2010. március 15.

OWASP AppSec konferenciák

2010. június 2.
Froc 2010
Denver, Colorado

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

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

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

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

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

OWASP Security Spending projekt kérdőív
Boaz Gelbord

Az OWASP Security Spending Benchmarks projekt célja, hogy egy általánosan elfogadott, viszonyítási alapként használható útmutató jöjjön létre, amely web alkalmazások teljes költségének igazolására használható. Ez a projekt rendszeresen jelentet meg a jelenlegihez hasonló felmérési adatokat.

A kérdőív kitöltése teljesen névtelen és semmilyen személyes adatot nem gyűjtünk a válaszadóktól.

A jelentéssel együtt a nyers felmérési adatok is publikálva lesznek. Az OWASP Security Spending Benchmarks projekt legújabb verziója április 5-ig érhető el.

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

Jelszó: OWASP_Spending

OWASP AppSec USA, Kaliforinia 2010— felhívás (Call for Papers)

A konferencia az UC Irvine Conference Center -ben lesz (Orange County, Kalifornia) 2010. szeptember 7. és 10. között.

A benyújtott anyagoknak tartalmazniuk kell:

- Az előadó(k) nevét
- Az előadó(k) e-mail címét és/vagy telefonos elérhetőségét
- Az előadó(k) életrajzát
- Az előadás címét
- Az előadás kivonatát
- Bármilyen, az előadáshoz tartozó kutatást vagy eszközt (csak a CFP bizottság belső használatára)

Jelentkezési határidő: június 6., 12 óra PST (GMT-8)

Jelentkezések beküldése:
http:www.easychair.org/conferences/?conf=appsec2010

Projekt és Global Committee finanszírozás

A tagsági modell kiterjesztésre került a projektekre és a Global Committee-re. Ezek a csoportok mostantól saját szponzorokat kereshetnek a projekt vagy a Global Committee finanszírozása céljából.

Hogyan működik mindez?

A projektek és bizottságok saját szponzorokat kereshetnek a projekt vagy bizottság finanszírozására. Az OWASP alapítvány kezeli és osztja el forrásokat ugyanúgy, ahogy azt most is történik a tagozatoknál a céges tagsági díjak 40/60 arányú felosztásával.

A források a projekthez kapcsolódó kiadások fedezésére fordíthatók, de nem használhatók az OWASP tagok kifizetésére.

A források felhasználhatók például:

- projekttagok utazási költségeinek fedezésére (a projekttel összefüggő utazások esetén)
- a projekttel kapcsolatos dokumentumok nyomtatására (rendezvényeken való kiosztás céljából)
- CD-k készítésére

A források nem használhatók projekttagok projekten végzett munkájának ellentételezéseként.

Keresd Kate Hartmann-t a szponzoroktól való támogatások begyűjtésével és további kérdésekkel kapcsolatban.

OWASP Podcast sorozat

Házigazda: Jim Manico

Ep 60 Jeremiah Grossman és Robert Hansen (A Google fizet a sérülékenységekért)

Ep 59 AppSec Kerekasztal: Boaz Gelbord, Ben Tomhave, Dan Cornell, Jeff Williams, Andrew van der Stock és Jim Manico (Aurora+)

Ep 58 Interjú: Ron Gula (web szerver szkennelés, IDS/IPS)

OWASP Italy Days

Matteo Meucci

Tavaly november 5-én és 6-án az OWASP nagyszabású rendezvényeket tartott két olaszországi helyszínen, Rómában és Milánóban.

Az első a közigazgatásban dolgozó CONSIP-pel (az olasz Gazdasági és Pénzügyminisztérium tulajdonában álló cég) való szoros együttműködés eredményeként jött létre. A rendezvény az „Alkalmazásbiztonság mint az olasz e-kormányzat előmozdítója” címet kapta. A hallgatóság az összes olasz minisztérium és közigazgatási intézmény CISO-iból állt.

A prezentációk itt érhetők el: http://www.owasp.org/index.php/Italy_OWASP_Day_E-gov_09

OWASP—Italy Day IV Milánóban– A második rendezvény Milánóban volt, több mint száz résztvevővel. A prezentációk, fotók és videók most lettek elérhetők itt.

OWASP—Italy Day a Security Summit 2010-en

Az OWASP olasz tagozata a március 18-án, Milánóban megrendezésre kerülő Security Summit 2010 rendezvényen az „OWASP útmutatók és eszközök a web alkalmazás biztonságban” előadással fog szerepelni. https://www.securitysummit.it/eventi/view/73

Man-in-the-Middle támadások—Michael Coates blogja 2010.03.03.

Talán már hallottál a MitM támadásokról, de most nézzük meg részleteiben, hogy megérthessük, pontosan hogyan is működik.

