Ασφάλεια Συστημάτων

Τζέριες Μπεσαράτ, PhD

8 Απριλίου 2022, Άρτα

Στο προηγούμενο μάθημα αναπτύξαμε

- Αρχές Ασφαλούς Προγραμματισμού
- Κατηγορίες Ευπαθειών
  - Υπερχείλιση ενταμιευτήρα (buffer overflow)
  - Μη επικυρωμένη είσοδος (invalidated input) χρήστη
  - Συνθήκες ανταγωνισμού (race conditions)
  - Προβλήματα ελέγχου πρόσβασης (access control)
  - Αποθήκευση σε σύστημα διαχείρισης βάσεων δεδομένων (ΣΔΒΔ)
- Μελέτη Περίπτωσης: Java

Ασφάλεια Διαδικτυακών Εφαρμογών

Σε αυτό το μάθημα παρουσιάζονται έννοιες που αφορούν την ασφάλεια των διαδικτυακών εφαρμογών (Web applications), στο πλαίσιο μιας σχετικής θεματολογίας και ορολογίας. Ακόμη, παρουσιάζεται ένα σύνολο δοκιμασμένων αρχών ασφάλειας, οι οποίες βασίζονται σε συστάσεις διεθνών οργανισμών και εταιρειών ανάπτυξης λογισμικού ιστού.

Τεκμηριώνεται, επίσης, η αναγκαιότητα υιοθέτησης μιας ολιστικής προσέγγισης σχετικά με τα ζητήματα ασφάλειας, ώστε να αντιμετωπίζονται σε όλα τα επίπεδα αρχιτεκτονικής μιας διαδικτυακής εφαρμογής και να επιτυγχάνεται αποτελεσματικότερα ο στόχος της προστασίας της. Τέλος, το κεφάλαιο αυτό παρουσιάζει και ορίζει τις συνηθέστερες κατηγορίες διαμόρφωσης εξυπηρετητή, ανάλογα με τις προσφερόμενες υπηρεσίες του και τις κατηγορίες ευπαθειών μιας διαδικτυακής εφαρμογής.

Σε αυτό το μάθημα θα δούμε

- Παράγοντες Ασφάλειας
- Παράγοντες Επιθέσεων
  - Μεθοδολογία επίθεσης
  - Απειλές
- Ασφαλής Σχεδιασμός Διαδικτυακών Εφαρμογών
  - Επικύρωση δεδομένων εισόδου
  - Αυθεντικοποίηση
  - Εξουσιοδότηση
  - Διαχείριση ρυθμίσεων
  - Προστασία ευαίσθητων δεδομένων
  - Διαχείριση συνόδου
  - Χρήση κρυπτογραφίας
  - Αλλοίωση παραμέτρων
  - Διαχείριση εξαιρέσεων
  - Έλεγχος και καταγραφή

Όταν σκεφτόμαστε ασφάλεια διαδικτυακών εφαρμογών, τι σκεφτόμαστε;

Η αναφορά σε ζητήματα ασφάλειας διαδικτυακών εφαρμογών, φέρνει στο μυαλό μας εικόνες επιτιθέμενων σε ιστότοπους, οι οποίοι «αρπάζουν» στοιχεία πιστωτικών καρτών ή εκτελούν επιθέσεις άρνησης εξυπηρέτησης (denial of service).
Ωστόσο, αυτό είναι μόνο ένα μέρος του συνολικότερου προβλήματος, το οποίο καλούμαστε να αντιμετωπίσουμε όταν επιθυμούμε να προστατεύσουμε μια διαδικτυακή εφαρμογή.

Firewall - SSL

Ο μηχανισμός του τείχους προστασίας (firewall), για παράδειγμα, προσφέρει προστασία περιορίζοντας την πρόσβαση σε συγκεκριμένες θύρες (ports), αλλά δεν αποτελεί μια ολοκληρωμένη λύση στο πρόβλημα της ασφάλειας.

Ομοίως, η χρήση της τεχνολογίας Secure Sockets Layer (SSL) είναι εξαιρετική για την κρυπτογραφημένη μεταφορά ευαίσθητων δεδομένων μέσω του ανασφαλούς Διαδικτύου, αλλά δε μας προστατεύει εκτελώντας και επικύρωση αυτών των δεδομένων στο πλαίσιο της λειτουργίας μιας διαδικτυακής εφαρμογής.

