18 Ιανουαρίου, 2010

Συνέδρια OWASP AppSec

21-24 Ιουνίου 2010
AppSec Research 2010
Στοκχόλμη

OWASP Μέλη Συμβουλίου 2010

Jeff Williams
Dinis Cruz
Dave Wichers
Tom Brennan
Sebastien Deleersnyder
Eoin Keary
Matt Tesauro

OWASP
The Open Web Application Security Project

AppSec USA 2010 Ανακοίνωση

Η Παγκόσμια Επιτροπή Συνεδρίων βρίσκεται στην ευχάριστη θέση να ανακοινώσει την ημερομηνία και την τοποθεσία διοργάνωσης του συνεδρίου OWASP AppSec US 2010. Το AppSec US 2010 θα διοργανώνεται από την Ομάδα Εργασίας του Bay Area μεταξύ 7 και 10 Σεπτεμβρίου 2010 στο University of California, Irvine, τη μόνη σχολή του Πανεπιστημίου της Καλιφόρνια με έμφαση στην Επιστήμη των Πληροφοριών και Υπολογιστών. Περισσότερες πληροφορίες σχετικά με την πρόσκληση για ομιλητές και εκπαιδευτές θα αποσταλούν σύντομα. Η Επιτροπή συγχαίρει την Ομάδα Εργασίας του Minneapolis για την εξαιρετική πρότασή τους. Παρόλο που δεν επιλέχθηκαν για το AppSec US 2010 ελπίζουμε να διοργανώσουμε σύντομα κάτι αντίστοιχο στις κεντρικές ΗΠΑ.

OWASP AppSec Research 2010 Call for Papers

Το συνέδριο OWASP AppSec σας καλεί να υποβάλλετε εργασιές που εμπίπτουν στις παρακάτω τρεις κατηγορίες:

Publish or Perish: Ερευνητικές εργασίες με ομότιμη αξιολόγηση (peer-review). Υποβολή: 12 σελίδες μέγιστο, δομή LNCS

Demo or Die: Παρουσίαση και Demo. Υποβολή: περίληψη 1 σελίδας + screenshot

Present or Repent: Μόνο παρουσίαση. Υποβολή: εκτεταμένη περίληψη 2 σελίδων.

http://tinyurl.com/yjv2otg Προθεσμία: 7 Φεβρουαρίου.

IBWAS 09

Περίπου 40 συμμετέχοντες και αρκετοί φοιτητές και καθηγητές παρακολούθησαν το συνέδριο Iberic Web Application Security (IBWAS'09) που πραγματοποιήθηκε στο Escuela Universitaria de Ingeniería Técnica de Telecomunicación, Universidad Politécnica de Madrid, στην Ισπανία στις 10 και 11 Δεκεμβρίου 2009.

Το συνέδριο, που είχε μεγάλη επιτυχία, οργανώθηκε από τις ομάδες εργασίας της Ισπανίας και Πορτογαλίας με στόχο να φέρουν κοντά ειδικούς στην ασφάλεια εφαρμογών, ερευνητές, καθηγητές και επαγγελματίες για να συζητήσουν προβλήματα και νέες λύσεις για την ασφάλεια εφαρμογών.

Μέσα από τη θερμή συζήτηση που πραγματοποιήθηκε με θέμα "**Ασφάλεια Εφαρμογών Διαδικτύου: Τι θα πρέπει να κάνουν οι κυβερνήσεις το 2010;**" προέκυψαν ορισμένα συμπεράσματα.

Τα συμπεράσματα αυτά αντικατοπτρίζουν τις αποφάσεις του πάνελ και θα πρέπει να συζητηθούν, ανανεωθούν και τελικά να εκδοθούν από το OWASP σαν ένα σύνολο συστάσεων.

1. Προκαλούμε τις κυβερνήσεις να συνεργαστούν με το OWASP για την αύξηση της διαφάνειας και της ασφάλειας των διαδικτυακών εφαρμογών, ειδικά σε ότι έχει να κάνει με οικονομικές εφαρμογές, εφαρμογές υγείας και γενικά, συστήματα στα οποία οι απαιτήσεις ιδιωτικότητας και εμπιστευτικότητας είναι κρίσιμες

2. Το OWASP θα αναζητήσει συνεργασία με κυβερνήσεις ανά τον κόσμο για την ανάπτυξη συστάσεων για την υιοθέτηση συγκεκριμένων απαιτήσεων ασφάλειας εφαρμογών και την ανάπτυξη κατάλληλου πλαισίου πιστοποίησης για τις προμήθειες εφαρμογών κρατικών φορέων.

