ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ

ΤΜΗΜΑ: ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧ/ΚΩΝ & ΜΗΧ/ΚΩΝ Η/Υ
ΜΑΘΗΜΑ: ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Διδακτικό έτος: 2025 -2026

Θέμα εργασίας: Ανάδειξη προβλημάτων ασφάλειας σε δικτυακή εφαρμογή αποθήκευσης κωδικών πρόσβασης (password manager) και αντιμετώπισή τους.

Ζητούμενα

Σας δίνεται μια web εφαρμογή μιας απλουστευμένης υλοποίησης ενός password manager σε PHP που χρησιμοποιεί μια ΒΔ σε MySQL με όνομα: `pwd_mgr`. Η υλοποίηση αυτή έχει διάφορα προβλήματα ασφάλειας που θα πρέπει να εντοπίσετε και να διορθώσετε.

Αναλυτικότερα θα πρέπει:

1. να επισημάνετε και να επεξηγήσετε τα προβλήματα ασφάλειας που εντοπίσατε, παρουσιάζοντας κάποιο παράδειγμα εκμετάλλευσης του κενού ασφαλείας
2. να προτείνετε κάποιο τρόπο αντιμετώπισης των παραπάνω προβλημάτων και να εφαρμόσετε μια λύση

μαζί με το κείμενο της εργασίας θα πρέπει να καταθέσετε και τα απαραίτητα ψηφιακά αρχεία της βελτιωμένης υλοποίησής σας μαζί με τα στοιχεία σας (ονοματεπώνυμο, ΑΕΜ και ιδρυματικό email).

Πρόσθετες οδηγίες

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

Χρησιμοποιήστε το πακέτο XAMPP (διατίθεται και στο elearning στην εργαστηριακή άσκηση 6), που περιλαμβάνει όλα τα απαραίτητα πακέτα (Apache web server, PHP, MySQL) χωρίς να απαιτεί εγκατάσταση. Αναλυτικότερες οδηγίες υπάρχουν στο elearning στην ενότητα: "Οδηγίες χρήσης του XAMPP".

Η επεξεργασία του PHP κώδικα μπορεί να γίνει με οποιοδήποτε editor (π.χ. Notepad++).

Η διαχείριση της ΒΔ μπορεί να γίνει με το πρόγραμμα HeidiSQL.

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 `pwd_mgr`. Ο χρήστης της εφαρμογής, αφού συνδεθεί μέσω login φόρμας, μπορεί να προβάλει τα δεδομένα που είναι ήδη αποθηκευμένα στη ΒΔ καθώς και να εισάγει νέα δεδομένα. Κατά τη δημιουργία της ΒΔ δημιουργείται και ένας δοκιμαστικός χρήστης με username/password: `u1` / `p1`

Η υλοποίηση της εφαρμογής έχει προβλήματα ασφάλειας όπως:

- Η σύνδεση της εφαρμογής με τη βάση δεδομένων γίνεται με διαπιστευτήρια διαχειριστή. Έτσι, κάποιος που μπορεί να εκτελέσει εντολές SQL, δεν περιορίζεται από προνόμια στο τί επιτρέπεται να κάνει.

- Τα δεδομένα που εισάγονται στις διάφορες φόρμες κειμένου δεν ελέγχονται. Αυτό επιτρέπει σε κάποιον να επωφεληθεί από την τεχνική SQL injection για να εκτελέσει διάφορα ερωτήματα SQL.
- Τα δεδομένα που εισάγονται στη φόρμα σημειώσεων/ανακοινώσεων δεν ελέγχονται. Αυτό επιτρέπει την υποκλοπή authentication cookies άλλων χρηστών με την τεχνική cross site scripting (XSS).

  (Σημ. στον υποφάκελο xss της υλοποίησης που σας δίνεται συμπεριλαμβάνεται σχετικός κώδικάς για την υποκλοπή και χρήση των cookies από τον υποκλοπέα).
- Οι ευαίσθητες πληροφορίες καταχωρούνται στη ΒΔ ως απλό κείμενο (π.χ. οι κωδικοί πρόσβασης). Επομένως, κάποιος που έχει πρόσβαση στη ΒΔ μπορεί να τις διαβάσει.
- Η χρήση του μη ασφαλούς πρωτοκόλλου HTTP επιτρέπει την υποκλοπή των πληροφοριών που παρουσιάζονται σε έναν χρήστη από κάποιον που παρακολουθεί την κίνηση του δικτύου.

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

Σύντομη περιγραφή αρχείων του passman:

- index.html: default σελίδα του passman
- register.php: σελίδα εγγραφής νέου χρήστη
- login.php/logout.php: σελίδες login/logout χρηστών στο passman
- dashboard.php: σελίδα εισαγωγής και εμφάνισης usernames/passwords ιστοσελίδων
- notes.php: σελίδα που εισάγονται και εμφανίζονται ανακοινώσεις

Σύντομη περιγραφή αρχείων του υποφακέλου xss (που αντιστοιχεί σε κάποιον κακόβουλο hacker):

- index.html: αρχική σελίδα
- getcookie.php: αρχείο που χρησιμεύει για την υποκλοπή authentication cookies (μέσω ανακοινώσεων που καταχωρούνται από τη σελίδα notes.php)
- stolencookies.txt: αρχείο καταγραφής υποκλεμμένων cookies
- listcookies.php: εμφάνιση υποκλεμμένων cookies
- usecookie.php: χρήση κάποιου υποκλεμμένου authentication cookie για πρόσβαση στο passman με το session id άλλου χρήστη

Τα παρακάτω εξαιρούνται των βελτιώσεων ασφαλείας καθώς είναι βοηθητικά αρχεία και δεν αποτελούν τμήμα της εφαρμογής passman: test_encrypt.php, test_hash.php, όλα τα αρχεία του υποφακέλου xss.
