Εισαγωγή:

Στόχος της παρούσας έκθεσης είναι να εντοπίσει και να περιγράψει πέντε ελαττώματα ασφαλείας που υπάρχουν σε μια εφαρμογή ιστού και να παράσχει συγκεκριμένες διορθώσεις για κάθε ελάττωμα. Η διαδικτυακή εφαρμογή αξιολογήθηκε για κοινά τρωτά σημεία ασφαλείας με βάση τον κατάλογο OWASP Top Ten. Κάθε ελάττωμα θα παρουσιαστεί μαζί με την περιγραφή του, τους πιθανούς κινδύνους και τα πρακτικά βήματα για τον μετριασμό των ευπαθειών.

---

ΕΥΠΑΘΕΙΑ 1: Cross-Site Scripting (XSS)

Σύνδεσμος πηγής: detail.html, γραμμή 7

Περιγραφή:
Το Cross-Site Scripting (XSS) είναι μια ευπάθεια που επιτρέπει σε έναν εισβολέα να εισάγει κακόβουλα σενάρια σε μια εφαρμογή ιστού. Στον παρεχόμενο κώδικα, το πρότυπο polls/detail.html δεν αποφεύγει σωστά τις εισόδους του χρήστη κατά την εμφάνιση των επιλογών ερωτήσεων. Ως αποτέλεσμα, αφήνει την εφαρμογή εκτεθειμένη σε πιθανές επιθέσεις XSS.

Πιθανοί κίνδυνοι:
Εάν ένας επιτιθέμενος εισάγει με επιτυχία κακόβουλα σενάρια στη σελίδα, μπορεί να υποκλέψει ευαίσθητα δεδομένα χρήστη, όπως cookies συνεδρίας ή διαπιστευτήρια σύνδεσης, και να εκτελέσει μη εξουσιοδοτημένες ενέργειες εκ μέρους του χρήστη.

Διόρθωση:
Για τον μετριασμό της ευπάθειας XSS, απαιτείται κατάλληλη επικύρωση εισόδου και κωδικοποίηση εξόδου. Τροποποιήστε το πρότυπο polls/detail.html για να αποφύγετε τις εισόδους του χρήστη χρησιμοποιώντας το ασφαλές φίλτρο.

---

ΕΥΠΑΘΕΙΑ 2: Ανασφαλείς άμεσες αναφορές αντικειμένων (IDOR)

Σύνδεσμος πηγής: views.py, γραμμή 24

Περιγραφή:
Ανασφαλείς άμεσες αναφορές αντικειμένων (IDOR) συμβαίνουν όταν μια εφαρμογή εκθέτει ευαίσθητες πληροφορίες ή λειτουργίες με αναφορές σε αντικείμενα απευθείας μέσω εισόδου που παρέχεται από τον χρήστη, όπως αναγνωριστικά. Στον παρεχόμενο κώδικα, η συνάρτηση vote δεν διαθέτει κατάλληλο έλεγχο πρόσβασης, επιτρέποντας σε οποιονδήποτε χρήστη να ψηφίσει σε οποιαδήποτε ερώτηση χωρίς έλεγχο δικαιωμάτων.

Πιθανοί κίνδυνοι:
Αυτή η ευπάθεια θα μπορούσε να οδηγήσει σε μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητους πόρους, χειραγώγηση δεδομένων και μη εξουσιοδοτημένες ενέργειες εντός της εφαρμογής.

Διόρθωση:
Για την αντιμετώπιση του IDOR, εφαρμόστε κατάλληλους ελέγχους δικαιωμάτων για να διασφαλίσετε ότι μόνο πιστοποιημένοι χρήστες μπορούν να ψηφίσουν σε ερωτήσεις. Προσθέστε το διακοσμητικό login_required στη συνάρτηση vote για να επιβάλλετε τον έλεγχο ταυτότητας.

---

ΕΥΠΑΘΕΙΑ 3: Εσφαλμένη ρύθμιση ασφαλείας (DEBUG = False)

Σύνδεσμος πηγής: settings.py, γραμμή 28

Description: (Περιγραφή):
Η λανθασμένη διαμόρφωση ασφαλείας συμβαίνει όταν μια εφαρμογή ιστού αναπτύσσεται με μη ασφαλείς ρυθμίσεις. Στον παρεχόμενο κώδικα, η λειτουργία DEBUG της εφαρμογής έχει οριστεί σε True, η οποία είναι ακατάλληλη για περιβάλλον παραγωγής.