3. Προσφέρουμε βοήθεια για την επεξήγηση και τον εκσυγχρονισμό της νομοθεσίας για την ασφάλεια πληροφοριακών συστημάτων, που θα επιστρέψει στην κυβέρνηση, τους πολίτες και τους οργανισμούς να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με την ασφάλεια.

4. Ζητούμε από τις κυβερνήσεις να ενθαρρύνουν τις εταιρίες στην υιοθέτηση προτύπων ασφάλειας εφαρμογών τα οποία όταν εφαρμόζονται βοηθούν στην προστασία όλων από παραβιάσεις ασφάλειας που μπορεί να προκαλέσουν διαρροή εμπιστευτικών πληροφοριών, διενέργεια παράνομων συναλλαγών και άλλες αξιόποινες πράξεις.

5. Προσφέρουμε συνεργασία με την κεντρική και τοπική αυτοδιοίκηση για την οργάνωση εξειδικευμένων σημείων συσσώρευσης γνώσης

[OWASP Podcasts Series](#)

Οικοδεσπότης: Jim Manico

Επ. 57 David Linthicum (cloud Computing)

Επ. 56 Adar Weidman (Regular Expression DOS)

Επ. 55 AppSec Justification Roundtable with Boaz Gelbord, Jason Lam, Jim Manico and Jeff Williams

Επ. 54 George Hesse

Επ. 53 Amichai Shulman (WAF)

Ψάχνετε για εργασία σχετική με ασφάλεια λογισμικού; Δείτε OWASP Job Page

Θέλετε να δημοσιεύσετε μία αγγελία εργασίας σχετική με ασφάλεια λογισμικού;

Επικοινωνήστε με την:

Αντιστοίχηση Κατηγοριοποίησης Απειλών WASC v2/ OWASP Top Ten 2010 RC1 προτυπα.
Blog του Jeremiah Grossman

Αναδημοσίευση από το blog του Jeremiah Grossman http://jeremiah-grossman.blogspot.com/

WASC Threat Classification v2	OWASP Top Ten 2010 RC1
WASC-19 SQL Injection	A1 - Injection
WASC-23 XML Injection	
WASC-28 Null Byte Injection	
WASC-29 LDAP Injection	
WASC-30 Mail Command Injection	
WASC-31 OS Commanding	
WASC-39 XPath Injection	
WASC-46 XQuery Injection	
WASC-08 Cross-Site Scripting	A2 –Cross Site Scripting (XSS)
WASC-01 Insufficient Authentication	A3 - Broken Authentication and Session
WASC-18 Credential/Session Prediction	
WASC-37 Session Fixation	
WASC-47 Insufficient Session Expiration	
WASC-01 Insufficient Authentication	A4 - Insecure Direct Object References
WASC-02 Insufficient Authorization	
WASC-33 Path Traversal	
WASC-09 Cross-site Request Forgery	A5 - Cross-Site Request Forgery
WASC-14 Server Misconfiguration	A6 - Security Misconfiguration
WASC-15 Application Misconfiguration	
WASC-02 Insufficient Authorization	A7 - Failure to Restrict URL Access
WASC-10 Denial of Service	
WASC-11 Brute Force	
WASC-21 Insufficient Anti-automation	
WASC-34 Predictable Resource Location	
WASC-38 URL Redirector Abuse	A8 - Unvalidated Redirects and Forwards
WASC-50 Insufficient Data Protection	A9 - Insecure Cryptographic Storage
WASC-04 Insufficient Transport Layer Protection	A10 -Insufficient Transport Layer Protection

"Μετά από πολλή δουλειά από τον Bil Corry (@bilcorry), σας παρουσιάζουμε μια καλή πρώτη προσπάθεια για τη δημιουργία αντιστοιχίας μεταξύ του νέου WASC's Threat Classification v2 και του OWASP's Top Ten 2010 RC1. Πιστεύουμε ότι αυτό θα βοηθήσει όσους χρησιμοποιούν ένα από τα δύο

OWASP TOP 10 2010 RC1—Update
Dave Wichers

Το OWASP Top 10 2010 RCI παρουσιάστηκε στο συνέδριο AppSec DC . Η περίοδος σχολίων έληξε στις 31/12/09. Η ομάδα του έργου ελπίζει να ανακοινώσει τη νέα έκδοση στις 4/2/10.

