ΓΙΑ ΑΜΕΣΗ ΑΝΑΚΟΙΝΩΣΗ:

ΚΥΚΛΟΦΟΡΗΣΕ ΤΟ OWASP TOP 10 ΓΙΑ ΤΟ 2010

Θα μας βοηθήσετε να πλησιάσουμε όλους όσους αναπτύσσουν λογισμικό;

Κολούμπια, 19/4/2010 —

Από το 2003 ερευνητές και ειδικοί της ασφάλειας λογισμικού εφαρμογών από όλο τον κόσμο παρακολουθούν προσεκτικά μέσα από το Open Web Application Security Project (OWASP) την κατάσταση της ασφάλειας των διαδικτυακών εφαρμογών και δημοσιεύουν ένα κείμενο ευαισθητοποίησης που αποτελεί πλέον πρότυπο στο οποίο βασίζονται διεθνείς οργανισμοί όπως οι PCI, DOD, FTC, και πολλοί ακόμα.

Σήμερα, το OWASP δημοσιεύει μια ενημερωμένη έκθεση που αποτυπώνει τους δέκα σημαντικότερους κινδύνους που σχετίζονται με τη χρήση διαδικτυακών εφαρμογών σε έναν οργανισμό. Η έκθεση αυτή είναι γεμάτη με παραδείγματα και αναλύσεις που εξηγούν τους κινδύνους αυτούς σε όσους αναπτύσσουν λογισμικό, σε επικεφαλείς ομάδων ανάπτυξης και οργανισμών και γενικότερα, σε όσους ενδιαφέρονται για το μέλλον της ασφάλειας στο διαδίκτυο. Ότι παράγεται από το OWASP είναι δωρεάν και ανοικτό σε οποιονδήποτε. Έτσι, μπορείτε να κατεβάσετε το τελευταίο OWASP Top 10 δωρεάν από το:

http://www.owasp.org/index.php/Top_10

Ο Dave Wichers, μέλος του διοικητικού συμβουλίου του OWASP και COO της Aspect Security, είναι υπεύθυνος του συγκεκριμένου έργου από τη στιγμή της σύλληψής του. «Φέτος έχουμε ανανεώσει το Top 10 ώστε να είναι ξεκάθαρο ότι μιλάμε για κινδύνους και όχι απλά ευπάθειες. Δεν έχει νόημα να κατηγοριοποιούμε ως προς τη σημασία τους τις ευπάθειες χωρίς να γνωρίζουμε το γενικότερο περιβάλλον. Δεν μπορούμε να λάβουμε σωστές επιχειρηματικές αποφάσεις αν δεν κατανοούμε τους κινδύνους και τις επιπτώσεις στην επιχείρησή μας.» Αυτή η νέα στόχευση στους κινδύνους αποσκοπεί στο να κατευθύνει τους οργανισμούς σε μια πιο ώριμη θεώρηση και διαχείριση της ασφάλειας εφαρμογών.

Έχει έρθει η στιγμή να ευαισθητοποιήσουμε ως προς την ασφάλεια εφαρμογών όχι μόνο όσους ασχολούνται με την ασφάλεια αλλά απευθείας όσους έχουν μεγαλύτερη ανάγκη να γνωρίζουν για αυτή. Φέτος, στόχος μας είναι η ενημέρωση **κάθε προγραμματιστή στον κόσμο** για το OWASP Top 10. Αλλά χρειαζόμαστε τη βοήθειά σας. Όσοι διαβάζετε το κείμενο αυτό, είστε διατεθειμένοι να κάνετε ένα απλό πράγμα για να βοηθήσετε στην προστασία του Internet; Αν γνωρίζετε ανθρώπους που γράφουν κώδικα, προωθήστε τους το OWASP Top 10 και ρωτήστε τους…

Γνωρίζετε όλους τους κινδύνους που περιγράφονται στο OWASP Top 10;

Δεσμεύεστε σήμερα να προστατεύσετε τον κώδικά σας απέναντι στους κινδύνους του OWASP Top 10;

Για πολύ καιρό οι οργανισμοί βασίζονται αποκλειστικά σε περιστασιακούς ελέγχους ή δοκιμές παρείσδυσης για τη διασφάλιση των εσωτερικών και εξωτερικών εφαρμογών διαδικτύου που χρησιμοποιούν. Η προσέγγιση αυτή έχει υψηλό κόστος και δεν παρέχει πολλές πληροφορίες σχετικά με την αντιμετώπιση των κινδύνων. Όπως και για άλλους τομείς της ασφάλειας, έτσι και για την ασφάλεια λογισμικού εφαρμογών απαιτείται ένα πρόγραμμα