Μπορούμε να ομαδοποιήσουμε τα απαραίτητα χαρακτηριστικά ασφάλειας μιας διαδικτυακής εφαρμογής σε διαδικασίες όπως:

- Εμπιστευτικότητα
- Ακεραιότητα
- Διαθεσιμότητα
- Αυθεντικοποίηση
- Εξουσιοδότηση
- Αδυναμία Αποποίησης

Παράγοντες Ασφάλειας

Για την ανάπτυξη μιας ασφαλούς διαδικτυακής εφαρμογής, προτείνεται η υιοθέτηση μιας ολιστικής προσέγγισης ασφάλειας, σε συνδυασμό με την πιστή εφαρμογή αρχών, κανόνων και πρακτικών ασφάλειας σε τρία επίπεδα:

- Επίπεδο δικτύου.
- Επίπεδο υπολογιστικού συστήματος.
- Επίπεδο εφαρμογής.

Ολιστική προσέγγιση ασφάλειας

Ασφαλής Υποδομή Δικτύου

- Δρομολογητές (routers)
- Τείχη Προστασίας (Firewalls)
- Μεταγωγείς (Switches)

- Προστασία σε επίπεδο Πρωτοκόλλων

Για την προστασία ενός υπολογιστικού συστήματος μπορούν να χρησιμοποιηθούν διαφορετικές τεχνικές και αντίμετρα, ανάλογα με το ρόλο και τις υπηρεσίες που προσφέρει.
Τέτοιοι ρόλοι είναι

- ο εξυπηρετητής ιστού (web server),
- ο εξυπηρετητής εφαρμογών (application server) και
- ο εξυπηρετητής βάσεων δεδομένων (database server).

Σημεία τα οποία θα πρέπει να εξετάζονται προσεκτικά σε όλους τους τύπους εξυπηρετητών, είναι τα παρακάτω:

Αναβαθμίσεις και ανανεώσεις λογισμικού	Πολλές ευπάθειες αντιμετωπίζονται με την αναβάθμιση του λογισμικού το οποίο έχουμε εγκαταστήσει στον εξυπηρετητή μας. Το πρώτο και ευκολότερο βήμα για την προστασία ενός εξυπηρετητή είναι η πιστή εφαρμογή μιας διαδικασίας εγκατάστασης ενημερωμένων εκδόσεων του λογισμικού που χρησιμοποιείται.
Υπηρεσίες	Το σύνολο των προσφερόμενων υπηρεσιών καθορίζεται από το ρόλο του εξυπηρετητή και τις εφαρμογές που φιλοξενεί. Με την απενεργοποίηση περιττών και σπάνια χρησιμοποιούμενων υπηρεσιών, μειώνεται η «επιφάνεια επίθεσης».
Δικτυακές Συνδέσεις	Για τη μείωση της «επιφάνειας επίθεσης» είναι απαραίτητη η απενεργοποίηση όλων των περιττών ή αχρησιμοποίητων συνδέσεων δικτύου.
Λογαριασμοί Χρηστών	Ο αριθμός των λογαριασμών που έχουν πρόσβαση σε ένα εξυπηρετητή θα πρέπει να περιορίζεται στο ελάχιστο επίπεδο. Επιπλέον, θα πρέπει να εφαρμόζονται κατάλληλες πολιτικές λογαριασμού, όπως πολιτική ορθής χρήσης, ισχυρού συνθηματικού κλπ.
Αρχεία και Κατάλογοι	Η πρόσβαση στα αρχεία και τους καταλόγους θα πρέπει να περιορίζεται στη βάση καθορισμένων δικαιωμάτων πρόσβασης που επιβάλλονται από το σύστημα αρχείων του εξυπηρετητή, ώστε να επιτρέπεται η πρόσβαση μόνο στους απαραίτητους λογαριασμούς υπηρεσιών και χρηστών, σύμφωνα με την Αρχή του Ελάχιστου Προνομίου.
Διαμοιρασμοί	Όλοι οι κατάλογοι οι οποίοι διαμοιράζονται, ενώ δεν είναι απαραίτητοι, θα πρέπει να αφαιρεθούν από το σύστημα αρχείων του εξυπηρετητή.
Θύρες	Υπηρεσίες οι οποίες εκτελούνται σε έναν εξυπηρετητή, χρησιμοποιούν συγκεκριμένες θύρες για να δέχονται τα εισερχόμενα αιτήματα. Οι ανοιχτές θύρες σε ένα διακομιστή, πρέπει να είναι γνωστές και να ελέγχονται τακτικά για να διασφαλίζεται ότι δεν είναι ενεργές και διαθέσιμες για επικοινωνία υπηρεσίες που δεν παρέχουν ικανό επίπεδο ασφαλούς λειτουργίας.
Έλεγχος και Καταγραφή	Η Ελεγκτική (auditing) είναι μια σημαντική βοήθεια για τον εντοπισμό εισβολών ή ακόμη και επιθέσεων σε εξέλιξη. Η Καταγραφή (logging) αποδεικνύεται ιδιαίτερα χρήσιμη κατά τη συλλογή στοιχείων που μπορούν να αξιοποιηθούν κατάλληλα στο πλαίσιο μιας ανάλυσης εγκληματολογικών ευρημάτων (forensics) με σκοπό την διαλεύκανση του τρόπου επιτυχούς πραγματοποίησης μιας εισβολής και των συνεπειών που προκάλεσε στον εξυπηρετητή.

