15 Μαρτίου 2010

Συνέδρια OWASP AppSec

2 Ιουνίου 2010
Froc 2010
Denver, Colorado

3-4 Ιουνίου 2010
Ημέρα OWASP Μεξικού
Aguascalientes, Mexico

21-24 Ιουνίου 2010
AppSec Research 2010
Stockholm, Norway

7-10 Σεπτεμβρίου 2010
AppSec USA 2010
Irvine, California

16-19 Νοεμβρίου 2010
AppSec Brasil 2010
Campinas, Brasil

OWASP Μέλη Συμβουλίου

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

OWASP
The Open Web Application Security Project

OWASP Security Spending Project Survey
Boaz Gelbord

Το έργο «Security Spending Benchmarks» του OWASP έχει ως σκοπό να παράγει οδηγίες και ένα αποδεκτό από τη βιομηχανία σύστημα μέτρησης επιδόσεων (benchmark) που θα δικαιολογεί το συνολικό κόστος των διαδικτυακών εφαρμογών. Αυτό το έργο δημοσιεύει αναφορές σε τακτά χρονικά διαστήματα από τα αποτελέσματα των ερευνών -δημοσκοπήσεων, όπως αυτή παρακάτω.

Αυτή η έρευνα είναι ανώνυμη και καμία προσωπική πληροφορία των ερωτηθέντων δεν θα συλλέγεται. Μαζί με τη δημοσιευμένη αναφορά θα υπάρχουν διαθέσιμα και τα δεδομένα της έρευνας στη κοινότητα. Η νεότερη έκδοση του έργου «Security Spending Benchmarks» είναι ανοιχτή έως τις 15 Απριλίου.

https://www.surveymonkey.com/s/TPYZLXK

Password: OWASP_Spending

OWASP AppSec USA, Californiia 2010 Call for Papers

Το συνέδριο θα λάβει χώρα στο UC Irvine Conference Center, Orange County, CA στις 7-10 Σεπτεμβρίου 2010.

Οι υποβολές προτάσεων θα πρέπει να περιλαμβάνουν:

- Όνομα Ομιλητή/Ομιλητών
- E-mail ή και τηλέφωνο ομιλητή/ομιλητών
- Σύντομο βιογραφικό
- Τίτλο
- Περίληψη
- Οποιαδήποτε σχετική έρευνα/εργαλεία (δεν θα κοινοποιηθεί εκτός της επιτροπής συνεδρίου)

Η προθεσμία υποβολής λήγει στις 6 Ιουνίου στις 12 μμ PST (GMT-8)

Υποβάλετε προτάσεις στο: http:www.easychair.org/conferences/?conf=appsec2010

Χρηματοδότηση Έργων και Παγκόσμιας Επιτροπής

Το συνδρομητικό μοντέλο έχει επεκταθεί στα έργα και στις επιτροπές. Αυτές οι ομάδες μπορούν τώρα να βρίσκουν τους δικούς τους χορηγούς ώστε να δημιουργούν δικές τους πηγές χρηματοδοτήσεων για να υποστηρίζουν το έργο ή την επιτροπή.

Πώς δουλεύει:

Τα έργα και οι επιτροπές μπορούν να βρίσκουν τους δικούς τους χορηγούς που θα συνεισφέρουν στο έργο ή την επιτροπή. Το OWASP θα διαχειρίζεται τους πόρους και θα τους μοιράζει με τον ίδιο τρόπο που έχει ήδη γίνει για τις τοπικές ομάδες εργασίας (Chapters) δηλαδή 40/60 για τα εταιρικά μέλη.

Οι πόροι μπορούν να χρησιμοποιηθούν για να καλύψουν τα σχετικά έξοδα των έργων, αλλά όχι για να πληρωθούν τα μέλη του OWASP.