διαχείρισης επικινδυνότητα που παρέχει πληροφορίες για όλο το πορτφόλιο εφαρμογών και τα στρατηγικά μέτρα ελέγχου που στοχεύουν στη βελτίωση της ασφάλειας. Αν ο οργανισμός σας είναι έτοιμος να αντιμετώπιση την ασφάλεια εφαρμογών υπάρχουν δεκάδες δωρεάν βιβλία, εργαλεία, έργα, φόρουμ, λίστες ηλεκτρονικού ταχυδρομείου κ.α. στο OWASP. Μπορείτε επίσης να συμμετάσχετε σε μια από τις 180 τοπικές ομάδες εργασίες ή να παρακολουθήσετε ένα από τα υψηλού επιπέδου αλλά χαμηλού κόστους συνέδρια AppSec.

Το OWASP Top 10 για το 2010 είναι:

A1: Έγχυση (Injection)
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Ανασφαλής Απευθείας Αναφορά σε Αντικείμενα (Insecure Direct Object References)
A5: Πλαστογράφηση αίτησης μεταξύ θέσεων (Cross-Site Request Forgery - CSRF)
A6: Λανθασμένες Ρυθμίσεις Ασφάλειας (Security Misconfiguration)
A7: Ανασφαλής Κρυπτογραφική Αποθήκευση (Insecure Cryptographic Storage)
A8: Αποτυχία Περιορισμού της Πρόσβασης URL (Failure to Restrict URL Access)
A9: Ανεπαρκής Προστασία Επιπέδου Μεταφοράς (Insufficient Transport Layer Protection)
A10: Μη Επαληθευμένες Αναδρομολογήσεις και Προωθήσεις (Unvalidated Redirects and Forwards)

Η ενημερωμένη έκδοση του 2010 βασίζεται σε περισσότερες πηγές πληροφόρησης για ευπάθειες διαδικτυακών εφαρμογών σε σχέση με την προηγούμενη. Επιπλέον παρουσιάζει τις πληροφορίες με πιο συνοπτικό και συναρπαστικό τρόπο, ώστε να μπορούν εύκολα να τεθούν σε εφαρμογή αφού περιλαμβάνουν πολλές αναφορές σε νέο, πλούσιο υλικό που μπορεί να χρησιμοποιηθεί για να αντιμετωπίσει το κάθε θέμα, όπως το νέο Enterprise Security API (ESAPI) του OWASP και το Πρότυπο Ελέγχου Ασφάλειας Εφαρμογών (Application Security Verification Standard - ASVS).

ΣΧΕΤΙΚΑ ΜΕ ΤΟ OWASP

Το Open Web Application Security Project (OWASP) είναι μια παγκόσμια, ανοικτή κοινότητα που εστιάζει τη βελτίωση της ασφάλειας το λογισμικού εφαρμογών. Στόχος μας είναι η ευαισθητοποίηση ως προς την ασφάλεια εφαρμογών, ώστε άνθρωποι και οργανισμοί να λαμβάνουν σωστές αποφάσεις για τους πραγματικούς κινδύνους για την ασφάλεια εφαρμογών. Η συμμετοχή στο OWASP είναι ελεύθερη και **όλο το υλικό** είναι διαθέσιμο κάτω από άδεια ελεύθερου και ανοικτού λογισμικού. Το OWASP είναι ένας μη κερδοσκοπικός οργανισμός που διασφαλίζει την διαρκή διαθεσιμότητα και υποστήριξη των έργων. Μέλη του είναι: Ιδιώτες, Οργανισμοί και Πανεπιστήμια.

Συνεντεύξεις: Jeff Williams – Πρόεδρος του OWASP και Ιδρυτής του Top 10 Project (jeff.williams@owasp.,org)
Συνεντεύξεις: Dave Wichers – Μέλος Δ.Σ. OWASP και Επικεφαλής του Top 10 Project (dave.wichers@owasp.org)
Επικοινωνία: Lorna Alamri – Επιτροπή Διασυνδέσεων (lorna.alamri@owasp.org)
Συντονιστής Ελληνικής Ομάδας Εργασίας: Κωνσταντίνος Παπαπαναγιώτου (conpap@owasp.gr)
Επωνυμία: Open Web Application Security Project (OWASP)
Διαδικτυακή Διεύθυνση: http://www.owasp.org
Διαδικτυακή Διεύθυνση Ελληνικής Ομάδας Εργασίας: http://www.owasp.gr – http://blog.owasp.gr

# # #