης κοινών νομικών πλαισίων.			
Επίπεδο σοβαρότητας συνεπειών: ☒ Υψηλό ☐ Μεσαίο ☐ Χαμηλό		**Πιθανότητα:** ☐ Μεγάλη ☒ Μεσαία ☐ Μικρή	
Πρώτο γεγονός ενεργοποίησης κινδύνου: Αναφορά από κάποιον χρήστη ή φορέα για διαρροή δεδομένων, ή πρόστιμο για μη τήρηση πλαισίων.			
Στρατηγική μετριασμού: Άμεση πρόσληψη νομικής ομάδας			
Γεγονός έναρξης της επιβολής της στρατηγικής αντιμετώπισης: Συνεχόμενη αύξηση περιστατικών αναφοράς από χρήστες ή φορείς.			
Στρατηγική αντιμετώπισης: Σχεδιασμός της εφαρμογής καθώς και της αποθήκευσης δεδομένων με σκοπό την αποφυγή των νομικών θεμάτων που προκύπτουν.			
Παρακολούθηση κινδύνου			
Ημερομηνία	Δράση		Κατάσταση
Κριτήρια απενεργοποίησης κινδύνου: Επίλυση των νομικών ζητημάτων που υπάρχουν.		**Τρέχουσα κατάσταση:** ☐ Ενεργός ☒ Ανενεργός	
Τελική ημερομηνία παρακολούθησης κινδύνου:			

Αδυναμία επιτυχίας της εφαρμογής

ΑΔΥΝΑΜΙΑ ΕΠΙΤΥΧΙΑΣ ΤΗΣ ΕΦΑΡΜΟΓΗΣ			
Α/Α: 5 **Συνδεόμενη δραστηριότητα:**	**Υπεύθυνος αντιμετώπισης:**	**Ημερομηνία:** 24-03-2024	**Προτεραιότητα:** ☒ 1 ☐ 2 ☐ 3

Περιγραφή κινδύνου:

Ο τομέας της μόδας και της ενδυμασίας με τον οποίο ασχολείται η εφαρμογή μας έχει την ιδιαιτερότητα να μεταβάλλεται συνεχώς και σε καθημερινή βάση, κάτι το οποίο θα δυσκολέψει την δουλειά μας να συνδυάζουμε επιλογές για τους χρήστες. Για αυτό το λόγο είναι πιθανό να υπάρχουν χρήστες οι οποίοι δεν είναι ικανοποιημένοι με τις επιλογές που προσφέρουμε.

Τύπος: ☐ Σχέδιο ☐ Ποιότητα ☒ Κόστος

Επεξήγηση: Αδυναμία προσέλκυσης χρηστών στην εφαρμογή έχει καταστροφικές συνέπειες για το μέλλον της εφαρμογής εφόσον δεν θα υπάρχει οικονομική ροή για τη στήριξη της ύπαρξης της.

Επίπεδο σοβαρότητας συνεπειών:	**Πιθανότητα:**
☒ Υψηλό ☐ Μεσαίο ☐ Χαμηλό	☐ Μεγάλη ☐ Μεσαία ☒ Μικρή

Πρώτο γεγονός ενεργοποίησης κινδύνου:

Μειωμένη κίνηση χρηστών και πωλητών στη πλατφόρμα με βάση τα κόστη που χρειάζεται για την επιβίωση της, μετά ένα αρχικό χρονικό διάστημα.

Στρατηγική μετριασμού:

Αναθεώρηση του marketing και πρόσληψη ομάδας με συγκεκριμένα αυτό το σκοπό.

Γεγονός έναρξης της επιβολής της στρατηγικής αντιμετώπισης:

Συνεχόμενη μείωση της κίνησης στη πλατφόρμα, ακόμη και μετά τις αλλαγές στο marketing.

Στρατηγική αντιμετώπισης:

Έρευνα στην αγορά για τις ανάγκες των χρηστών, καθώς και μελέτη των κριτικών της εφαρμογής, ιδιαίτερα των αρνητικών.

Παρακολούθηση κινδύνου

Ημερομηνία	Δράση	Κατάσταση

Κριτήρια απενεργοποίησης κινδύνου:	**Τρέχουσα κατάσταση:**
Ομαλή κίνηση με συνεχομένη σταδιακή αύξηση των χρηστών.	☐ Ενεργός ☒ Ανενεργός
Τελική ημερομηνία παρακολούθησης κινδύνου:	