

2010. július 17.



OWASP

The Open Web Application Security Project

Alkalmazásbiztonsági konferenciák



2010. szept. 7-10., Irvine, CA - USA

Regisztráció: <http://www.appsecusa.org/register-now.html>



2010. szept. 16-17., Dublin, Írország

CFP, CFT: http://www.owasp.org/index.php/OWASP_IRELAND_2010#Call_for_Papers Regisztráció: http://www.owasp.org/index.php/OWASP_IRELAND_2010#Registration

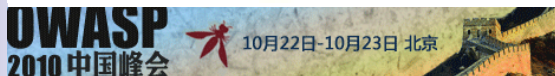


October 20-21, 2010, Rochester, NY – USA CFP: <http://www.rochestersecurity.org/call-for-presentations>



2010. október 20., Nürnberg, Németország

CFP: http://www.owasp.org/index.php/OWASP_AppSec_Germany_2010_Conference#tab=Call_for_Papers_-_English_Version



2010. október 20-23., Peking, Kína CFP, CFT: - http://www.owasp.org/index.php/OWASP_China_Summit_2010#tab=Call_For_Paper



2010. október 29., Austin, Texas - USA

CFP: http://www.owasp.org/index.php/Lonestar_Application_Security_Conference_2010#tab=Call_for_Papers



2010. november 8-11., Washington, DC – USA

CFP, CFT:- http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=CFP

Regisztráció: http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=Registration



2010. november 11-12, Lisszabon, Portugália

CFP: http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers



OWASP AppSec Brasil 2010

2010. november 16-19., Campinas, SP, Brazília

CFP, CFT:- http://www.owasp.org/index.php/AppSec_Brasil_2010#tab=Calls



OWASP Podcast sorozat

Házigazda: **Jim Manico**

Ep 72 [Interjú: Ivan Ristic \(WAF\)](#)

Ep 73 [Jeremiah Grossman és Robert Hansen](#)

**Köszönjük
céges
tagjaink
júniusi és
júliusi
támogatását!**



Interjú Matt Tesauro-val *Lorna Alamri*

Az OWASP egyik legnagyobb erénye, hogy fórumot biztosít az alkalmazásbiztonság megszállottjainak. Matt Tesauro a LiveCD projekt vezetője, aki munkájával nagy mértékben növelte az OWASP tudásbázist és az alkalmazásbiztonsággal kapcsolatos tudatosságot.

Miért csináltad az első live CD-t?

Az OWASP Live CD-t az OWASP Summer of Code 2008 keretén belül csináltam. Amikor a felhívásban megláttam egy alkalmazásbiztonságot és Linuxot vegyítő projektet, akkor tudtam, hogy ez nekem való, mivel ez a két kedvenc témám.

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

Az első cél az volt, hogy legyen egy működő verzió a SoC határidő lejártáig ;).

Valójában a legjobb alkalmazásbiztonsági eszközöket próbáltam összegyűjteni, egyszerűen használható formába öntve. Nem egy általános „hekker” eszközyűjteményt akartam csinálni, hanem kifejezetten az appsec témára fókuszáltam.

A live CD nyilván egy csomót változott a 2008. szeptemberi első verzió óta. Az első nagy változást a projektből kinőtt számtalan alprojekt jelentette (mint például a VMware és VirtualBox virtuális telepítések). Volt egy működő, de borzasztóan lassú, USB meghajtóról futó virtuális gépünk is.

Az igazság az, hogy ez a dolog kinőtte magát, sokkal több már, mint egy live CD és pont ezért át is neveztük OWASP WTE -re (Web Testing Environment). Az OWASP Live CD alapját átraktuk SLAX-ról Ubuntura, aztán minden eszközhöz a többitől függetlenül telepíthető csomagot készítettünk. Ennek az a legnagyobb előnye, hogy könnyebben tudjuk majd eljuttatni a tesztelőeszközöket a biztonsági szakemberekhez, hiszen egy teljesen alap Ubuntu telepítésre pillanatok alatt felrakható a teljes WTE környezet.

