OWASP Live CD:
An open environment for web application security.

Matt Tesauro
OWASP Live CD Project Lead
OWASP Global Projects Committee
OWASP Board Member
matt.tesauro@owasp.org

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org
Presentation Overview

- Who are we and what's this OWASP Live CD thing anyway?

- Where are we now?

- Where are we going?

- What have you done for me lately?

- How can I get involved?
About Matt

- Varied IT Background
  - Developer, DBA, Sys Admin, Pen Tester, Application Security, CISSP, CEH, RHCE, Linux+

- Long history with Linux & Open Source
  - First Linux install ~1998
  - DBA and Sys Admin was all open source
  - Last full-time commercial OS = Windows 2000
  - Contributor to many projects, leader of one
General goals going forward

- Showcase great OWASP projects
- Provide the best, freely distributable application security tools/documents
- Ensure that the tools provided are easy to use as possible
- Continue to document how to use the tools and how the modules were created
- Align the tools with the OWASP Testing Guide v3 to provide maximum coverage
- Awesome training environment
Where are we now?

Current Release
- AppSecDC Nov 2009  DOH!

Previous Releases
- AppSecEU May 2009
- AustinTerrier Feb 2009
- Portugal Release Dec 2008
- SoC Release Sept 2008
- Beta1 and Beta2 releases during the SoC

Overall downloads = 330,081 (of 2009-10-05)
- ~5,094 GB of bandwidth since launch (Jul 2008)
- Most downloads in 1 month = 81,607 (Mar 2009)
Lets Google that...
Available Tools: 26 'Significant'

**OWASP Tools:**

**Web Scarab**
- a tool for performing all types of security testing on web apps and web services

**Web Goat**
- an online training environment for hands-on learning about app sec

**CAL9000**
- a collection of web app sec testing tools especially encoding/decoding

**JBroFuzz**
- a web application fuzzer for requests being made over HTTP and/or HTTPS.

**WSFuzzer**
- a fuzzer with HTTP based SOAP services as its main target

**Wapiti**
- audits the security of web apps by performing "black-box" scans

**DirBuster**
- a multi threaded Java app to brute force directory and file names

**SQLiX**
- a SQL Injection scanner, able to crawl, detect SQL-i vectors
<table>
<thead>
<tr>
<th>Other Proxies:</th>
<th>Scanners:</th>
<th>SQL-i:</th>
<th>Others:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burp Suite</td>
<td>w3af</td>
<td>sqlmap</td>
<td>Metasploit</td>
</tr>
<tr>
<td>Paros</td>
<td>Grendel Scan</td>
<td>SQL Brute</td>
<td>Httopt</td>
</tr>
<tr>
<td>Spike Proxy</td>
<td>Nikto</td>
<td></td>
<td>Maltego CE</td>
</tr>
<tr>
<td>Rat Proxy</td>
<td>namp</td>
<td>Firefox</td>
<td>netcat</td>
</tr>
<tr>
<td></td>
<td>Zenmap</td>
<td>Duh:</td>
<td>Wireshark</td>
</tr>
<tr>
<td></td>
<td>Fierce Domain Scanner</td>
<td></td>
<td>tcpdump</td>
</tr>
</tbody>
</table>
Its Demo time!

DEM0 AHEAD

Watch out for explosions and demo gremlins
There's a new kid in town

Web Testing Environment

image from:
http://www.gregoryeuclide.com/Euclide_RELIEF.html
What's this WTE thingie?

- The project has grown to more than just a Live CD
  - VMWare installs/appliances
  - VirtualBox installs
  - USB Installs
  - Training Environment
  - ....

- Add in the transition to Ubuntu and the possibilities are endless
  
  *(plus the 26,000+ packages in the Ubuntu repos)*
What OWASP WTE brings

Among the new ideas for WTE are

- Live CDs & Live DVDs
- Virtual installs/applicances
- A package repository
  - Can a 1+ tool to any Debian based Linux
  - `apt-get install owasp-wte-*`
- Custom remixes of any of the above
- Targeted installs
  - WebGoat Developer Version
- Wubi
- Kiosk version
Some WTE specifics

- Targeting Ubuntu
  - Specifically 9-04 for initial testing
  - Will test on other Debian variants too
  - Repository for apt-get'ing packages

- Each tool is its own self-contained package
  - Allows selective installs of the tools
  - OWASP menu dynamically grows/shrinks
  - Public svn

- OWASP WTE will initially produce
  - Live CD, VMware and VirtualBox installs
The WTE Hive

■ Me (duh)

■ Brad Causey
  ▶ Contributor to OWASP Live CD
    ▪ Maintains the virtual installs
      – Vmware & VirtualBox
    ▪ Creating packages for the next release

■ Drew Beebe
  ▶ Recent addition after AppSec DC
  ▶ Great packager and automation junkie

■ [Your Name Here]
  ▶ We're always looking for help
Its Demo time!