Ορισμένες κατηγορίες ευπαθειών μιας διαδικτυακής εφαρμογής εμπίπτουν στις κατηγορίες παρουσιάζονται

Επικύρωση Δεδομένων Εισόδου	Η επικύρωση των δεδομένων εισόδου αναφέρεται στον τρόπο με τον οποίο η εφαρμογή μας φιλτράρει και είτε αποδέχεται είτε απορρίπτει δεδομένα εισόδου, πριν χρησιμοποιηθούν σε επόμενες λειτουργίες.

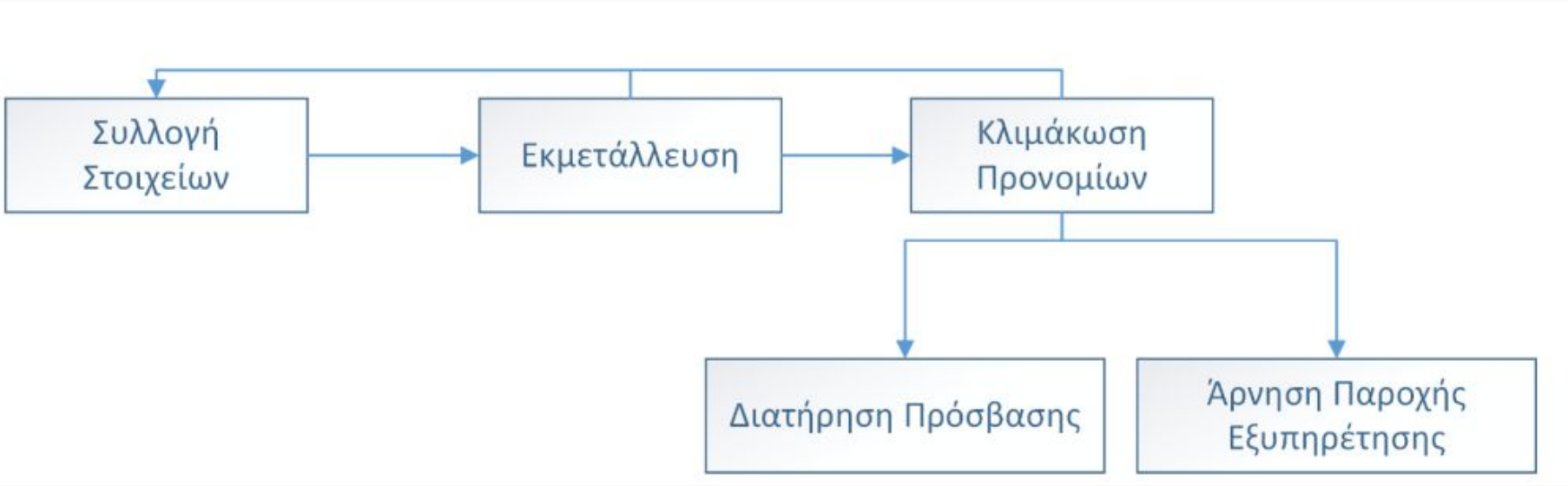
Αυθεντικοποίηση	Αυθεντικοποίηση είναι η διαδικασία κατά την οποία μια οντότητα αποδεικνύει την ταυτότητά της, συνήθως μέσω διαπιστευτηρίων (credentials), όπως όνομα χρήστη (username) και συνθηματικό (password).
Εξουσιοδότηση	Εξουσιοδότηση είναι το η διαδικασία αντιπαραβολής των χορηγημένων δικαιωμάτων πρόσβασης έναντι συγκεκριμένου αιτήματος πρόσβασης σε αντικείμενα της εφαρμογής.
Διαχείριση Αρχείων Ρυθμίσεων	Αφορά στη διαφύλαξη των ιδιοτήτων ασφάλειας των αρχείων ρυθμίσεων (configuration files) της εφαρμογής (π.χ. ρυθμίσεις σύνδεσης με τη βάση δεδομένων κ.ά.)
Ευαίσθητα Δεδομένα	Αναφέρεται στο τρόπο με τον οποίο η εφαρμογή χειρίζεται τα ευαίσθητα δεδομένα κατά την επεξεργασία, αποθήκευση και μετάδοσή τους.