Περισσότερες πληροφορίες μπορείτε να βρείτε στην αρχή της σελίδας του Top 10 project : http://www.owasp.org/index.php/

OWASP JBroFuzz

Το έργο OWASP JBroFuzz ελέγχθηκε πρόσφατα με βάση τα Κριτήρια Αξιολόγησης του OWASP (OWASP Assessment Criteria 2.0) και η τελική του έκδοση (JBroFuzz 1.7) θεωρήθηκε Σταθερή στις **2/12/09**.

http://www.owasp.org/index.php/Category:OWASP_JBroFuzz

http://www.owasp.org/index.php/Category:OWASP_JBroFuzz_Project_-_Version_1.7_Release_-_Assessment

http://www.owasp.org/index.php/Assessment_Criteria_v2.0

Συγχαρητήρια στο συντονιστή του έργου Γιάννη Παυλόσογλου και στην ομάδα του αποτελούμενη από τους Matt Tesauro και Leonardo Cavallari Militelli, που πραγματοποίησαν την πρώτη αξιολόγηση με βάση τα νέα κριτήρια αξιολόγησης του

Παγκόσμια Επιτροπή Οργανισμών (Global Industry Committee)

Colin Watson

Η αποστολή της Επιτροπής Βιομηχανίας είναι να ενημερώσει και να ευαισθητοποιήσει ως προς τις βέλτιστες πρακτικές ασφάλειας λογισμικού δημόσιους και ιδιωτικούς τομείς, συμπεριλαμβανομένων και οργανισμών που προωθούν πρότυπα και βέλτιστες πρακτικές. Η επιτροπή επιθυμεί ακόμα να γίνει η φωνή αυτών των οργανισμών στο OWASP, προωθώντας τις απόψεις και απαιτήσεις τους.

Για να επιτύχουμε αυτό το στόχο αναλαμβάνουμε δράσεις συμπεριλαμβανομένων παρουσιάσεων, ενίσχυσης των προσπαθειών άλλων οργανισμών και από κοινού συνεργασίες όταν αυτές είναι αναγνωρίσιμες και υπάρχουν διαθέσιμοι πόροι.

Στη διάρκεια του 2009, οι Rex Booth και David Campbell στην Βόρεια Αμερική, και οι Georg Hess , Eoin Keary και Colin Watson στην Ευρώπη, μαζί με τον εκπρόσωπο του συμβουλίου του OWASP Tom Brennan ανέλαβαν 19 εξωτερικές δράσεις, ηγήθηκαν ή βοήθησαν με απαντήσεις τους σε 9 προσχέδια κειμένων καθοδήγησης, έγγραφα προβληματισμού και πρότυπα, και ξεκίνησαν να καταγράφουν εξωτερικές πηγές που αναφέρουν το OWASP και τα έργα του. Το 2010 αποκτήσαμε τρία νέα μέλη, τους Joe Bernik, Alexander Fry και Γιάννη Παυλόσογλου καθώς και το νέο εκπρόσωπο του συμβουλίου, Dave Wichers. Στόχος μας είναι να λάβουμε έναν περισσότερο προ-δραστικό ρόλο στην επικοινωνία με ανθρώπους που δεν έχουν άμεση σχέση με πληροφορική και ασφάλεια σε τομείς όπως η ενέργεια, η υγεία, η οικονομία και η διακυβέρνηση, και επίσης να προωθήσουμε τα έργα και τους πόρους του OWASP στην ευρύτερη κοινότητα. Όταν μέλη του OWASP έχουν ήδη επαφές, επιθυμούμε να τα βοηθήσουμε να αναπτύξουν ένα διάλογο μεταξύ των οργανισμών.

Βασικοί Σύνδεσμοι:

Παγκόσμια Επιτροπή Οργανισμών του OWASP : http://www.owasp.org/index.php/Global_Industry_Committee

Mailing List Παγκόσμιας Επιτροπής http://lists.owasp.org/mailman/listinfo/global_industry_committee

Αναφορές στο OWASP:

Ενημέρωση για τα έργα του OWASP

Paulo Coimbra

Νέο Έργο:

OWASP Computer Based Training Project *(OWASP CBT Project)*, υπεύθυνος: *Nishi Kumar*

Ανακοινώσεις:

OWASP ModSecurity Core Rule Set Project - ModSecurity 2.0.3 Θα αξιολογηθεί από τους: Ivan Ristic & Leonardo Cavallari.

