2010. május 17.

OWASP AppSec konferenciák

2010. június 2.
Froc 2010
Denver, Colorado

2010. június 3-4.
OWASP Day Mexico
Aguascalientes, Mexico

2010. június 21-24.
AppSec Research 2010
Stockholm, Svédország

2010. június 30.
OWASP Argentina Day
Buenos Aires, Argentína

2010. szept. 7-10.
AppSec USA 2010
Irvine, Kalifornia

2010. szept. 17.
AppSec Ireland
Dublin, Írország

2010. nov. 16-19.
AppSec Brasil 2010
Campinas, Brazília

OWASP
The Open Web Application Security Project

OWASP AppSec Research 2010

Már elérhető a teljes konferencia és oktatási program. A Díszvacsora június 23-án (szerdán) lesz a Városházán (itt tartják a Nobel-díjkiosztókat is). További infók a Városházáról itt.

OWASP AppSec USA, Kalifornia 2010 keynote előadások

Az AppSec USA az UC Irvine Conference Center-ben lesz (Orange County, CA) 2010. szeptember 7. és 10. között.

Keynote előadók:

Bill Cheswick—AT&T Research
HD Moore—Metasploit/Rapid7
David Rice—Geekonomics
Jeff Williams—Aspect Security

A konferencia weboldala hamarosan elérhető lesz az alábbi címen:
www.appsecusa.org

OWASP AppSec, Brazília, 2010 keynote előadások

A 2010. november 16. 19. között megrendezésre kerülő OWASP AppSec Brasil konferencia keynote előadói Bruce Schneier és Jeremiah Grossman lesznek.

További infók:

www.owasp.org/index.php/AppSec_Brasil_2010

Megjelent az OWASP Top 10 2010

Az OWASP Top 10 2010 idén április 19-én jelent meg. A bejelentésnek nagy sajtóvisszhangja volt; ízelítőül álljon itt néhány link a nemzetközi médiából. Ha még nem tetted volna meg, akkor kérünk, hogy szánj egy pár percet a Top 10 2010-re és segíts, hogy az alkalmazásbiztonság még nagyobb teret kapjon.

Bejelentés:

http://www.owasp.org/index.php/OWASPTop10-2010-PressRelease

Cikkek:
Logic Flaws and the OWASP Top 10, Steve Ragan—The Tech Herald

Top 10 Most Critical Web App Security Risks, Ericka Chickowski—Channel Insider

Injection tops list of web application security risks, Angela Moscaritolo—SC Magazine

OWASP Issues Top 10 Web Application Security Risks List, Kelly Jackson—DarkReading

Security: 10 Most Dangerous Web App Security Risks, Brian Prince—eWEEK

OWASP Hírlevél —Cikkeket várunk

Alkalmazásbiztonsággal kapcsolatos, nem kereskedelmi célú cikkeket várunk az OWASP hírlevél következő számaiba.

További infók és cikkbeküldés az alábbi e-mail címen: Lorna.Alamri@owasp.org

OWASP Podcast sorozat

Házigazda: Jim Manico

Ep 61 Richard Bejtlich (Network Monitoring)

Ep 62 Amichai Shulman (WAF)

Ep 63 Ed Bellis (eCommerce)

Ep 64 Andy Ellis (Availability)

Ep 65 AppSec Round Table: Boaz Gelbord, Dan Cornell, Jeff Williams, Johannes Ullrich & Jim Manico

Ep 66 Brad Arkin (Adobe)

Ep 67 Top Ten– Jeff Williams (XSS)

Ep 68 Top Ten— Kevin Kenan (Cryptographic Storage)

Ep 69 Top Ten—Eric Sheridan (CSRF)

Ep 70 Top Ten— Michael Coates (TLS)

Ep 71 Top Ten— Robert Hansen

Interjú Jim Manico-val

Lorna Alamri

Az OWASP legnagyobb előnyeinek egyike, hogy teret ad az alkalmazásbiztonság megszállottjainak. Jim Manico nevéhez fűződik az a podcast sorozat, amelyben ismert alkalmazásbiztonsági szakértőket szólaltat meg. Az OWASP Podcast Series életre hívásával a saját karrierjének is lökést adott, illetve sikeresen növelte az OWASP tudásbázisát és általában az alkalmazásbiztonsággal kapcsolatos tudatosságot.