Διαχείριση Συνόδου	Μια σύνοδος (session) αναφέρεται σε μια αλληλουχία σχετικών αλληλεπιδράσεων μεταξύ χρήστη και εφαρμογής. Η διαχείριση της συνόδου αναφέρεται στον τρόπο με τον οποίο η εφαρμογή χειρίζεται και προστατεύει αυτές τις αλληλεπιδράσεις.
Κρυπτογραφία	Η αξιοποίηση κρυπτογραφικών τεχνικών από την εφαρμογή για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.
Διαχείριση Παραμέτρων	Η διαχείριση παραμέτρων αφορά τόσο τον τρόπο διασφάλισης από την εφαρμογή της προστασίας των τιμών των παραμέτρων από πιθανές αλλοιώσεις, όσο και τον τρόπο με τον οποίο τις χειρίζεται.
Διαχείριση Εξαιρέσεων	Όταν μια κλήση μεθόδου αποτύχει, πρέπει η εφαρμογή να παρέχει προστασία των πληροφοριών εξαίρεσης που επιστρέφονται.

Παράγοντες Επιθέσεων

Μεθοδολογία επίθεσης

Η κατανόηση μιας τυπικής μεθοδολογίας που χρησιμοποιείται από τους επιτιθέμενους κατά τη διάρκεια μιας επίθεσης σε μια διαδικτυακή εφαρμογή, μας δίνει αρκετά από τα απαραίτητα εφόδια γνώσης, ώστε να λάβουμε κατάλληλα μέτρα προστασίας (είτε αμυντικού είτε ακόμη και επιθετικού χαρακτήρα).

Μεθοδολογία επίθεσης.



Απειλές

Τα είδη απειλών για μια διαδικτυακή εφαρμογή μπορούν να ταξινομηθούν στις παρακάτω κατηγορίες:

- Πλαστογράφηση
- Αλλοίωση
- Αποποίηση
- Δημοσιοποίηση πληροφοριών
- Άρνηση παροχής εξυπηρέτησης
- Κλιμάκωση δικαιωμάτων