Παραδείγματα για το πώς μπορούν να χρησιμοποιηθούν οι πόροι:

Για να καλυφθούν τα έξοδα ταξιδιού ενός μέλους ενός έργου, ο οποίος πρόκειται να μιλήσει σχετικά με το έργο.

Για να εκτυπωθούν έγγραφα σχετικά με ένα έργο τα που θα μοιραστούν σε μία συνάντηση.

Για να εγγραφούν CDs.

Οι πόροι δεν μπορούν να χρησιμοποιηθούν για να αποζημιωθεί ένα μέλος του έργου για το χρόνο που ξόδεψε δουλεύοντας σε αυτό .

Επικοινωνήστε με την Kate Hartmann για να συλλέξετε πόρους από τους χορηγούς ή αν έχετε περαιτέρω ερωτήσεις για το πως έχει στηθεί αυτό το πρόγραμμα.

OWASP Podcasts Series

Οικοδεσπότης: Jim Manico

Επ. 60 Jeremiah Grossman και Robert Hansen (Η Google πληρώνει για ευπάθειες)

Επ. 59 Συζήτηση με τους Boaz Gelbord, Ben Tomhave, Dan Cornell, Jeff Williams, Andrew van der Stock και Jim Manico (Aurora+)

Επ. 58 Συνέντευξη με τον Ron Gula (Web Server Scanning, IDS/IPS)

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

Θέλετε να δημοσιεύσετε μία αγγελία εργασίας σχετική με ασφάλεια λογισμικού;

Επικοινωνήστε με την:
Kate Hartmann

Ημέρες OWASP στην Ιταλία
Matteo Meucci

Στις 5 και 6 του προηγούμενου Νοεμβρίου, το OWASP οργάνωσε δύο μεγάλες εκδηλώσεις στη Ρώμη και στο Μιλάνο της Ιταλίας .

Η πρώτη πραγματοποιήθηκε σε συνεργασία με τη CONSIP, μια εταιρία του υπουργείου Οικονομίας και Χρηματοοικονομικών της Ιταλίας. Συγκεκριμένα η εκδήλωση είχε το τίτλο «Η ασφάλεια λογισμικού σαν οδηγός για την Ηλεκτρονική Διακυβέρνηση στην Ιταλία". Το κοινό απαρτιζόταν από τους CISOs όλων των ιταλικών υπουργείων και δημόσιας διοίκησης. Οι παρουσιάσεις βρίσκονται στο παρακάτω δικτυακό τόπο : http://www.owasp.org/index.php/Italy_OWASP_Day_E-gov_09

Η δεύτερη μέρα έλαβε χώρα στο Μιλάνο με περισσότερους από εκατό συμμετέχοντες. Ανεβάσαμε τις παρουσιάσεις, τις φωτογραφίες και τα videos εδώ.

Ημέρα OWASP στην Ιταλία στο Security Summit 2010

Στις 18 Μαρτίου η Ιταλική ομάδα εργασίας του OWASP θα παρουσιάσει «Συστάσεις και Εργαλεία του OWASP για Ασφάλεια στις Διαδικτυακές Εφαρμογές στο Security Summit 2010 στο Μιλάνο στην Ιταλία. https://www.securitysummit.it/eventi/view/73

Επεξήγηση της επίθεσης Ενδιάμεσου Ανθρώπου (Man In The Middle)
Από το blog του Michael Coates 3/3/2010

«Είναι ευπαθής σε μία επίθεση Ενδιάμεσου Ανθρώπου!»

Πιθανότατα το έχετε ακούσει, αλλά ας εμβαθύνουμε στις λεπτομέρειες αυτού το είδος της επίθεσης για να καταλάβουμε πως ακριβώς λειτουργεί.

