Δρ. Μαριάς Ιωάννης
Επικ. Καθηγητής

Προπτυχιακό Πρόγραμμα Σπουδών
Χειμερινό εξάμηνο 2022-2023

Ασφάλεια Δικτύων Εργαστηριακή Άσκηση 2

Σύντομη περιγραφή:

Στην συγκεκριμένη εργασία θα χρησιμοποιήσετε και επεκτείνετε την υποδομή που υλοποιήσατε στην εργαστηριακή άσκηση 1 (στο ίδιο VM). Πιο συγκεκριμένα πρέπει:

1. Να επεκτείνετε την φόρμα που δημιουργήσατε να δέχεται username και password.
2. Να υλοποιήσετε backend σύστημα σε Java, Python. PHP(προτείνουμε τη χρήση του framework java spring boot, python django, php symfony) το οποίο να υποστηρίζει δυνατότητες login.
3. Να ανεβάσετε την υλοποίηση σας στον server
   Μέχρι την ανακοίνωση των αποτελεσμάτων της 1ης εργασίας δεν πρέπει να κάνετε καμία μεταβολή στον server (εκτιμώμενη ημερομηνία 11/1)
4. Να φτιάξετε μηχανισμούς παρακολούθησης δραστηριότητας στο login endpoint που δημιουργήσατε.

Εισαγωγή:

Στα πληροφοριακά συστήματα παγκόσμιου ιστού (Web apps) η είσοδος στο ιδιωτικό περιβάλλον του συστήματος πραγματοποιείται ύστερα από διαδικασία login κατά την οποία ο εγγεγραμμένος χρήστης εισάγει τα διαπιστευτήρια του όνομα χρήστη και κωδικό πρόσβασης σε κατάλληλη web-form, που τα αποστέλλει μέσω κομβίου submit (Είσοδος/Login) για επεξεργασία είτε σε server side script (PHP, Python, Perl CGI) είτε σε Rest Web Service endpoint του web application server της εφαρμογής που υλοποιεί τον έλεγχο των διαπιστευτηρίων. Ο βασικός έλεγχος που πραγματοποιείται αναλύεται στα εξής δύο (2) βήματα:

I. Έλεγχος στη βάση δεδομένων του web πληροφοριακού συστήματος αν υπάρχει χρήστης με αυτό το όνομα χρήστη
II. Υπολογισμός της σύνοψης (hash) του κωδικού που έδωσε ο χρήστης στο web-form και ανακτώντας την εγγραφή με τα στοιχεία του χρήστη από τη βάση δεδομένων ελέγχετε αν το αποθηκευμένο hash του κωδικού του καταχωρημένου χρήστη είναι ίδιο με το hash που υπολογίστηκε από τον κωδικό πρόσβασης που έδωσε στο αντίστοιχο πεδίο του web-form.

Αν τα hashes ταυτίζονται ο χρήστης εισάγεται στο ιδιωτικό περιβάλλον της web εφαρμογής που παρέχει λειτουργίες που δεν είναι δημόσιες στον παγκόσμιο ιστό αλλά είναι διαθέσιμες μόνο για τους νόμιμους χρήστες της.

Στα πλαίσια της εργασίας καλείστε να κάνετε τα εξής :

Να δημιουργήσετε σχεσιακή βάση δεδομένων με όνομα GDPR σε σύστημα διαχείρισης βάσεων δεδομένων MySQL ή MariaDB ή PostgreSQL και πίνακα users στη βάση που αποθηκεύει τα απαραίτητα δεδομένα για τη βασική λειτουργία Μηχανισμού Login με πεδία (columns) όνομα χρήστη (username), κωδικός χρήστη (password), περιγραφή χρήστη (description) ορίζοντας τις κατάλληλες εντολές σε γλώσσα ερωτημάτων SQL που απαιτούνται όχι μόνο για τη δημιουργία της βάσης αλλά και του πίνακα όσον αφορά τόσο τον καθορισμό του τύπου δεδομένων των πεδίων του πίνακα όσο και τον ορισμό κατάλληλου πεδίου που θα παίξει το ρόλο πρωτεύοντος κλειδιού αναζήτησης (primary key) εγγραφών (records) στον πίνακα. Στην περίπτωση που χρησιμοποιήσετε κάποιο framework δεν είναι ανάγκη να μας παρέχετε τον SQL κώδικα καθώς αυτός παράγεται αυτόματα μέσα από τον κώδικα και μέσω του κώδικα μπορούμε να ελέγξουμε την ορθότητα του. Θα εισάγετε στον πίνακα users με τις κατάλληλες εντολές SQL δύο (2) χρήστες, ο πρώτος θα έχει όνομα χρήστη τον αριθμό μητρώου σας και ο δεύτερος θα έχει όνομα χρήστη admin. **(15 πόντοι)**