Πιθανοί κίνδυνοι:
Σε ένα περιβάλλον παραγωγής, η ενεργοποίηση της λειτουργίας DEBUG θα μπορούσε να εκθέσει ευαίσθητες πληροφορίες, όπως ίχνη στοίβας και διαπιστευτήρια βάσης δεδομένων, σε επιτιθέμενους.

Διόρθωση:
Στο αρχείο settings.py, ορίστε τη ρύθμιση DEBUG σε False σε περιβάλλον παραγωγής για να αποτρέψετε την εμφάνιση λεπτομερών πληροφοριών σφάλματος.

---

ΕΥΠΑΘΕΙΑ 4: Πλαστογράφηση αιτήσεων Cross-Site (CSRF)

Σύνδεσμος πηγής: settings.py, γραμμή 48

Περιγραφή:
Παρόλο που δεν περιλαμβάνεται ρητά στο OWASP Top Ten 2017, το Cross-Site Request Forgery (CSRF) εξακολουθεί να αποτελεί πρόβλημα ασφάλειας. Η εφαρμογή δεν προστατεύεται από επιθέσεις CSRF.

Πιθανοί κίνδυνοι:
Οι επιθέσεις CSRF μπορούν να οδηγήσουν στην εκτέλεση μη εξουσιοδοτημένων ενεργειών εκ μέρους πιστοποιημένων χρηστών.

Διόρθωση:
Το Django παρέχει ενσωματωμένη προστασία CSRF χρησιμοποιώντας ένα ενδιάμεσο λογισμικό (CsrfViewMiddleware). Συμπεριλαμβάνεται αυτόματα στη ρύθμιση MIDDLEWARE στο αρχείο settings.py. Βεβαιωθείτε ότι το CSRF token είναι παρόν στις φόρμες σας κατά την υποβολή δεδομένων στον διακομιστή.

---

ΕΥΠΑΘΕΙΑ 5: Εγχείρηση SQL

Σύνδεσμος πηγής: views.py, γραμμή 18

Description: (περιγραφή):
Παρόλο που η εφαρμογή χρησιμοποιεί SQLite, η οποία δεν είναι ευάλωτη στην κλασική έγχυση SQL, είναι ζωτικής σημασίας να καταδείξετε πώς να χειρίζεστε την είσοδο του χρήστη με ασφάλεια, ειδικά όταν εργάζεστε με άλλες βάσεις δεδομένων.

Πιθανοί κίνδυνοι:
Χωρίς την κατάλληλη επικύρωση εισόδου, η εφαρμογή θα μπορούσε να είναι ευάλωτη σε SQL injection όταν εργάζεται με ευάλωτες βάσεις δεδομένων.

Διόρθωση:
Εφαρμόστε την παραμετροποίηση ερωτημάτων του Django για τον ασφαλή χειρισμό της εισόδου χρήστη και την αποτροπή επιθέσεων SQL injection. Τροποποιήστε τη συνάρτηση vote ώστε να χρησιμοποιεί την παραμετροποίηση ερωτημάτων.

---

Συμπέρασμα:

Η παρούσα έκθεση εντόπισε και περιέγραψε πέντε ελαττώματα ασφαλείας στην εφαρμογή ιστού με βάση τον κατάλογο OWASP Top Ten 2017. Κάθε ελάττωμα συνοδευόταν από λεπτομερή περιγραφή της ευπάθειας, των πιθανών κινδύνων και των συγκεκριμένων διορθώσεων κώδικα για την αντιμετώπιση των προβλημάτων. Ακολουθώντας τις παρεχόμενες διορθώσεις και εφαρμόζοντας πρακτικές ασφαλούς κωδικοποίησης, η διαδικτυακή εφαρμογή μπορεί να προστατευτεί καλύτερα από κοινές απειλές ασφαλείας.

Είναι σημαντικό να δίνεται προτεραιότητα στην ασφάλεια των εφαρμογών ιστού καθ' όλη τη διαδικασία ανάπτυξης, να εκτελείτε τακτικά δοκιμές ασφαλείας και να ενημερώνεστε για τις αναδυόμενες απειλές και τις βέλτιστες πρακτικές, ώστε να διασφαλίζεται μια ισχυρή και ασφαλής εφαρμογή ιστού.