OWASP
The Open Web Application Security Project

OWASP Training Day

OWASP Projects and Resources you can use TODAY

25 Μαΐου 2011

Αμφιθέατρο Γενικής Γραμματείας Πληροφοριακών Συστημάτων,
Χανδρή 1 & Θεσσαλονίκης, Μοσχάτο, Αθήνα
(Σταθμός ΗΣΑΠ Καλλιθέα)

https://www.owasp.org/index.php/Greece/Training/OWASP_projects_and_resources_you_can_use_TODAY

Το **OWASP** (http://www.owasp.org) είναι ένας διεθνής, μη κερδοσκοπικός οργανισμός, που βασίζεται στη φιλοσοφία του ανοιχτού λογισμικού, στοχεύοντας στον εντοπισμό και στην καταπολέμηση των τρωτών σημείων του λογισμικού εφαρμογών. Πρόκειται για μια ανοικτή κοινότητα αφιερωμένη στην ενημέρωση ανθρώπων και οργανισμών για το πώς μπορούν να αναπτύξουν, να προμηθευθούν και να συντηρήσουν ασφαλείς εφαρμογές.

Αν εξαιρέσουμε το OWASP Top10, τα περισσότερα projects του **OWASP** δεν είναι ευρέως γνωστά. Παρόλο που πρόκειται για εύχρηστα, επαγγελματικού επιπέδου εργαλεία και μεθοδολογίες που παρέχονται δωρεάν υπό τη μορφή ανοικτού λογισμικού, εντούτοις συχνά δεν είναι κατανοητό πώς μπορούν να ενσωματωθούν στον Κύκλο Ζωής Ανάπτυξης Λογισμικού ή γενικότερα στο συνολικό οικοσύστημα ασφάλειας ενός οργανισμού.

Το **OWASP Training Day** στοχεύει στην παρουσίαση ώριμων projects του OWASP, τα οποία χρησιμοποιούνται ήδη από οργανισμούς σε παγκόσμιο επίπεδο. Πρόκειται για μια **υψηλού επιπέδου ημερίδα εκπαίδευσης** σε εργαλεία και μεθοδολογίες που σχετίζονται με την ασφαλή ανάπτυξη λογισμικού που **απευθύνεται σε προγραμματιστές, designers, architects, project managers** αλλά **και ειδικούς ασφάλειας**. Πέρα από τις παρουσιάσεις, θα πραγματοποιηθούν και πρακτικά παραδείγματα χρήσης των εργαλείων, ενώ στόχος μας είναι η ενθάρρυνση συζητήσεων και ανταλλαγής απόψεων, όχι μόνο γύρω από τη χρήση των έργων του OWASP, αλλά και γενικά για την ασφάλεια εφαρμογών στην Ελλάδα.

Δηλώστε συμμετοχή στο OWASP Training Day:

http://www.regonline.com/Register/Checkin.aspx?EventID=967109

Η συμμετοχή στο **OWASP Training Day** είναι **δωρεάν για τα μέλη του OWASP**.
Το κόστος της ετήσιας συνδρομής στο OWASP ανέρχεται στα $50 (35 €).

Λόγω περιορισμένου αριθμού θέσεων απαιτείται δήλωση συμμετοχής, αφού προηγηθεί εγγραφή στο **OWASP**, ακολουθώντας το σύνδεσμο: http://www.regonline.com/owasp_membership

