ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΤΜΗΜΑ: ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧ/ΚΩΝ & ΜΗΧ/ΚΩΝ Η/Υ
ΜΑΘΗΜΑ: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Διδακτικό έτος: 2024 -2025

Εργασία για το μάθημα «Ασφάλεια Πληροφοριακών Συστημάτων»

Αντικείμενο της εργασίας:

Ανάδειξη προβλημάτων ασφάλειας σε δικτυακή εφαρμογή αποθήκευσης κωδικών πρόσβασης (password manager), καθώς και βελτίωση της εφαρμογής ως προς την ασφάλεια.

Ζητούμενα

Σας δίνεται μια απλουστευμένη υλοποίηση μιας εφαρμογής τύπου password manager που έχει διάφορα προβλήματα ως προς την ασφάλεια.

Στην εργασία πρέπει σύντομα και περιεκτικά να

- να επισημάνετε τα διάφορα προβλήματα ασφάλειας της εφαρμογής (κενά ασφαλείας)
- να παρουσιάσετε παραδείγματα εκμετάλλευσης των κενών ασφαλείας (όπου είναι δυνατό)
- να προτείνετε τρόπους αντιμετώπισης των προβλημάτων ασφάλειας
- να εφαρμόσετε μια προτεινόμενη λύση (όπου είναι δυνατό)

Τελικός σκοπός είναι να βελτιώσετε την εφαρμογή ως προς της ασφάλεια.

Η εργασία θα περιλαμβάνει το κείμενο που θα απαντάει στα παραπάνω, καθώς και τα απαραίτητα ψηφιακά αρχεία της βελτιωμένης υλοποίησής σας. Στο κείμενο θα πρέπει να συμπεριλάβετε τα στοιχεία σας (ονοματεπώνυμο, ΑΕΜ και ιδρυματικό email).

Καθώς ο σκοπός της εργασίας επικεντρώνεται σε θέματα ασφάλειας, η εμφάνιση και η λειτουργικότητα της υλοποίησης είναι δευτερεύουσας σημασίας και δεν πρέπει να σας απασχολούν.

Η υλοποίηση της εφαρμογής που σας δίνεται είναι σε PHP. Το SQL script για τη δημιουργία της απαραίτητης ΒΔ που χρησιμοποιείται από την εφαρμογή είναι για MySQL. Συνιστάται η χρήση του πακέτου XAMPP που περιλαμβάνει όλα τα απαραίτητα πακέτα (PHP, Apache web server, MySQL) χωρίς να απαιτεί εγκατάσταση. *Σημ. η επεξεργασία του PHP κώδικα μπορεί να γίνει με οποιοδήποτε editor (π.χ. Notepad++).*

Περιγραφή της εφαρμογής password manager

Η εφαρμογή χρησιμεύει για την αποθήκευση/ανάκτηση στοιχείων σύνδεσης (username/passwords) σε διάφορες ιστοσελίδες. Τα στοιχεία αυτά αποθηκεύονται σε πίνακα της ΒΔ. Ο χρήστης της εφαρμογής, αφού συνδεθεί μέσω login φόρμας (εισάγοντας όνομα χρήστη και κωδικό πρόσβασης), μπορεί να προβάλει δεδομένα που είναι ήδη αποθηκευμένα στη ΒΔ καθώς και να εισάγει νέα δεδομένα.

Η υλοποίηση της εφαρμογής έχει προβλήματα ασφάλειας όπως:

- Η σύνδεση της διαδικτυακής εφαρμογής με τη βάση δεδομένων γίνεται με διαπιστευτήρια διαχειριστή. Έτσι, κάποιος που μπορεί να εκτελέσει εντολές SQL, δεν περιορίζεται με κανέναν τρόπο από προνόμια.

- Δεν ελέγχονται τα δεδομένα που εισάγονται στις διάφορες φόρμες εισαγωγής κειμένου. Αυτό επιτρέπει σε κάποιον να επωφεληθεί από την τεχνική SQL injection για να εκτελέσει διάφορα ερωτήματα SQL.
- Η φόρμα εισαγωγής και εμφάνισης σχολίων μπορεί να χρησιμοποιηθεί για την υποκλοπή authentication cookies άλλων χρηστών με την τεχνική cross site scripting (XSS). Σύμφωνα με αυτή την τεχνική κάποιος κακόβουλος μαζί με κάποιο σχόλιο μπορεί να εισάγει κατάλληλο κώδικα JavaScript. Έτσι, όταν το σχετικό σχόλιο εμφανίζεται σε κάποιο χρήστη, ο κώδικας JavaScript, αν και αόρατος, εκτελείται στο πρόγραμμα περιήγησης του χρήστη-θύματος χωρίς αυτό να γίνει αντιληπτό και να υποκλέψει πληροφορίες. Τα cookies που υποκλέπτονται μπορούν να χρησιμοποιηθούν από τον υποκλοπέα για να υποδυθεί τον χρήστη-θύμα υποκλοπής *(σημ. στον υποφάκελο xss της υλοποίησης που σας δίνεται συμπεριλαμβάνεται σχετικός κώδικάς για την υποκλοπή και χρήση των cookies από τον υποκλοπέα – ο κώδικας αυτός δεν χρειάζεται βελτιώσεις)*.
- Όλες οι πληροφορίες καταχωρούνται ως απλό κείμενο (συμπεριλαμβανομένων των κωδικών πρόσβασης). Επομένως, κάποιος που έχει πρόσβαση στη βάση δεδομένων μπορεί να διαβάσει τα ευαίσθητα δεδομένα που περιέχονται στη ΒΔ.
- Εφόσον χρησιμοποιείται μη ασφαλές πρωτόκολλο HTTP, οποιοσδήποτε παρακολουθεί την κίνηση του δικτύου μπορεί να υποκλέψει όλες τις πληροφορίες που παρουσιάζονται σε έναν χρήστη.

Σημ. στον κώδικα που σας δίνεται συμπεριλαμβάνονται σχόλια για κάποιες βελτιώσεις στον κώδικα, κάποιες τεχνικές SQL injection και XSS, καθώς και 2 αρχεία με παραδείγματα συναρτήσεων κρυπτογράφησης και hashing στην PHP (test_encrypt.php, test_hash.php). Αν και τα παραπάνω δεν είναι εξαντλητικά, βοηθούν επαρκώς για την ολοκλήρωση της εργασίας.