The OWASP EnDe Project

OWASP Vicnum Project OWASP Vicnum - Έκδοση 1.4 (31/12/2009) .

OWASP Content Validation using Java Annotations Project

OWASP Application Security Verification Standard (ASVS) – Πρόχειρες εκδόσεις της Γαλλικής και Ιαπωνικής μετάφρασης. Υπό ανάπτυξη: μετάφραση στα Γερμανικά και τα Κινέζικα.

Reviewers drive: The GPC is on its way to launch a Reviewers Drive .

releases will be assessed in accordance with the OWASP Assessment Criteria 2.0.

Συνδρομές

Συνδρομές ιδιωτών: 767

- Νέες Συνδρομές το Δεκέμβριο: 26
- Ανανεώσεις το Δεκέμβριο: 0
- Χαμένες συνδρομές το Δεκέμβριο (δεν ανανέωσαν): 9
- Συνδρομές Ιδιωτών: $900

Συνδρομές Οργανισμών: 27

- Νέες Συνδρομές το Δεκέμβριο: 0
- Ανανεώσεις το Δεκέμβριο: 1 (Nokia)
- Χαμένες συνδρομές το Δεκέμβριο (δεν ανανέωσαν): 1 (Corporate One Federal Credit Union)

Έσοδα Συνδρομών το Δεκέμβριο: $5,900

Ο Dinis Cruz παρουσιάζοντας στο IBWAS 09

IBWAS 09 Πάνελ Ομιλητών:

Ευχαριστούμε τη Nokia που ανανέωσε την υποστήριξή της στο OWASP Foundation το Δεκέμβριο.

NOKIA

OWASP Foundation

9175 Guilford Road
Suite #300
Columbia, MD 21046

Τηλ.: 301-275-9403
Fax: 301-604-8033
E-mail:
Kate.Hartman@owasp.org

Η ελεύθερη και ανοικτή κοινότητα για την ασφάλεια λογισμικού

Το Open Web Application Security Project (OWASP) είναι μια ανοικτή κοινότητα αφιερωμένη στην υποστήριξη των οργανισμών για την ανάπτυξη, προμήθεια, λειτουργία και συντήρηση έμπιστων εφαρμογών. Όλα τα εργαλεία, κείμενα, φόρουμ και ομάδες εργασίας του OWASP είναι ελεύθερα και ανοικτά σε οποιονδήποτε ενδιαφέρεται για τη βελτίωση της ασφάλειας εφαρμογών. Υποστηρίζουμε την προσέγγιση της ασφάλειας σαν ένα πρόβλημα που αφορά ανθρώπους, διαδικασίες και τεχνολογία καθώς οι πιο αποτελεσματικές λύσεις περιλαμβάνουν βελτιώσεις σε όλους αυτούς τους τομείς. Μπορείτε να μας βρείτε στο www.owasp.org.

Το OWASP είναι μια νέα μορφή οργανισμού. Η ανεξαρτησία μας από εμπορικές πιέσεις μας επιτρέπει να παρέχουμε ανεπηρέαστοι πρακτικές πληροφορίες σχετικά με την ασφάλεια εφαρμογών.

Το OWASP δε συσχετίζεται με καμία τεχνολογική εταιρία, παρόλο που υποστηρίζουμε την ενημερωμένη χρήση εμπορικών τεχνολογιών ασφάλειας. Αντίστοιχα με πολλά έργα ανοιχτού λογισμικού, το OWASP παράγει υλικό σε πολλές μορφές με ανοικτό και συνεργατικό τρόπο.

Το OWASP Foundation είναι ένας μη κερδοσκοπικός οργανισμός που διασφαλίζει μακροπρόθεσμα την επιτυχία του έργου.

Χορηγοί Υποστήριξης του OWASP

Αρχισυντάκτης Newsletter: Lorna Alamri, Φωτογραφίες IBWAS : Carlos Serrao
Μετάφραση στα Ελληνικά από το OWASP Greek Chapter: Γιώργος Αργυρός, Κωνσταντίνος Παπαπαναγιώτου