ΠΡΟΓΡΑΜΜΑ

9:30 - 10:15	Guided tour of OWASP Projects — Dinis Cruz Τα OWASP Projects αντικατοπτρίζουν το βασικότερο έργο του OWASP. Παρέχουν εργαλεία και μεθοδολογίες ασφάλειας για όλες τις πλατφόρμες ανάπτυξης (J2EE, .NET, Cold Fusion, IIS, WebSphere, Tomcat, κλπ.) τα οποία είναι ανοικτά και ελεύθερα προσβάσιμα από όλους.
10:15 – 11:15	OWASP Top 10 — Konstantinos Papapanagiotou Το OWASP Top10 περιγράφει τους 10 σημαντικότερους κινδύνους για την ασφάλεια των web εφαρμογών. Στόχος του είναι να ενημερώσει όλους όσους εμπλέκονται στην ανάπτυξη λογισμικού: developers, designers, architects, managers, αλλά και οργανισμούς, για τις συνέπειες των σημαντικότερων ευπαθειών των web εφαρμογών.
11:15 – 11:30	Διάλειμμα
11:30 – 12:30	OWASP Secure Coding Practices - Quick Reference Guide — Justin Clarke Ο οδηγός Secure Coding Practices Quick Reference Guide είναι ένα σύνολο από βέλτιστες πρακτικές ασφαλούς προγραμματισμού, που παρέχεται υπό τη μορφή checklist και μπορεί να ενσωματωθεί στον κύκλο ζωής του λογισμικού, ανεξαρτήτως γλώσσας ή τεχνολογίας προγραμματισμού, ή να χρησιμοποιηθεί σαν σημείο αναφοράς για κάθε προγραμματιστή.
12:30 – 13:30	OWASP AppSensor Project — Colin Watson Το AppSensor είναι ένα framework το οποίο συνδυάζει μεθοδολογίες και εργαλεία για την υλοποίηση ενός ολοκληρωμένου συστήματος ανίχνευσης εισβολέων και αυτοματοποιημένης απόκρισης μέσα σε μία εφαρμογή. Η λογική του βασίζεται στο γεγονός ότι οι επιτιθέμενοι χρησιμοποιούν συγκεκριμένες, επαναλαμβανόμενες μεθόδους για τον εντοπισμό πιθανών ευπαθειών σε μία εφαρμογή. Στόχος του είναι να προσφέρει προστασία στην εφαρμογή εκ των έσω.
13:30 – 14:30	Διάλειμμα - Γεύμα
14:30 – 15:00	OWASP ESAPI — Justin Clarke Το ESAPI (Eneterprise Security API) είναι μία βιβλιοθήκη που μπορεί να χρησιμοποιηθεί για την προστασία από τις ευπάθειες που περιγράφονται στο OWASP Top10. Έχει υλοποιηθεί με τέτοιο τρόπο, ώστε να είναι εύκολη η ενσωμάτωσή της σε οποιαδήποτε υπάρχουσα εφαρμογή, ενώ μπορεί να χρησιμοποιηθεί και σαν βάση για νέες εφαρμογές.
15:00 – 15:30	OWASP Software Assurance Maturity Model — Colin Watson Το SAMM είναι ένα ανοικτό πλαίσιο που βοηθά στο σχεδιασμό στρατηγικής για την ασφάλεια λογισμικού. Με το SAMM ένας οργανισμός μπορεί να αποτιμήσει υπάρχουσες πρακτικές ασφαλούς ανάπτυξης λογισμικού και να υλοποιήσει στη συνέχεια ένα πρόγραμμα διασφάλισης ανάλογα με τις ανάγκες και τους στόχους του, χρησιμοποιώντας απλές, σαφώς ορισμένες και μετρήσιμες διαδικασίες.
15:30 – 16:00	OWASP Application Security Verification Standard — Konstantinos Papapanagiotou Στόχος του ASVS είναι η κανονικοποίηση των απαιτήσεων αναφορικά με τον έλεγχο της ασφάλειας των εφαρμογών. Μπορεί να χρησιμοποιηθεί σαν πρότυπο για τον καθορισμό επιπέδων εμπιστοσύνης σε μία εφαρμογή, για τον ορισμό του επιθυμητού επιπέδου ασφάλειας κατά την προμήθεια εφαρμογών ή σαν καθοδήγηση προς την ομάδα ανάπτυξης λογισμικού.

16:00 – 16:15	Διάλειμμα
16:15 – 17:15	OWASP O2 Platform Dinis Cruz Το O2 είναι μία συλλογή από Open Source modules, που στόχο έχουν να βοηθήσουν κάθε ειδικό ασφάλειας εφαρμογών να αποκτήσει γρήγορα τις απαραίτητες πληροφορίες για την ασφάλεια μιας εφαρμογής. Συγκεντρώνει τεχνολογία από διαφορετικές μηχανές στατικής ανάλυσης, με σκοπό να αυτοματοποιήσει διαδικασίες και workflows κατά την ανάλυση μιας εφαρμογής.