Miért csináltad az első podcast-ot?

2008. októberében tanúja voltam több vitának, amelyek az OWASP önkéntesei és vezetősége között zajlott. Lenyűgözött a viták mélysége és arra gondoltam, hogy ezt valahogyan rögzíteni kellene. A podcast, mint közzétételi forma egyszerűnek tűnt, ezért—engedélykérés nélkül—csak úgy elkezdtem felvenni a beszélgetéseket :). Arshan, Jeff Williams és Jeremiah Grossman voltak az első áldozataim, gyakorlatilag azóta folyamatosak a közvetítések :)

Mi volt az eredeti célod? Változott ez azóta? Ha igen, hogyan?

Eredetileg egy könnyed hangvételű, „laza” beszélgetés rögzítését és mp3 formátumban történő publikálását szerettem volna. Akkoriban egy ingyenes telekonferencia-rendszert használtunk, de most már beszerzés alatt van egy felsőkategóriás stúdiómikrofon és elsősorban a minőségre koncentrálok (ez a vágásra és az utómunkálatokra is vonatkozik). Így már elég messze kerültem az eredeti elképzeléseimtől, de folyamatosan igyekszem javítani a műsor minőségét .

Hogyan alakult ki a projekt?

Ma (március közepe) vágom a 63. adást. Van egy csomó kész műsorom és most várom az új Top Ten hivatalos kiadását.

Hogyan készülsz egy interjúra?

Először időpontot egyeztetek a vendégekkel, de van egy havi ismétlődő meghívóm is a kerekasztal-beszélgetéshez. A kérdéseket előre kidolgozom a vendégek bevonásával, mivel értelmes válaszokat, hozzászólásokat várok, nem pedig meglepett interjúalanyokat.

Melyik volt a legnépszerűbb adás? És a legvitatottabb? Melyik a kedvenced?

A kerekasztal-beszélgetések a legnépszerűbbek. Volt egy vendégünk, aki az OWASP-ot „egy csapat kommunistának” nevezte, amit azért eléggé furcsálltak páran. A kedvenc műsorom az, amelyben Billy Hoffman (HP) szerepelt—azt mondta, hogy a nagymamám megérdemelné, hogy meghekkeljék ;), de Dave Aitel volt a legjobb arc. Richard Stallman eléggé nekem esett, amikor megkérdeztem, hogy mi a Skype azonosítója (a Stallman-nal készült anyagot csak ogg formátumban adtam ki! Tényleg!). Különösen hálás vagyok Andre Gironda-nak, Jeff Williams-nek és Boaz-nek a támogatásukért. De frankón, **minden vendégem király volt!**

Mit csinálnál máshogyan?

Bárcsak sose mondtam volna, hogy egy ingyenes telekonferencia-szolgáltatás megfelelő lesz egy podcast rögzítéséhez! :)

Mi volt a legnagyobb kihívás?

Csinálni. Ahogy elkezdődött az egész, a podcast szelleme átvette az irányítást. :)

Mi a sorozat sikerének titka?

A vendégek. Abban a megtiszteltetésben volt részem, hogy néhány igazán okos és tehetséges vendégem volt a műsorban. Ez az egész nem működhetne a közösség nélkül.

Ha bárkit meghívhatnál a műsorba, ki lenne az?

Az a microsoftos arc, aki kitalálta a httpOnly -t! :)

A viccet félretéve, Bruce Schneier egyike azoknak, akikre még mindig vadászom. A sorozat kezdetén volt egy interjúm vele, de az én hibámból annyira rossz minőségűre sikerült a felvétel, hogy nem tehettem ki. Bruce! Bocsánat! Kérlek, adj még egy esélyt! :)

Mi jön ezután?

A show-nak mennie kell! Számos cég támogatta az OWASP-ot cserébe a szereplési lehetőségért és ennek köszönhetően van egy kis keretem, hogy profi stúdiócuccokat vegyek. Köszönöm Tenable, az Adobe, az Orbitz és az Akamai nagylelkű támogatását!

Van bármilyen tanulság, tapasztalat vagy akármi, amit meg szeretnél osztani a közönségeddel?

Közzétettem a felszerelésem és az egész folyamat leírását a http://www.owasp.org/index.php/Talk:OWASP_Podcast címen. Ez a lista az elmúlt pár év tapasztalatai alapján született.