Ποιες είναι οι ενδεδειγμένες λύσεις για την αποθήκευση του κωδικού του χρήστη στη βάση ώστε να διασφαλιστεί η ιδιωτικότητα του σε περίπτωση παράνομης εξαγωγής δεδομένων από τη βάση; Να παραθέσετε τις εντολές SQL ή γλώσσα προγραμματισμού υψηλού επιπέδου (συμπεριλαμβάνεται η χρήση framework) που απαιτούνται για το σωστό μετασχηματισμό του πεδίου password με μεγαλύτερο επίπεδο ασφαλείας. **(25 πόντοι)**

Σε γλώσσα προγραμματισμού της επιλογής σας Java, Python, PHP και αν το επιθυμείτε με τη χρησιμοποίηση κάποιου framework (προτείνεται) θα δημιουργήσετε μια απλή web εφαρμογή μέσω της οποίας οι χρήστες που δηλώσατε θα μπορούν να κάνουν Login χρησιμοποιώντας κατάλληλο endpoint. Ο κώδικάς σας πρέπει να είναι κατάλληλα διαμορφωμένος ώστε να μην δύναται να πραγματοποιηθεί επίθεση SQL injection. **(25 πόντοι)**

Χρησιμοποιώντας τα κατάλληλα ερωτήματα SQL είτε μέσω γλώσσας υψηλού επιπέδου είτε μέσω framework, να σχεδιάσετε πίνακα με όνομα logging στη βάση GDPR που θα καταγράφει τις απόπειρες επιτυχούς login με κατάλληλο πεδίο χρονοσφραγίδας. Θα πρέπει να προσθέσετε είτε sql procedures είτε να ρυθμίσετε μέσω της εφαρμογής σας ελέγχους για το πόσες φορές θα επιτρέπεται σε έναν χρήστη να κάνει login attempt μέχρι να τον “κλειδώσετε” και να εμφανίσετε κατάλληλο μήνυμα μέσω alert στο front end. Επίσης, υλοποιήστε ελέγχους οι οποίοι θα ελέγχουν

πότε αλλάχτηκε τελευταία φορά ο κωδικός του χρήστη και να ορίσετε χρονικό διάστημα το οποίο αν παρέλθει θα πρέπει να ζητάτε από τον χρήστη να αλλάξει τον κωδικό του(την αλλαγή κωδικού σαν λειτουργία δεν είναι ανάγκη να την υλοποιήσετε). Δώστε αναλυτικά παραδείγματα με screenshots από την υλοποίηση σας για τα παραπάνω. **(35 πόντοι).**

Προαιρετικά:
Δημιουργία login και access μέσω jwt token. Προϋποθέτει την δημιουργία κλειδιών τα οποία θα παράγουν το token το οποίο θα γίνεται assign στο χρήστη και θα λήγει σύμφωνα με το configuration σας. Πρέπει να δημιουργήσετε και ένα dummy HelloWorld endpoint προκειμένου να παρουσιάσετε τη λειτουργία με το jwt. Δηλαδή κάποιος για να χτυπήσει το HelloWorld, πρέπει πρώτα να κάνει login να πάρει το jwt του και μετά να το χρησιμοποιήσει για να χτυπήσει το helloworld. Σε διαφορετική περίπτωση δεν θα είναι δυνατόν να έχει access σε αυτό. **(bonus +30 πόντοι)**

Παραδοτέα:
Σε αρχείο zip με όνομα τον αριθμού μητρώου σας πρέπει να υποβάλλετε ένα αρχείο (report) pdf που θα περιέχει τα στοιχεία σας και τις απαντήσεις σας (όπου σας έχει ζητηθεί), καθώς και τα αρχεία κώδικα.

Απορίες:
στο eclass -> Συζητήσεις/ Εργαστηριακές Ασκήσεις / 4. SQL Injection

Χρήσιμα links για frameworks symfony, spring:

- https://www.baeldung.com/spring-security-login
- https://www.baeldung.com/spring-security-oauth-jwt
- https://medium.com/@joeymasip/how-to-create-an-api-with-symfony-4-and-jwt-b2334a8fbec2
- https://symfony.com/doc/current/security/form_login_setup.html

Deadline: 24/1/2022