ΟΜΙΛΗΤΕΣ

Ο **Justin Clarke** είναι συνιδρυτής και Γενικός Διευθυντής της Gotham Digital Science στην Αγγλία. Έχει πάνω από 12 χρόνια εμπειρία στον έλεγχο ασφάλειας δικτύων, web εφαρμογών και ασύρματων δικτύων για μεγάλους πελάτες στο χρηματοπιστωτικό, τεχνολογικό, εμπορικό και κυβερνητικό τομέα. Έχει συγγράψει βιβλία όπως το “SQL Injection Attacks and Defense” (Syngress 2009), "Network Security Tools: Writing, Hacking, and Modifying Security Tools" (O’Reilly 2005), "Network Security Assessment: Know Your Network, 2nd Edition" (O’Reilly 2007) ενώ έχει παρουσιάσει σε μεγάλο αριθμό συνεδρίων όπως Black Hat USA, EuSecWest, OSCON, ISACA, RSA, SANS, OWASP, BCS. Είναι ο δημιουργός του εργαλείου SQLBrute και ο Chapter Leader του OWASP London Chapter.

Ο **Dinis Cruz** είναι ανεξάρτητος σύμβουλος ασφάλειας με εξειδίκευση στην ασφάλεια εφαρμογών για τις πλατφόρμες ASP.NET και J2EE και στον έλεγχο ασφάλειας εφαρμογών. Στο παρελθόν έχει εργαστεί ως σύμβουλος ασφάλειας προσφέροντας υπηρεσίες για μεγάλους τραπεζικούς οργανισμούς (ABN AMRO) ή διευθύνοντας ομάδες ασφάλειας και ελέγχου εφαρμογών (Ounce Labs, IBM). Παράλληλα, προσφέρει εκπαιδευτικές υπηρεσίες σε θέματα ασφάλειας εφαρμογών. Στο OWASP έχει αναπτύξει πολλές πρωτοβουλίες μέσα από έργα, αλλά και τη συμμετοχή του στο διοικητικό συμβούλιο του οργανισμού, το OWASP Global Projects Committee και το OWASP Connections Committee.

Ο **Colin Watson** είναι σύμβουλος ασφάλειας εφαρμογών και Διευθυντής Τεχνολογίας στη Watson Hall Ltd. στο Λονδίνο. Είναι μέλος του OWASP Global Industry Committee και βασικός συντελεστής στο έργο AppSensor, ενώ συνεισφέρει τακτικά και σε άλλα έργα όπως SAMM, OWASP Top10, κλπ. Έχοντας ξεκινήσει πριν από 15 χρόνια από το χώρο του σχεδιασμού και της ανάπτυξης web εφαρμογών, πλέον η ειδίκευσή του είναι στους τομείς προστασίας εφαρμογών, διαχείρισης κινδύνων web εφαρμογών, ασφαλούς κύκλου ζωής ανάπτυξης λογισμικού, ανάπτυξης πολιτικών ασφάλειας και ιδιωτικότητας σε web εφαρμογές, καθώς και ανάπτυξη μεθοδολογιών ασφαλούς προγραμματισμού.

Ο **Δρ. Κωνσταντίνος Παπαπαναγιώτου** είναι Διευθυντής Υπηρεσιών Διαχείρισης Κινδύνων στη Syntax Πληροφορική ΑΒΕΕ και συντονιστής της Ελληνικής Ομάδας Εργασίας του Open Web Application Security Project (OWASP), υπεύθυνος για την προώθηση της ασφαλούς ανάπτυξης λογισμικού στην Ελλάδα. Διαθέτει συνολικά πάνω από 7 χρόνια εμπειρίας στο χώρο της Ασφάλειας Πληροφοριών τόσο ως σύμβουλος επιχειρήσεων όσο και ως ερευνητής, ενώ είναι κάτοχος των πιστοποιήσεων CISSP και ITILv3 Foundation. Είναι συγγραφέας περισσότερων από 10 επιστημονικών δημοσιεύσεων, ενώ αρθρογραφεί τακτικά σε περιοδικά του χώρου. Επίσης, είναι μέλος των οργανισμών ACM και IEEE, καθώς και ιδρυτικό μέλος του Institute of Information Security Professionals (IISP).

ΧΟΡΗΓΟΙ

Χορηγός OWASP Training Day Greece:
Syntax Πληροφορική ΑΒΕΕ
(http://www.syntax.gr)

Ο χώρος διεξαγωγής του OWASP Training Day είναι μια ευγενική προσφορά της **Γενικής Γραμματείας Πληροφοριακών Συστημάτων**
(http://www.gsis.gr)

Διοργάνωση:
OWASP Greek Chapter
(http://www.owasp.gr)