DEMO AHEAD

Watch out for explosions and demo gremlins
Documentation available

- OWASP Documents
  - Testing Guide v2 & v3
  - CLASP
  - Top 10 for 2007
  - Top 10 for Java Enterprise Edition
  - AppSec FAQ
  - Books

- Others
  - WASC Threat Classification, OSTTMM 3.0 & 2.2
Where are we going with WTE?

- The cool fun stuff ahead
  - Project Tindy
  - Project Aqua Dog
  - Builder vs Breaker
  - Auto-update installed tools
  - Website update
  - OWASP Education Project
  - Crazy Pie in the Sky idea
Project Tindy & Aqua Dog

Project Tindy
- OWASP Live CD installed to a virtual hard drive
- Persistence!
- VMWare, Virtual Box & Parallels

Project Aqua Dog
- OWASP Live CD on a USB drive
- VM install + VM engine + USB drive = mobile app sec platform
- Currently testing
- Qemu is the current VM engine
Builder vs Breaker

Builder is where the ROI is

But darn it, breaking is really fun.

Builder tools coming in future packages.

(Thanks Top Gear!)
Website Update

Quick, spell my last name...

Need a much easier URL – AppSecLive.org

- Community site around OWASP Live CD
  - Forums, articles, screen casts, etc

- Online Tool database
  - Seeded with the 331 I've already got

- Articles and HowTos published by users
- www.owasp.org will *always* be its home
- AppSecLive allows us to go beyond wiki
To establish a community around the OWASP Live CD and Web Application Security.

Welcome

Welcome to AppSecLive.org! We are an online community focused on, you guessed it, web application security. We welcome all folks from all arenas to join us in discussing everything from tools to techniques relating to the security of the web. WebAppSec.org is also the new home of the OWASP Live CD, which is maintained by Matt Tesauro. This is where you will find support for the OWASP Live CD.

A few quick pointers:

Creating a VirtualBox Image from the OWASP Live CD

Creating a VirtualBox image from the OWASP Live CD

I’d like to thank Kort (if you know him, you know him), if not, don’t worry about it) for the early versions of this document and for working out the kinks early on. You’ve been an amazing help to our virtualization efforts.

A few notes on this tutorial.

We’ve done this so you don’t have to.

Making the Sqlmap Module

Submitted by miszuso on Sat, 05/03/2009 - 15:03

Get the source for sqlmap

Go to the sqlmap website and grab the latest source tarball. In this case, that is sqlmap-0.7rc1.tar.gz.

Yes, its a release candidate but per the site, it works fine on Linux. That’s what we’re using so no worries.
Going forward with WTE

Design goals

- Easy for users to keep updated
- Easy for project lead to keep updated
- Easy to produce releases (every 6 months)
  - Crank out new .debs when new tool releases
  - Continually updating repository
- Focused on just application security – not general pen testing
  - Both dynamic and static tools
  - Developer tools also
Natural ties between these projects

- Already being used for training classes
- Need to coordinate efforts to make sure critical pieces aren't missing from WTE
- Training environment could be customized for a particular class thanks to the individual modules
  - Student gets to take the environment home
- As more packages get built, even more potential for cross pollination
- Builder tools/docs only expand its reach
- All of OWASP on a DVD?
My Crazy Pie in the Sky idea

- .deb package + auto update + categories = install profiles
  - Allows someone to customize the OWASP Live CD to their needs
  - Example profiles
    - Whitebox testing
    - Blackbox testing
    - Static Analysis
    - Target specific (Java, .Net, ...)
  - Profile + VM = custom persistent work environment
So what will WTE do for me?