Hogyan fejlődött a projekt?

Ahogy már említettem, egy bootolható CD-ből indultunk ki és most ott tartunk, hogy a szükséges eszközöket egy csomóféleképp eljuttathatjuk a célközönséghez.

Ahogy befejezzük a SLAX-Ubuntu migrációt, a következő módokon lesz majd elérhető a WTE:

- live CD
- virtuális telepítések (VMware, VirtualBox, Parallels, ...)
- meglévő Ubuntura való telepítés
- WTE USB meghajtón
- Wubi—Windows-Ubuntu dual boot megoldás újraparticionálás nélkül
- egyedi verzió (pl. Java statikus eszközök, eszközök és támadási célok stb.)
- új eszközkategóriák (pl. statikus analízishez)

Szerencsére számos ember hozzájárult a projekthez: Nishi Kumar a kiadások grafikai munkáit intézte, de Brad Causey és Drew Beebe szintén rengeteg időt ölt a projektbe és nagyon sokat segítettek.

Bevallom, hogy amióta a Trustwave SpiderLabs-nél dolgozom, azóta több időt fordítottam ennek az új, csodálatos munkahelynek a megismerésére, mint a projektre. Hatalmas élmény ilyen kaliberű emberekkel együtt dolgozni és tényleg több időt töltöttem velük, mint WTE Debian csomagok készítésével. Viszont izgalomra semmi ok, mert lesz egy munkára szánt WTE virtuális telepítem és már csak idő kérdése, hogy folytassam ezt a témát.

Melyik volt a legnépszerűbb alkalmazás a live CD-n? És a legvitatottabb? Melyik a kedvenced?

Magasan a WebGoat az, amelyikről a legtöbb szó esett, illetve amelyiket a legtöbben kérték és valószínűleg használták. Úgy vélem, hogy az a tény, hogy a WebGoat egy pillanat alatt használatra kész, sokak számára óriási vonzerővel bírt, legyenek akár tanulók vagy maguk a tanárok.

Nem tudom, hogy volt-e igazán vitatott alkalmazás—talán a Metasploit, amelyik nem kifejezetten webappsec eszköz. A zárt forrású Maltego CE próbaverzió miatt is volt némi morgás. Én nem vagyok ilyen szigorú, mivel tudom, hogy a srác, aki írta, ennek a cuccnak az eladásából tartja fenn magát.

Személyes kedvenc... nem szeretnék csak egyet kiválasztani. A legtöbbet a WebScarab-ot, Burp Suite-et, a JBroFuzz-t, Nikto-t és DirBuster-t használok, de van még egy pár új kedvenc, amik a következő WTE kiadásba fognak bekerülni.

Mit csinálnál másképp?

Tényleg szerettem a SLAX-ot live CD készítésére használni, mert tök jó volt erre a célra, de abban a pillanatban, ahogy elkezdünk a VM-ek felé kacsintgatni és megpróbáltuk a live CD-t dinamikusan frissíteni, már nem volt olyan kényelmes.

Szóval ha bármit előlről kéne kezdenem, akkor olyan Linuxszal indulnék, aminek megfelelő csomagkezelő rendszere van. A Debian csomagkezelője mögött sok év tapasztalata van, úgyhogy miért ne használnánk? Egyébként az RPM is jó csomagkezelő. Szeretnék RPM-gurukkal dolgozni, hogy a WTE .deb-ekből RPM-ek is készülhessenek.

Mi volt a legnagyobb kihívás?

Az egyik legelső kihívás az ésszerűség megtartása volt. Megnéztem mindenféle alkalmazásbiztonsági eszközt és összejött egy 330 eszközt tartalmazó lista. Beletelt némi időbe, mire ezt leszorítottam egy értelmes mennyiségre. A helyes csomagkészítést is elég fájdalmas megtanulni eleinte, de ha már benne vagy, akkor automatizálható a csomagok frissítése, úgyhogy hosszú távon kifizetődő.

Miből gondolod, hogy a live CD sikeres?