Ορισμός
Μία επίθεση Man In The Middle (MitM) πραγματοποιείται όταν η επικοινωνία μεταξύ δύο χρηστών παρακολουθείται λαθραία ή πιθανότατα τροποποιείται από ένα τρίτο, μη εξουσιοδοτημένο, άτομο. Επιπλέον, η επίθεση λαμβάνει χώρα σε πραγματικό χρόνο (έτσι για παράδειγμα, η υποκλοπή των logs ή η παρακολούθηση κάποιων πακέτων επικοινωνίας και η μετέπειτα ανάλυσή τους δεν συνιστούν μία επίθεση MitM). Παρ' όλο που μία τέτοια επίθεση μπορεί να εφαρμοστεί σε οποιοδήποτε πρωτόκολλο ή επικοινωνία, εμείς θα συζητήσουμε τη σχέση της επίθεσης με το πρωτόκολλο HTTP.

Απαιτήσεις για μια επίθεση
Μία επίθεση MitM μπορεί να επιτευχθεί με δύο διαφορετικούς τρόπους:

1. Ο επιτιθέμενος έχει τον έλεγχο ενός δρομολογητή (router) μεταξύ του θύματος και του εξυπηρετητή με τον οποίο επικοινωνεί το θύμα .

2.a. Ο επιτιθέμενος «βρίσκεται» στην ίδια δικτυακή γειτονιά αναμετάδοσης (broadcast domain, π.χ. subnet) με το θύμα .
2.b. Ο επιτιθέμενος «βρίσκεται» στην ίδια δικτυακή γειτονιά αναμετάδοσης (broadcast domain, π.χ. subnet) ως κάποια συσκευή δρομολόγησης που χρησιμοποιεί το θύμα για να δρομολογήσει τα πακέτα του .

Η επίθεση
Διαβάστε το υπόλοιπο άρθρο στο blog του Michael Coates blog

Έκδοση—OWASP ESAPI ver. 1.4.4 για JAVA ver. 1.4 και νεώτερη
Jim Manico

Αλλαγές:

http://owasp-esapi-java.googlecode.com/svn/branches/1.4/changelog.txt

Άλλοι σημαντικοί σύνδεσμοι:

Κατεβάστε το σε μορφή zip από εδώ: http://owasp-esapi-java.googlecode.com/files/ESAPI-1.4.4.zip

Μπορείτε να βρείτε τα Javadoc του ESAPI 1.4.4 εδώ: http://owasp-esapi-java.googlecode.com/svn/trunk_doc/1.4.4/index.html

Ερωτήσεις σχετικά με τη χρήση και τις ρυθμίσεις του ESAPI; Επισκεφθείτε το: https://lists.owasp.org/mailman/listinfo/esapi-user και εγγραφείτε στη mailing list.

Ενδιαφέρεστε να συμβάλλετε; Εγγραφείτε στη mailing list: https://lists.owasp.org/mailman/listinfo/esapi-dev

Κοινή αρίθμηση έργων του OWASP
Mike Boberski

Ένα νέο σχήμα αρίθμησης το οποίο θα είναι κοινό σε όλους τους οδηγούς και τις αναφορές του OWASP (OWASP Guides and References) έχει αναπτυχθεί. Η αρίθμηση ήταν μια ομαδική προσπάθεια, καθοδηγούμενη από τον Mike Boberski (ASVS project lead and co-author). Οι επικεφαλείς και οι συμβάλλοντες στο Top Ten, στους οδηγούς και στις αναφορές του OWASP καθώς και η ηγεσία του OWASP εργάστηκαν μαζί ώστε να αναπτύξουν την αρίθμηση που αφενός θα επιτρέψει την εύκολη χαρτογράφηση των οδηγών και των αναφορών του OWASP, και αφετέρου θα εισάγει μία περίοδο μεταγωγής στην οποία οι οδηγοί και οι αναφορές θα ανανεώνονται ώστε να αντικατοπτρίζουν το νέο σχήμα αρίθμησης. Αυτό το έργο θα εντοπίζει τους πεπαλαιωμένους αριθμούς και θα παρέχει νέα αρίθμηση της πληροφορίας από ένα κεντρικοποιημένο σύστημα. Μπορείτε να επισκεφθείτε την ιστοσελίδα του έργου για περισσότερες πληροφορίες: :

