2010. január 18.

OWASP AppSec konferenciák

2010. június 21-24.
AppSec Research 2010
Stockholm

OWASP *elnökségi tagok* 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 Bejelentés

A Global Conferences Committee (Globális konferencia-bizottság) izgatottan jelenti be az OWASP AppSec US 2010 konferencia helyét és időpontját. A konferencia 2010. szeptember 7 és 10. között kerül lebonyolításra a Bay Area Chapter által a Kaliforniai Egyetemen (Irvine), amely az egyetlen olyan oktatási intézmény a kaliforniai egyetemi rendszerben, amely önálló informatikai és számítógép-tudományi karral rendelkezik. A további információkat (call for speakers, call for training stb.) hamarosan közzétesszük.

Bár nem ők nyerték az AppSec US 2010 rendezési jogát, a Bizottság gratulál a Minneapolis Chapternek a kiváló pályázatért és reméli, hogy a közeljövőben ebben a régióban is lesznek hasonló

OWASP AppSec Research 2010 Call for Papers

Az OWASP AppSec Research konferenciára a következő három kategóriában várunk anyagokat:

Publish or Perish: kutatási anyagok szakmai lektorációra. Beküldendő: max. 12 oldal LNCS formátumban

Demo or Die: prezentáció és demó. Beküldendő: 1 oldalas kivonat + képernyőkép

Present or Repent: csak prezentáció. Beküldendő: 2 oldalas részletes kivonat.

http://tinyurl.com/yjv2otg Határidő: február 7.

IBWAS 09

Körülbelül 40 előadó, több tucat diák és tanáraik részvételével zajlott le az Iberic Web Application Security konferencia (IBWAS 09) a Madridi Műszaki Egyetemen 2009 december 10-11-én.

A spanyol és portugál OWASP szervezetek által életre hívott, igen nagy sikerrel záruló konferencia célja az volt, hogy összehozzuk az ipar és az akadémiai szektor biztonsági szakembereit, kutatóit és oktatóit azért, hogy nyíltan megvitathassák a problémákat és új megoldásokkal álljanak elő.

A „Webalkalmazás biztonság: mit kellene a kormányoknak 2010-ben tenniük?” panel szenvedélyes vitáinak eredményeként számos határozat született.

Ezek a határozatok a panel döntéseit tükrözik és további vita és aktualizálás tárgyát kell, hogy képezzék, majd végül az OWASP publikálja őket javaslatok formájában.

1. Felszólítjuk a kormányokat, hogy működjenek együtt az OWASP-pal a webalkalmazás biztonság átláthatóságának növelésében, különös tekintettel a pénzügyi és egészségügyi rendszerekre, illetve minden olyan rendszerre, amelyek esetén a személyes adatok védelme és a bizalmassági követelmények alapvető fontosságúak;

2. Az OWASP az egész világon keresni fogja a kormányokkal való együttműködés lehetőségét olyan követelmények létrehozását illetően, amelyek a kormányzati szoftverbeszerzési folyamatok alkalmazásbiztonsági követelményekkel és minősítési keretrendszerek kifejlesztésével való kiegészítését célozzák;

3. Felkínáljuk a segítségünket az informatikai biztonsági törvények modernizálására és tisztázására azért, hogy mind a kormányok, mind az állampolgárok, mind pedig a szervezetek jól megfontolt biztonsági döntéseket hozhassanak;

4. Arra kérjük a kormányokat, hogy ösztönözzék a cégeket olyan alkalmazásbiztonsági szabványok alkalmazására, amelyek segítenek a betörések elleni védekezésben, így elkerülhetővé válnak a bizalmas adatok napvilágra kerülésével, illetve pénzügyi és jogi következményekkel járó visszaélések.

5. Felkínáljuk annak lehetőségét, hogy a helyi és nemzeti kormányokkal együttműködve alkalmazásbiztonsági bizottságok jöjjenek létre, betekintést biztosítva az alkalmazásbiztonsággal kapcsolatos kiadásokra és támogatásra.

OWASP Podcasts Series

Hosted by Jim Manico

Ep 57 David Linthicum (cloud Computing)

Ep 56 Adar Weidman (Regular Expression DOS)

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

Ep 54 George Hesse

Ep 53 Amichai Shulman (WAF)

Alkalmazásbiztonsággal kapcsolatos munkát keresel?

Nézz szét az OWASP Job oldalon!

Alkalmazásbiztonsággal kapcsolatos munkát kínálsz?

Keresd Kate Hartmann-t!

WASC Threat Classification v2/ OWASP Top Ten 2010 RC1 megfeleltetés—Jeremiah Grossman blogja

Újraközlés Jeremiah Grossman blogjának engedélyével

http://jeremiah-grossman.blogspot.com/

„Legnagyobbrészt Bil Corry (@bilcorry) munkájának köszönhetően itt az első megfeleltetés a WASC Threat Classification v2 és az OWASP Top Ten 2010 RC1 között. Segítség lehet azoknak, akik aktívan használják valamelyik vagy mindkét dokumentumot."

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

OWASP TOP 10 2010 RC1—Frissítés Dave Wichers

Az OWASP Top 10 2010 RC1 az AppSec DC-n került kiadásra. A kommentelési időszak 2009.december 31-ig tartott. A projekt csapat tervei szerint a frissítés 2010.február 4-én jelenik meg.

További információk a Top 10 projekt oldalán (felül):http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP JBroFuzz

Az OWASP JBroFuzz projekt nemrég átesett egy OWASP Assessment Criteria 2.0 szerinti értékelésen és az utolsó kiadás (JBroFuzz 1.7) stabilnak nyilváníttatott 2009. december 2-án.