És a legfontosabb: köszönöm, hogy hallgattok! A sorozat nem lenne ilyen sikeres, ha nem a mi fantasztikus hallgatóinkért csinálnánk!

Ha bármilyen megjegyzésed van, kérjük, írd meg a podcast@owasp.org címre!

Tudsz segíteni abban, hogy *minden* fejlesztő értesüljön az OWASP Top 10-ről?
Terjeszd ezt a linket:
OWASP_Top_10_-_2010.pdf

London OWASP Chapter
OWASP AppSec Training Project

A londoni OWASP tagozat április 16-án tartotta első oktatását.

A prezentációk az alábbi problémákat járták körül:

- Az OWASP Top 10 kivételével a legtöbb OWASP projekt nem nagyon ismert és használt. Ennek oka nem a projektek minőségében keresendő, hanem abban, hogy kevesen értik pontosan, hogy hogyan illeszkednek ezek a projektek egy vállalati biztonsági környezetbe vagy a webalkalmazás-fejlesztési életciklusba.
- Jelen kurzus ezen a problémán érett vállalati projektek és kapcsolódó gyakorlati, használati példák bemutatásával kíván segíteni.
- A kurzus erősen gyakorlat-orientált.

Az anyagok letölthetők a következő helyről:

OWASP Projects and Resources you can use today.

Várjuk, hogy más OWASP tagozatok is megtartsák ezeket az oktatásokat az anyagok felhasználásával.

Köszönjük céges tagjaink márciusi és április támogatásait!

Booz | Allen | Hamilton

cigital

symantec

fishnet SECURITY

Új céges támogatónk április-ban: Qualys

Köszönjük a

QUALYS

Kövesd az OWASP-ot

OWASP a Twitteren:

http://twitter.com/statuses/user_timeline/16048357.rss

IBWAS '10—Call for Papers

Carlos Serrão, Ph.D.

A második ibériai-amerikai webalkalmazás-biztonsági konferencia (IBWAS'10) Lisszabonban (Portugália) kerül megrendezésre 2010. november 11 -12-én.
A konferencia célja, hogy összehozza az ipar, az akadémiai szektor és a nemzetközi közösség biztonsági szakembereit, kutatóit és oktatóit azért, hogy nyíltan megvitathassák a problémákat és új megoldásokkal álljanak elő. Ez a légkör lehetőséget teremt arra, hogy az akadémiai szféra kutatói kombinálhassák az eredményeiket a gyakorlati szakemberek tapasztalataival.
A konferencia szervezői már publikálták a Call for Papers (CfP) felhívást. Bárki, aki szeretne anyagot küldeni, megteheti ezt a CfP utasításai alapján, legkésőbb 2010. szeptember 24-ig.
Néhány javasolt téma:

- Biztonságos alkalmazásfejlesztés
- Szolgáltatásorientált architektúrák biztonsága
- Fejlesztői keretrendszerek biztonsága
- Fenyegetettség-modellezés web alkalmazások esetén
- Cloud biztonság
- Web alkalmazások sérülékenységei és ezek elemzése (code review, behatolási tesztelés, statikus elemzés stb.)
- Alkalmazásbiztonsági metrikák
- Biztonságos kódolási technikák
- Platform vagy nyelv biztonsági jellemzők, szolgáltatások, amelyek segítenek a web alkalmazások biztonságának növelésében
- Biztonságos adatbázis-használat web alkalmazások esetén
- Hozzáférés-ellenőrzés web alkalmazások esetén
- Adatvédelem web alkalmazások esetén
- Web alkalmazásokat érintő szabványok, minősítések és biztonsági vizsgálati kritériumok
- Alkalmazásbiztonsági tudatosság és oktatás
- Támadások, sérülékenységek kihasználása

Minden elfogadott előadás ISBN hivaktozás alatt publikálásra kerül a konferenciaanyagokban. A konferenciaanyagokat a Springer adja ki a Communications in Computer and Information Science (CCIS) sorozatban.
További infók:
Call for Papers: http://www.owasp.org/

OWASP Projects hírek

Paulo Coimbra, OWASP Project Manager

Új projektek

Magyar fordítás projekt
http://www.owasp.org/index.php/OWASP_Hungarian_Translation_Project#tab=Project_Details