Utoljára tavaly novemberben néztem a letöltések számát; éppen 300.000 fölött járt akkor, az első SoC kiadás óta számolva. Ez elég sok embert jelent, aki megismerte az OWASP-ot és az alkalmazásbiztonságot. Számtalan tanárról is tudok, akik a CD-t használják az óráikon, de a legmeglepőbb az volt, amikor egy főiskolai jegyzetben találkoztam a live CD-vel. Pár hete Stockholmban, az AppSec EU 2010 konferencián egy résztvevő oda-jött hozzám és megköszönte a legutóbbi WTE kiadást, szóval hogyan is panaszkodhatnék?

Hogyan befolyásolta a live CD a karriered?

Óriási élmény volt már maga az is, hogy az OWASP-pal együtt dolgoztam és a live CD egy remek módja volt annak, hogy bekerüljek az OWASP közösségbe. A live CD, illetve az ezzel kapcsolatos előadások révén eljutottam Portugáliába, Brazíliába meg még egy csomó helyre az USA-n belül. Megismertem egy rakás remek OWASP-os arcot és a nevem ismert lett az appsec közösségen belül.

Mindezeneken felül meggyőződésem, hogy a live CD-vel és a Global Projects Committee-ben végzett munkám hozzásegített ahhoz, hogy OWASP alapítványi elnökségi tag lehessen. Csodálatos élmény a többi elnökségi taggal együtt dolgozni az OWASP missziójának végrehajtása érdekében.

Pragmatikusan szemlélve a dolgot: többször voltam fizetett oktató a live CD projektből kifolyólag, nem beszélve arról, hogy az OWASP-pal való aktív együttműködés és elnökségi tagság nagyon jól mutatnak az ember önéletrajzában. Biztos vagyok benne, hogy az OWASP-nál szerzett tapasztalatom sokat nyomott a latban, amikor bekerültem a Trustwave SpiderLabs-hez.

Mi jön ezután?

A WTE esetében növelni szeretném a közreműködők számát, hogy ne én jelentsem a szűk keresztmetszetet (mint most év elején). Ezen kívül bővíteni szeretném a WTE csomagokat, hogy legyenek közöttük cuccok statikus kódanalízishez, Flash eszközök, és talán néhány sérülékeny alkalmazás is.

Az OWASP elnökségen belül az OWASP operációs infrastruktúráján dolgozom. Remélhetőleg az OWASP-nak új, nagyvállalati szintű infrastruktúrája lesz, ami egy teljesen új szintre emelheti a közösséget.

Még valami, amit meg szeretnél osztani a projekt rajongóival?

Nem tudom eléggé megköszönni azoknak, akik a licenszelést leegyszerűsítik és olyan általános nyílt forrású licenzeket választanak, mint amilyen a GPL, az Apache vagy a BSD. Sokkal bonyolultabb megállapítani, hogy biztonságosan betehetek-e egy eszközt a WTE-be, mint ahogy arra számítottam. El sem tudod képzelni, hogy hány projektet kellett letöltenem és szétválogatnom, mielőtt rájöttem, hogy milyen licenst használ.

Egyetlen dolgot szeretnék üzeni a projekt rajongóinak: kérlek benneteket, hogy küldjétek javaslatokat, a panaszaitokat vagy bármit a levlistára vagy írjátok meg a gondolataitokat a projekt fórumán. A legegyszerűbb módja a projekt javításának, ha megtudjuk, hogy mi az ami működik, és mi az, ami nem.

**Új céges
támogatók
június-
júliusban—
köszönjük!**



**Kövess az
OWASP-ot**

**OWASP a
Twitteren:**

[http://
twitter.com/
statuses/
user_timeline/
16048357.rss](http://twitter.com/statuses/user_timeline/16048357.rss)

**Tudsz segíteni
abban, hogy
minden fe-
jlesztő értesül-
jön az OWASP
Top 10-ről?
Terjeszd ezt a
linket:**

[**OWASP Top 10 - 2010.pdf**](#)