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

OWASP ASVS
Mike Boberski

Η πρώτη ολοκληρωμένη μετάφραση στα ιαπωνικά ολοκληρώθηκε, και ένα παράρτημα του οδηγού ASVS στην ιαπωνική γλώσσα ξεκίνησε να αναπτύσσεται. Μεταφράσεις στα γαλλικά, γερμανικά, κινέζικα, ουγγαρέζικα και μαλεσιανά βρίσκονται καθ' οδόν. Το έργο αναζητά συνεχώς εθελοντές για μετάφραση. Εάν ενδιαφέρεστε επικοινωνήστε με τον: mike.boberski@owasp.org

Οδηγός Ανάπτυξης Λογισμικού OWASP (OWASP Development Guide)
Mike Boberski

Το επόμενο στάδιο εργασιών του οδηγού έχει ξεκινήσει. Η επόμενη έκδοση του οδηγού ανάπτυξης (Development Guide) θα είναι ουσιαστικά ένας λεπτομερής οδηγός σχεδίασης για τις απαιτήσεις του OWASP ASVS. Μία ομάδα 26 εθελοντών έως στιγμής έχει εγγραφεί. Το έργο αναζητά συνεχώς εθελοντές.

OWASP Development Guide Project Page

OWASP ESAPI for PHP
Mike Boberski

Οι εργασίες συνεχίζονται για το PHP port του ESAPI. Οι περισσότερες κλάσεις του πυρήνα έχουν ολοκληρωθεί ή βρίσκονται στο τέλος της αρχικής ανάπτυξης, συμπεριλαμβανομένων των Security Configuration, Validator, Encoder και Logger. Ήδη έχει προκύψει ένας πυρήνας πρώιμων χρηστών. Παρακαλώ επισκεφθείτε το διαδικτυακό τόπο του έργου για περισσότερες πληροφορίες .

Δύο Νέα Έργα
Paulo Coimbra

OWASP Broken Web Application Project

http://www.owasp.org/intex.php/OWASP_Broken_Web_Applicaitons_Project#tab=project_Details

Το έργο αυτό χρηματοδοτείται εν μέρει από τη: Mandiant.

OWASP Ecosystem Project

Οραματιζόμαστε μια συνεργασία μεταξύ δημιουργών τεχνολογικών πλατφόρμων και ενός αναπτυσσόμενου οικοσυστήματος με έμφαση στην ασφάλεια της τεχνολογίας τους. Το οικοσύστημα θα περιλαμβάνει ερευνητές («κατασκευαστές» και «καταστροφείς»), εργαλεία, βιβλιοθήκες, οδηγίες, υλικό ενημέρωσης, πρότυπα, εκπαίδευση, συνέδρια, φόρουμ, ανακοινώσεις και άλλα.

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

134K άνθρωποι ξόδεψαν1.5 εκατομμύριο λεπτά στο site του OWASP το Φεβρουάριο!

Δωρεές για την Αϊτή:

Συνολική δωρεά από το OWASP: $1378,67

Απεστάλη στους Γιατρούς Χωρίς Σύνορα.

Τα χρήματα δόθηκαν απευθείας στην ανθρωπιστική βοήθεια για την Αϊτή.

Ευχαριστούμε τα εταιρικά μέλη που ανανέωσαν την υποστήριξή τους στο OWASP τον Ιανουάριο και το Φεβρουάριο.

Booz | Allen | Hamilton

hp invent

INFOVISION

protiviti
Independent Risk Consulting

OWASP Foundation

9175 Guilford Road
Suite #300
Columbia, MD 21046

Phone: 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
Μετάφραση στα Ελληνικά από το OWASP Greek Chapter: Σπύρος Κόλλιας, Κωνσταντίνος Παπαπαναγιώτου