Meghatározás

A beékelődéses (MitM) támadás olyan támadás, amelynek során két felhasználó között folyó kommunikációt titokban megfigyel és adott esetben módosít egy illetéktelen harmadik fél. Ezt a tevékenységet a támadó valós időben végzi, tehát naplóállományok ellopása vagy rögzített hálózati forgalom későbbi elemzése nem számít MitM támadásnak.

Bár ilyen támadás bármilyen protokoll vagy kommunikáció esetén előfordulhat, most a HTTP vonatkozásában fogjuk megvizsgálni.

A támadás előfeltételei

MitM támadás kétféleképpen történhet:

1. A támadó az áldozat és annak szervere közötti kommunikációs útvonalon egy útválasztót felügyel

2.a. A támadó ugyanazon szórási tartományban (hálózati szegmensben) van, mint az áldozat

2.b. A támadó ugyanazon szórási tartományban (hálózati szegmensben) van, mint az áldozat által használt bármely útválasztó eszköz

A támadás

Folytatás Michael Coates blogjában.

Kiadás: OWASP ESAPI ver. 1.4.4 JAVA ver. 1.4-hez (és újabbakhoz)

Jim Manico

Changelog:

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

További fontos linkek:

A teljes .zip kiadás letölthető innen: http://owasp-esapi-java.googlecode.com/files/ESAPI-1.4.4.zip

ESAPI 1.4.4 Javadoc: http://owasp-esapi-java.googlecode.com/svn/trunk_doc/1.4.4/index.html

Kérdéseid vannak az ESAPI használatával vagy beállításával kapcsolatban? Itt feliratkozhatsz a levlistára: https://lists.owasp.org/mailman/listinfo/esapi-user

Szeretnél közreműködni? Levlista: https://lists.owasp.org/mailman/listinfo/esapi-dev

OWASP Common Numbering projekt
Mike Boberski

Új számozási séma került kidolgozásra, amely a jövőben egységesen alkalmazva lesz az OWASP útmutató és referencia dokumentumokban. Az új rendszer kidolgozását Mike Boberski (ASVS projektvezető és társszerző) csapata végezte. Az OWASP Top Ten, Guide és Reference projektek vezetői és egyéb munkatársai együtt dolgoztak az OWASP vezetőségével egy olyan számozási séma kifejlesztésén, amely az OWASP dokumentumok egyszerű megfeleltethetőségét teszi lehetővé. Az útmutatók és referenciák folyamatosan kerülnek frissítésre. Ez a projekt követi a visszavont számokat és központosítottan lehetőséget teremt az információk megfeleltetéséhez. További információk a projekt honlapján:

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

OWASP ASVS
Mike Boberski

Az első teljes japán fordítás elkészült; most egy japán nyelvű ASVS concept guide függeléken folyik a munka. Az ASVS francia, német, kínai, magyar és maláj nyelvű fordításai már folyamatban vannak. A projekt folyamatosan várja a fordításra az önkénteseket.

Jelentkezés: mike.boberski@owasp.org

OWASP Development Guide
Mike Boberski

Megkezdődött a fejlesztési útmutató következő verziójának kidolgozása, amely tulajdonképpen egy részletes tervezési útmutató lesz az ASVS követelményei alapján. A csapat jelenleg 26 önkéntesből áll és folyamatosan bővül, de várjuk a további jelentkezőket.

Az OWASP Development Guide projekt honlapja

OWASP ESAPI PHP-hoz
Mike Boberski

Folytatódik a munka az ESAPI PHP portján. A legtöbb core osztály elkészült vagy a fejlesztés utolsó lépcsőfokán jár (pl. Security Configuration, Validator, Encoder és Logger). Egyre növekszik a korai felhasználók száma.

További információk a projekt honlapján.

Két új projekt
Paulo Coimbra

OWASP Broken Web Application projekt

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

A projekt részleges szponzora a Mandiant.

technológiáik biztonságára koncentráló, egyre gyarapodó közösség között. Ebben az ökoszisztémában helyet kapnak majd a kutatók, valamint eszközök, könyvtárak, útmutatók, tudatosságfokozó anyagok, szabványok, oktatások, konferenciák, fórumok és sok más egyéb.

OWASP Ecosystem projekt

Egy partnerség körvonalazódik a technológiai platform forgalmazók és az ő

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

Februárban 134 ezer ember összesen 1.5 millió percet töltött az OWASP website-on!

Haiti felajánlások:

Teljes OWASP-támoatás: $1378.67

Kapja: Doctors Without Borders.

A felajánlások közvetlenül haiti segélyezésre lettek fordítva.

Köszönjük céges tagjaink januári és februári támogatásait.

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 céges támogatók

Hírlevél szerkesztú: Lorna Alamri Fordította: Trifonov Gergely