ESAPI frissítés

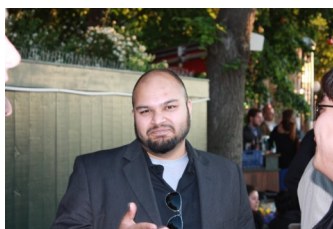
Jeff Williams

Az NSA felajánlotta, hogy elvégzi az ESAPI biztonsági felülvizsgálatát és publikálja az eredményeket. Ha valaki nem ismerné az NSA-t: a küldetésük egyik legfontosabb területe a védekezés. A múltban támogatták a National Computer Security Conference-t, megalkották a Rainbow Series-t, és szponzorálták az SSE-CMM-t. Mostanában a SCAP-on és az SE-Linuxon dolgoztak.

Az OWASP-ot támogató NSA csapat nagyon tapasztalt a kriptográfia és alkal-

mazások átvizsgálásának területén és hamarosan megkezdik a munkát. Először a Java ESAPI-n fognak dolgozni, majd ha végeztek, akkor talán más nyelvű verziókon is. Az előzetes becslések szerint több hónapot fog igénybe venni a munka.

Nagyon izgatott vagyok ezzel kapcsolatban és beszámolok majd a fejleményekről.



OWASP projekt frissítések

Paulo Coimbra, OWASP Project Manager

Új projektek

[http://www.owasp.org/index.php/Projects/
ESAPI_Swingset-](http://www.owasp.org/index.php/Projects/ESAPI_Swingset)

[http://www.owasp.org/index.php/Projects/
Owasp_Esapi_Ruby](http://www.owasp.org/index.php/Projects/Owasp_Esapi_Ruby)

[http://www.owasp.org/index.php/
OWASP_Application_Security_Program_for
_Managers](http://www.owasp.org/index.php/OWASP_Application_Security_Program_for_Managers)

Friss kiadással rendelkező projekt

[http://www.owasp.org/index.php/
OWASP_JavaScript_Sandboxes](http://www.owasp.org/index.php/OWASP_JavaScript_Sandboxes)

Új kiadáshoz közreműködőket kereső projekt

[http://www.owasp.org/index.php/
Cate-
gory:OWASP_Testing_Project#tab=Project_
About \(Testing Guide V 4.0\)](http://www.owasp.org/index.php/Catagory:OWASP_Testing_Project#tab=Project_About)

Újraindított projekt

[http://www.owasp.org/index.php/
OWASP_Related_Commercial_Services](http://www.owasp.org/index.php/OWASP_Related_Commercial_Services)

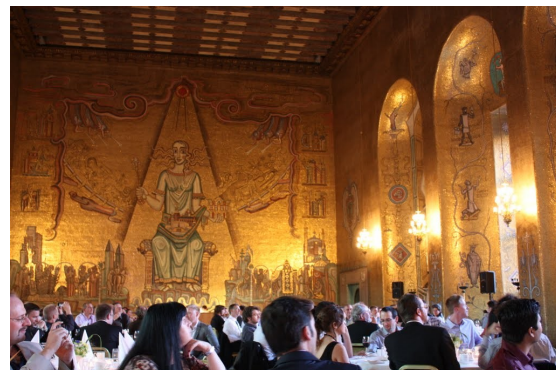
OWASP ESAPI Swingset—új vezető

Üdvözljük Cathal Courtney-t!

[http://www.owasp.org/index.php/
ESAPI_Swingset#tab=Project_About](http://www.owasp.org/index.php/ESAPI_Swingset#tab=Project_About)

Ennek a projektnek már van kiadása (ESAPI Swingset RC 4), amely épp most vált elérhetővé—nézzétek meg.

[http://www.owasp.org/index.php/Projects/
ESAPI_Swingset/Releases/Current](http://www.owasp.org/index.php/Projects/ESAPI_Swingset/Releases/Current)



OWASP Site

Google Analytics

Látogatók májusban: 233,765
 Oldalletöltések: 573,144
 Látogatásonkénti oldalak száma: 2.45
 Site-on eltöltött átlagos idő: 00:02:57
 58.3% új látogató
<http://conf.oss.my>
 Content overview:
/index.php/Main_Page 63,070 page views
</index.php/>
 Category:OWASP_Top_Ten_Project 21,610 oldalletöltés

OWASP O2 Platform

Dinis Cruz

Boldog vagyok, hogy bejelenthetem: elkészült az [OWASP O2 Platform](#) első fő kiadása (telepítővel, dokumentációval és videókkal és egy halom fontos/egyedi képességgel).