Μέθοδοι αντιμετώπισης απειλών και αντίμετρα

ΑΠΕΙΛΗ	ΑΝΤΙΜΕΤΡΟ
Πλαστογράφηση	Χρήση ισχυρών μηχανισμών ελέγχου ταυτότητας. Αποφυγή αποθήκευσης μυστικών (για παράδειγμα, διαπιστευτηρίων) μέσα σε απλό κείμενο. Αποφυγή μετάδοσης διαπιστευτηρίων σύνδεσης σε μορφή απλού κειμένου μέσω απροστάτευτης δικτυακής σύνδεσης.
Αλλοίωση	Αξιοποίηση μηχανισμών συναρτήσεων κατακερματισμού. Χρήση ψηφιακών υπογραφών. Χρήση ισχυρών μηχανισμών αυθεντικοποίησης. Χρήση πρωτοκόλλων που παρέχουν προστασία της ακεραιότητας του κάθε μεταδιδόμενου μηνύματος.
Αποποίηση	Τήρηση και προστασία αρχείων καταγραφής. Χρήση ψηφιακών υπογραφών.
Δημοσιοποίηση πληροφοριών	Χρήση ισχυρών μηχανισμών αυθεντικοποίησης. Χρήση ανθεκτικής κρυπτογράφησης. Χρήση πρωτοκόλλων που παρέχουν προστασία της εμπιστευτικότητας των μεταδιδόμενων μηνυμάτων. Αποφυγή αποθήκευσης μυστικών μέσα σε απλό κείμενο.
Άρνηση εξυπηρέτησης	Παρακολούθηση, διαχείριση και ρύθμιση της χρήσης των πόρων του υπολογιστικού συστήματος. Επικύρωση και φιλτράρισμα των δεδομένων εισόδου.
Κλιμάκωση προνομίων	Εφαρμογή της Αρχής του Ελάχιστου Προνομίου. Χρήση επαρκών λογαριασμών για την εκτέλεση των διεργασιών και την πρόσβαση στους πόρους.

Συσχετισμός ευπαθειών και απειλών.

ΕΥΠΑΘΕΙΑ	ΑΠΕΙΛΗ
Επικύρωση δεδομένων εισόδου	Υπερχείλιση ενταμιευτήρα. Ενδεχόμενο επίθεσης XSS. Ψεκασμός SQL εντολών
Αυθεντικοποίηση	Ενδεχόμενο επίθεσης ωμής βίας (brute force) Ενδεχόμενο επίθεσης λεξικού (dictionary) Επανάληψη ψηφιακού μπισκότου (cookie replay). Αλλοίωση δεδομένων.
Εξουσιοδότηση	Κλιμάκωση προνομίων. Δημοσιοποίηση πληροφοριών. Αλλοίωση δεδομένων.
Διαχείριση αρχείων ρυθμίσεων	Μη εξουσιοδοτημένη πρόσβαση σε εργαλεία διαχειριστικού ελέγχου. Μη εξουσιοδοτημένη χρήση λογαριασμών με υψηλά προνόμια.
Ευαίσθητα δεδομένα	Πρόσβαση σε αποθηκευμένα δεδομένα. Παρακολούθηση δικτυακής κίνησης. Αλλοίωση δεδομένων.
Διαχείριση Συνόδου	Υφαρπαγή συνόδου. Επανάληψη συνόδου. Ενδεχόμενο επίθεσης του ενδιάμεσου (MITM).
Κρυπτογραφία	Αδύναμοι μηχανισμοί κρυπτογραφίας. Κακή διαχείριση κλειδιών.\ Παραγωγή αδύναμων κλειδιών
Διαχείριση παραμέτρων	Διαχείριση αλφαριθμητικών ερωτημάτων SQL. Διαχείριση δεδομένων εισόδου σε φόρμες εισαγωγής στοιχείων. Διαχείριση ψηφιακών μπισκότων (cookies) και κεφαλίδων HTTP.
Διαχείριση εξαιρέσεων	Δημοσιοποίηση πληροφοριών. Αποποίηση.
Έλεγχος και Καταγραφή	Αποποίηση. Κάλυψη ιχνών επίθεσης.