RFP– Criteria
http://www.owasp.org/index.php/Projects/RFP-Criteria

Új kiadások

JSReg: JavaScript regex-alapú sandbox
https://code.google.com/p/jsreg/

HTML Reg: JavaScript regex-alapú sandbox HTML-hez
http://code.google.com/p/htmlreg/

JavaScript regex-alapú sandbox CSS-hez
http://code.google.com/p/cssreg/

OWASP oktatások

London Training: OWASP projects and resources you can use today May 28th, 2010

London Training: OWASP projects and resources you can use today April 16th, 2010

Oktatóvideók

http://www.youtube.com/watch?v=pYp-kJTrzCE&feature=player_embedded

http://www.youtube.com/watch?v=eRRwaAmKhVg&feature=player_embedded

ASVS fordítások & ESAPI for PHP Project hírek

Mike Boberski

Az ASVS befejezett fordításainak száma háromra emelkedett (francia, német, japán):
ASVS Translations
További, folyamatban lévő fordítások: maláj, kínai, magyar, perzsa, spanyol és thai

Az ESAPI for PHP projekt lassan kiadási fázisban lép; már csak a végső simítások vannak hátra (pl. a kódbázis PEAR-kompatibilissé tétele, phpdoc hozzáadása stb.):
http://www.owasp.org/index.php/Category:OWASP_Enterprise_Security_API#tab=PHP

OWASP

Az alkalmazásbiztonság láthatóbbá tétele

Idén az OWASP az alkalmazásbiztonság láthatóbbá tételére koncentrál. Ehhez az egyik út az OWASP előadók nem-OWASP rendezvényeken való részvétele. Összegyűjtöttünk néhány rendezvényt, amelyeken az OWASP felszólal:

Franciaország: a francia tagozat az RMML 2010-en: http://2010.rmll.info/OWASP.html?lang=en
Pár gondolat RMLL2010-ről :
A Libre Software Meeting (LSM vagy RMLL, a francia Rencontres Mondiales du Logiciel Libre elnevezés rövidítéseként) egy szabad szoftverekkel kapcsolatos konferencia-ciklus, amely 2000-ben indult és évente kerül megrendezésre, 2003-tól mindig más városban. Az LSM rendezvények ingyenesek, jelentkezési korlátozás nélkül. A 2010-es rendezvény Bordeaux-ban lesz július 6. és 11. között, 7 fő témával (minden témához több, részletesebb session tartozik majd). Bemutatunk néhány eszközt és appsec trükköt (pl. egy kis pót OWASP London oktatást), de lesz még Top 10 2010 Webgoat/WebScarab példákkal.

Görögország: a görög tagozat támogatja az AthCon konferenciát (http://www.athcon.org/), amely Athénban kerül megrendezésre június 3-4-én. OWASP tagoknak 15% kedvezmény a regisztrációs díjból!

Malajzia: a maláj OWASP tagozat jelen lesz a Malaysia Open Source Conference 2010-en (http://conf.oss.my).

Szingapúr: a szingapúri chapter a következő rendezvényeket támogatja:

1) ISC2 SecureAsia@Singappore július 26-27-én (http://www.informationsecurityasia.com/)
2) GovernmentWare (a szingapúri belügyminisztérium szervezésében) szept. 28. és 30. között (http://www.govware.sg).

Szlovénia: a szlovén chapter részt vesz az OTS 2010 konferencián (http://cot.uni-mb.si/ots2010/), amely Mariborban kerül megrendezésre június 15. és 16. között. Az OTS a 15. évfordulóját ünnepli és a szlovén chapter büszke, hogy az alkalmazásbiztonsági szekciót vezetheti június 16-án (szerda) 16:15-től.

USA: OWASP részvétel az ICCS-en (http://www.iccs.fordham.edu), amely az FBI és a Fordham University közös szervezésű konferenciája. Hely és idő: Fordham Law Center, New York, NY, augusztus 2-5.

Alkalmazásbiztonsággal kapcsolatos munkát keresel?

Nézz szét az OWASP Job oldalon!

Alkalmazásbiztonsággal kapcsolatos munkát kínálsz? Keresd Kate Hartmann-t!

OWASP Foundation

9175 Guilford Road
Suite #300
Columbia, MD 21046

Telefon: 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 céges támogatók

UPDATING LOGOS

Hírlevél szerkesztő: Lorna Alamri Fordította: Trifonov Gergely