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

Gratulálunk a projektvezetőnek, Yiannis Pavlosoglou-nak és a csapatnak (Matt Tesauro, Leonardo Cavallari Militelli), akik a legelső felülvizsgálatot végezték az új OWASP értékelési kritériumok szerint.

Global Industry Committee
Colin Watson

A bizottság célja a tudatosság fokozása és a szoftverbiztonsági bevált gyakorlatok használatának népszerűsítése a nyilvános és magán szektorokban, beleértve azon szervezeteket is, amelyek szabványokat és bevált gyakorlatokat promotálnak. A bizottság ezen szervezeteket is képviselni kívánja az OWASP-on belül, teret adva a nézőpontjaiknak és elvárásaiknak.

Ezen cél elérését prezentációkkal kívánjuk elősegíteni, illetve részt vállalunk más szervezetek munkájában és együttműködési erőfeszítéseiben, amennyiben ezek beazonosíthatók és a megfelelő erőforrások rendelkezésre állnak.

2009 folyamán Rex Booth és David Campbell Észak-Amerikában, Georg Hess, Eoin Keary és Colin Watson pedig, az OWASP elnökségi képviselőjével, Tom Brennan-nel együtt Európában összesen 19 ilyen jellegű eseményen vett részt, 9 útmutató dokumentum vázlatának elkészítésén dolgozott, illetve elkezdte az OWASP projektjeinek más helyekről való hivatkozásainak dokumentálását. 2010-ben három új tag csatlakozott új elnökségi képviselőnk, Dave Wichers mellett Joe Bernik, Alexander Fry és Yiannis Pavlosoglou személyében. Az eddigieknél is aktívabban fogunk azon dolgozni, hogy eljussunk olyan emberekhez, akik nem IT-vel és nem biztonsággal foglalkoznak például az energia-, az egészségügyi ,a pénzügyi vagy a kormányzati szektorban, továbbá, hogy minél szélesebb körben népszerűsítsük az OWASP projektjeit és anyagait. Mindezeken túlmenően segíteni szeretnénk, hogy az OWASP-emberei fejleszthessék a szervezetek közötti párbeszédet.

Fontos linkek :

OWASP Global Industry Committee:
http://www.owasp.org/index.php/Global_Industry_Committee

Industry Committee Mailing List
http://lists.owasp.org/mailman/listinfo/global_industry_committee

OWASP Citations:
http://www.owasp.org/index.php/Industry:Citations

OWASP Projekt Hirek
Paulo Coimbra

Új projekt:

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

Kiadások:

OWASP ModSecurity Core Rule Set Project - ModSecurity 2.0.3 értékelés:

Ivan Ristic & Leonardo Cavallari.

The OWASP EnDe Project

OWASP Vicnum Project OWASP Vicnum - 1.4-es kiadás (2009.12.31.)

OWASP Content Validation using Java Annotations Project

OWASP Application Security Verification Standard (ASVS) – Japán és francia fordítás vázlat verziók. Folyamatban: német és kínai fordítás

Reviewers drive: hamarosan reviewers drive indul

A kiadások az OWASP Assessment Criteria 2.0 szerint lesznek értékelve.

Tagság

Tagság
Egyéni tagok: 767

- Új tagok decemberben: 26
- Megújított tagságok decemberben: 0
- Elvesztett (nem megújított) tagságok decemberben: 9
- Egyéni tagságok: $900

Szervezeti tagok: **27**

- Új tagok decemberben: 0
- Megújított tagságok decemberben: 1 (Nokia)
- Elvesztett (nem megújított) tagságok decemberben:1 (Corporate One Federal Credit Union)

Tagsági díjakból származó bevétel decemberben: $5,900

Dinis Cruz presenting azIBWAS 09 –en

Az BWAS 09 panel előadói:

Köszönjük a Nokiának, hogy decemberben megújította az OWASP Foundation támogatását!

OWASP Foundation

9175 Guilford Road
Suite #300
Columbia, MD 21046

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

A szabad és nyílt alkalmazásbiztonsági közösség

Az Open Web Application Security Project (OWASP) egy nyílt közösség, mely azzal a céllal jött létre, hogy a szervezetek számára lehetővé tegye megbízható alkalmazások fejlesztését, vásárlását és karbantartását. Minden OWASP eszköz, dokumentum, fórum és helyi tagozat nyitott bárki számára, akit érdekel az alkalmazások biztonságának javítása. Véleményünk szerint az alkalmazásbiztonság elsősorban emberi, folyamatszervezési és technológiai probléma, mert az alkalmazásbiztonsággal kapcsolatos leghatékonyabb megközelítési módok javulást eredményeznek mindezen területeken. A www.owasp.org címen vagyunk elérhetők.

Az OWASP egy újfajta szervezet. Mivel nem állunk piaci nyomás alatt, elfogulatlan és gyakorlatias alkalmazásbiztonsági anyagokat tudunk költséghatékony módon prezentálni .

Az OWASP nem függ egyetlen technológiai cégtől sem, habár támogatjuk a kereskedelmi biztonsági technológiák megfelelő ismereteken alapuló alkalmazását. Hasonlóan sok nyílt forrású szoftver projekthez, az OWASP különféle anyagai közös, nyílt munka eredményeként jönnek létre.

Az OWASP Foundation egy nonprofit szervezet; ez a projekt hosszú távú sikerének záloga.

OWASP szervezeti támogatók

Hírlevél szerkesztő: Alamri Lorna IBWAS képek: Serrao Carlos Fordította: Trifonov Gergely