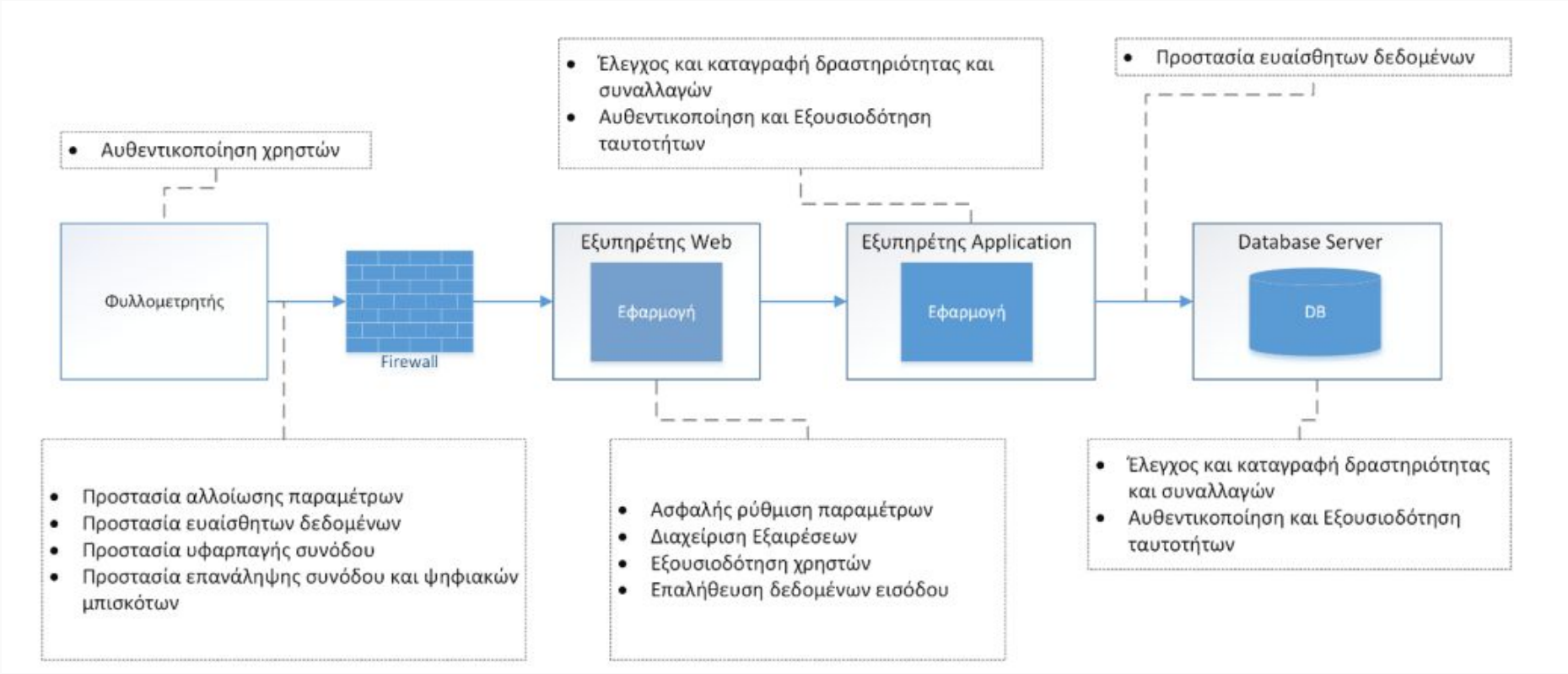
Ασφαλής Σχεδιασμός Διαδικτυακών Εφαρμογών

Η διαδικασία ασφαλούς ανάπτυξης διαδικτυακών εφαρμογών παρουσιάζει σημαντικές προκλήσεις για τους σχεδιαστές και τους προγραμματιστές.

Δεδομένου ότι συνήθως οι επόμενες αποφάσεις εξουσιοδότησης λαμβάνονται με βάση την ταυτότητα του χρήστη, είναι σημαντικό η διαδικασία αυθεντικοποίησης να είναι προστατευμένη και ο μηχανισμός χειρισμού της συνόδου που χρησιμοποιείται για την παρακολούθηση εξουσιοδοτημένων χρηστών να είναι εξίσου καλά προστατευμένος.

Ο σχεδιασμός ασφαλών μηχανισμών αυθεντικοποίησης και διαχείρισης συνόδου είναι μόνο μερικά από τα ζητήματα που αντιμετωπίζουν οι σχεδιαστές και οι προγραμματιστές διαδικτυακών εφαρμογών.