Teljesen új GUI van, ami nagyban megkönnyíti az O2-n belül elérhető scriptek, eszközök és API-k megtalálását (ha használtad ez előző verziót, akkor ezt nagyon fogod értékelni).

Itt megnézheted az új GUI-t és letöltheted a cuccot: http://www.o2platform.com/wiki/O2_Release/v1.1_Beta

[Kérem, hogy próbáljátok ki](#) és közöljétek, hogy mi tetszik, mi működik, mi nem működik, mit kellene javítani stb. Hibabejelentéshez ezt a webes felületet használjátok:

OWASP AppSec Research összefoglaló

John Wilander

Az európai OWASP AppSec konferencia június 21. és 24. között került megrendezésre Stockholm-ban. Három tagozat (a svéd, norvég és dán) a Stockholmi Egyetemmel karöltve rendezte az eseményt, amelyen 275 résztvevő tette tiszteletét.

Az első két napon oktatások folytak biztonságos fejlesztés, behatolási tesztek, malware elemzés és architektúráis átvizsgálás témakörökben. A hétfői közös vacsorán az amerikai vendégek megtanulták, hogyan kell hamburgert késsel és villával enni, ami egy svéd különlegesség :).

A konferencia három párhuzamos ágon folyt, előadókkal mind az iparból, mind az akadémiai szektorból. Vitaindító előadások hangzottak el a böngészőbiztonság jövőjéről és az SDL fejlődéséről a '90-es évektől kezdve. A szponzorok

</index.php/>
 Category:OWASP_WebScarab_Project
 16,615 oldalletöltés
[/index.php/Category:](/index.php/Category:OWASP_WebGoat_Project)
 OWASP_WebGoat_Project
 13,502 oldalletöltés
/index.php/Category:OWASP_Project
 10,915 oldalletöltés
 Leggyakoribb keresőkifejezések:
 Owasp, webcarb, owasp top 10, webgoat, sql injection.

<http://code.google.com/p/o2platform/issues/list>)

Az O2 ezen verziója már elég érett ahhoz, hogy bátran intézhessem felétek ezt a kérést, mivel tudom, hogy függetlenül attól, hogy valaki pontosan milyen webappsec területen tevékenykedik, biztosan lesz olyan O2 script, modul vagy eszköz, ami növeli a produktivitását.

Mivel az új GUI nagyon friss, a legtöbb [doksi](#) és [videó](#) az előző felülettel indul, de mivel most már könnyen tudok az O2-vel wiki oldalakat és/vagy videókat csinálni, azt tervezem, hogy a kérdésekre ilyen formában válaszolok majd (videóval vagy wiki bejegyzéssel).

kiállításán 12 cég vett részt, a gyémánt szponzor Microsoft vezetésével.

Szerda este a konferencia látogatói párjaikkal részt vettek a stockholmi Városházán tartott díszvacsorán. A vacsora közben az asztalok három kategóriában - kultúra, geek-ség és művészetek—versengtek pezsgőért. Utolsó feladatként csőtisztítókból kellett OWASP-ihletésű szobrot alkotni, amelynek során a csapatok nagyon kreatívnak bizonyultak (vagy csak a bor tette volna?).

Az OWASP AppSec Research konferencia szervezői ezúton is köszönik minden támogatónak és résztvevőnek a közreműködést.

Viszlát jövőre Dublinban!

Alkalmazásbiztonsággal kapcsolatos munkát keresel?

Nézz szét az [OWASP Job oldalon!](#)

Alkalmazásbiztonsággal kapcsolatos munkát kínálsz?

Keress [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 ismereteiken 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