Επιμέρους ζητήματα ασφάλειας διαδικτυακής εφαρμογής



Επικύρωση δεδομένων εισόδου

Η σωστή επικύρωση των δεδομένων εισόδου είναι ένα από τα ισχυρότερα μέτρα άμυνας κατά των επιθέσεων σε μια διαδικτυακή εφαρμογή. Ο προγραμματιστής μιας διαδικτυακής εφαρμογής επιφορτίζεται με την ευθύνη της δημιουργίας της πρώτης γραμμής άμυνας, όπου με τη χρήση κατάλληλων αντιμέτρων πρέπει να βοηθήσει στην πρόληψη επιθέσεων XSS, ψεκασμού εντολών SQL, υπερχείλισης ενταμιευτήρα κ.ά.
Για το σκοπό αυτό:

- Υποθέτουμε ότι όλες οι είσοδοι προέρχονται από μη αξιόπιστη πηγή.
- Χρησιμοποιούμε έναν εξυπηρετητή αυθεντικοποίησης.
- Φιλτράρουμε, περιορίζουμε και απορρίπτουμε όλες τις εισόδους.

Αυθεντικοποίηση

Τρεις πτυχές που πρέπει να εξετάζονται, είναι οι εξής:

- Εντοπισμός των σημείων της εφαρμογής όπου απαιτείται έλεγχος ταυτότητας. Αυτό, συνήθως, συμβαίνει σε σημεία όπου χρειάζεται να ξεπεραστεί ένα όριο εμπιστοσύνης.
- Επαλήθευση της ταυτότητας του χρήστη που εκτελεί μια κλήση. Αυτό, συνήθως, γίνεται με χρήση ζεύγους username και password.
- Προσδιορισμός της ταυτότητας του χρήστη σε επόμενες κλήσεις. Αυτό απαιτεί κάποια μορφή χρήσης token για παρουσίαση της ελεγμένης ταυτότητας.

Οι πρακτικές που ακολουθούνται για την αντιμετώπιση των ζητημάτων αυθεντικοποίησης

- Διαχωρισμός δημόσιων και περιορισμένων (ιδιωτικών) ζωνών χρήσης της εφαρμογής.
- Χρήση πολιτικών αποκλεισμού για τους λογαριασμούς των τελικών χρηστών.
- Υποστήριξη περιόδου λήξης του κάθε συνθηματικού.
- Δυνατότητα άμεσης απενεργοποίησης λογαριασμών.
- Να μην αποθηκεύονται συνθηματικά σε αποθηκευτικό χώρο του τελικού χρήστη.
- Να απαιτείται η χρήση ισχυρών συνθηματικών.
- Να μη μεταδίδονται απροστάτευτα συνθηματικά μέσω του δικτύου.
- Να προστατεύονται τα ψηφιακά μπισκότα (cookies) ταυτότητας.

Εξουσιοδότηση

Η εξουσιοδότηση καθορίζει τις ενέργειες που μπορεί να εκτελέσει μια οντότητα, η οποία έχει επαληθεύσει την ταυτότητά της. Μια λανθασμένη εξουσιοδότηση μπορεί να οδηγήσει σε αποκάλυψη πληροφοριών και σε αλλοίωση δεδομένων.
Οι συνηθέστερες πρακτικές που ακολουθούνται για ζητήματα εξουσιοδότησης είναι :

- Χρήση πολλαπλών ελέγχων εξουσιοδότησης.
- Περιορισμός των δικαιωμάτων του χρήστη.
- Χρήση επιπέδων εξουσιοδότησης.

Διαχείριση ρυθμίσεων

Οι συνηθέστερες πρακτικές που ακολουθούνται για ζητήματα διαχείρισης των ρυθμίσεων είναι:

- Διασφάλιση της ελεγχόμενης πρόσβασης στις διεπαφές διαχείρισης.
- Προστασία του χώρου όπου αποθηκεύονται οι ρυθμίσεις.
- Ανάπτυξη διαφορετικών επιπέδων διαχείρισης για κάθε ρόλο / χρήστη.
- Χρήση λογαριασμών με ελάχιστα δικαιώματα για κάθε ξεχωριστή υπηρεσία.

Προστασία ευαίσθητων δεδομένων

Πρακτικές που ακολουθούνται για την προστασία των ευαίσθητων δεδομένων είναι, συνήθως, οι παρακάτω:

- Αποθήκευση μόνο των ευαίσθητων δεδομένων που είναι απαραίτητα για την εκάστοτε λειτουργία της εφαρμογής.
- Αποφυγή αποθήκευσης ευαίσθητων δεδομένων μέσα στον κώδικα της εφαρμογής.
- Κρυπτογραφημένη αποθήκευση των ρυθμίσεων σύνδεσης σε συστήματα διαχείρισης
- βάσεων δεδομένων, συνθηματικών, κλειδιών κρυπτογράφησης κλπ.
- Εκτεταμένη χρήση κρυπτογραφικών τεχνικών.

Διαχείριση συνόδου

Οι ακόλουθες πρακτικές βελτιώνουν την ασφάλεια της διαχείρισης συνόδου μιας διαδικτυακής εφαρμογής:

- Εφαρμογή πρωτοκόλλου SSL για την προστασία των μεταδιδόμενων δεδομένων.
- Κρυπτογράφηση των ψηφιακών μπισκότων αυθεντικοποίησης.
- Περιορισμός χρόνου ζωής μιας ενεργής συνόδου.
- Προστασία από το ενδεχόμενο υφαρπαγής κατάστασης μιας συνόδου από μη εξουσιοδοτημένους χρήστες.

Χρήση κρυπτογραφίας

Οι διαδικτυακές εφαρμογές συχνά χρησιμοποιούν κρυπτογραφικές μεθόδους για να προστατεύσουν τα δεδομένα κατά την αποθήκευση ή τη μετάδοσή τους. Οι ακόλουθες πρακτικές βελτιώνουν την ασφάλεια των διαδικτυακών εφαρμογών όταν χρησιμοποιούμε κρυπτογραφία:

- Δεν χρησιμοποιούμε δικές μας μεθόδους κρυπτογράφησής αλλά προτιμούμε έτοιμες ολοκληρωμένες και δοκιμασμένες λύσεις.
- Χρησιμοποιούμε το σωστό αλγόριθμο και με το κατάλληλο μήκος κλειδιού, εφόσον
  υποστηρίζεται μεταβλητό μήκος.
- Προστατεύουμε επαρκώς τα κρυπτογραφικά κλειδιά.

Αλλοίωση παραμέτρων

Με τις επιθέσεις χειραγώγησης παραμέτρων ο εισβολέας αποσκοπεί στο να τροποποιεί τα δεδομένα που αποστέλλονται μεταξύ του χρήστη και της διαδικτυακής εφαρμογής. Αυτά τα δεδομένα μπορεί να είναι αλφαριθμητικά ερωτήματος, πεδία φόρμας, cookies, ή κεφαλίδες HTTP κ.ά. Οι ακόλουθες πρακτικές προστατεύουν τη χειραγώγηση παραμέτρων μιας διαδικτυακής εφαρμογής:

- Κρυπτογράφηση ψηφιακών μπισκότων κατάστασης.
- Επικύρωση των δεδομένων εισόδου.
- Προσεκτικός έλεγχος των κεφαλίδες HTTP.

Διαχείριση εξαιρέσεων

Μια καλή προσέγγιση είναι να σχεδιαστεί μια κεντρική λύση διαχείρισης εξαιρέσεων και καταγραφής τους, έτσι ώστε να υποστηριχθεί αποτελεσματικά η εργασία των διαχειριστών του συστήματος. Οι ακόλουθες πρακτικές βοηθούν στη διασφάλιση του σωστού χειρισμού εξαιρέσεων από μια διαδικτυακή εφαρμογή:

- Δεν επιτρέπουμε την επιστροφή κρίσιμων πληροφοριών στον χρήστη.
- Καταγράφουμε λεπτομερώς τα μηνύματα λάθους.
- Υπάρχει χειρισμός για όλες τις εξαιρέσεις.

Έλεγχος και καταγραφή

Οι ακόλουθες πρακτικές βελτιώνουν τη διαδικασία ελέγχου και καταγραφής:

- Έλεγχος και καταγραφή σε όλα τα επίπεδα λειτουργίας της εφαρμογής μας.
- Λεπτομερής καταγραφή κύριων συμβάντων.
- Διασφάλιση και προστασία των αρχείων καταγραφής.
- Περιοδική δημιουργία αντιγράφων και ανάλυση των αρχείων καταγραφής.