- **For Testers / QA testers**
  - Wide array of tools, pre-configured and ready
  - Nice “jump kit” to keep in your laptop bag
  - Great platform to test or learn the tools

- **For App Sec Professionals**
  - Both dynamic and static tool coverage
  - Ability to customize the job you’re on

- **For Trainers**
  - Ready to go environment for students
  - Ability to customize for the class
How can you get involved?

- Join the mail list
  - Announcements are there – low traffic
- Post on the AppSecLive.org forums
- Download an ISO or VM
  - Complain or praise, suggest improvements
  - Submit a bug to the Google Code site
- Create deb package of a tool
  - How I create the debs will be documented, command by command and I'll answer questions gladly
- Suggest missing tools, docs or links
- Do a screencast of one of the tools being used on the OWASP Live CD
Learn More

- **OWASP Site:**
  or Google “OWASP Live CD”

- **Download & Community Site:**
  [http://AppSecLive.org](http://AppSecLive.org)

- **Google Code Site:**

- **Original site:** [http://mtesauro.com/livecd/](http://mtesauro.com/livecd/)
## OWASP WTE Synaptic Pride...

<table>
<thead>
<tr>
<th>Package</th>
<th>Installed Version</th>
<th>Latest Version</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>owasp-wte-burpsuite</td>
<td>1.2</td>
<td></td>
<td></td>
<td>Burp Suite is an integrated platform for attacking web applications.</td>
</tr>
<tr>
<td>owasp-wte-cal9000</td>
<td>2.0</td>
<td></td>
<td></td>
<td>CAL9000 is a collection of web application security testing tools.</td>
</tr>
<tr>
<td>owasp-wte-dirbuster</td>
<td>0.12</td>
<td></td>
<td></td>
<td>DirBuster is a multi-threaded Java application design flaw finder.</td>
</tr>
<tr>
<td>owasp-wte-doc</td>
<td>1.0</td>
<td></td>
<td></td>
<td>This package includes OWASP Documentation.</td>
</tr>
<tr>
<td>owasp-wte-fierce</td>
<td>1.0.3</td>
<td></td>
<td></td>
<td>Fierce is not an IP scanner.</td>
</tr>
<tr>
<td>owasp-wte-grendel-scan</td>
<td>1.0</td>
<td></td>
<td>0 B</td>
<td>Grendel-Scan is an open-source web application security tool.</td>
</tr>
<tr>
<td>owasp-wte-httpprint</td>
<td>1.0</td>
<td></td>
<td>301</td>
<td>htprint is a web server fingerprinting tool.</td>
</tr>
<tr>
<td>owasp-wte-jbrofuzz</td>
<td>1.2</td>
<td></td>
<td></td>
<td>JBroFuzz is a web application fuzzer for requests being sent to a protected web server.</td>
</tr>
<tr>
<td>owasp-wte-maltego</td>
<td>2.0</td>
<td></td>
<td></td>
<td>Maltego is an open-source intelligence and forensics tool.</td>
</tr>
<tr>
<td>owasp-wte-metasploit</td>
<td>3.3.3</td>
<td></td>
<td></td>
<td>Metasploit provides useful information to people who need to use or exploit software flaws.</td>
</tr>
<tr>
<td>owasp-wte-netcat</td>
<td>0.7.1</td>
<td></td>
<td></td>
<td>Netcat is a featured networking utility.</td>
</tr>
<tr>
<td>owasp-wte-nikto</td>
<td>2.0.3</td>
<td></td>
<td></td>
<td>Nikto is an Open Source web server scanner.</td>
</tr>
<tr>
<td>owasp-wte-nmap</td>
<td>4.76</td>
<td></td>
<td></td>
<td>Nmap is a free and open source utility for network exploration.</td>
</tr>
<tr>
<td>owasp-wte-paros</td>
<td>3.2.13</td>
<td>3.2.13</td>
<td>0 B</td>
<td>Paros is a proxy that intercepts and modifies all HTTP and HTTPS requests.</td>
</tr>
<tr>
<td>owasp-wte-ratproxy</td>
<td>1.5.3beta</td>
<td>1.57+dfsg</td>
<td>0 B</td>
<td>SpikeProxy is a professional-grade tool for looking for vulnerabilities.</td>
</tr>
<tr>
<td>owasp-wte-spikeproxy</td>
<td>1.4.8</td>
<td></td>
<td></td>
<td>SQLBrute is a tool for brute forcing data out of databases.</td>
</tr>
<tr>
<td>owasp-wte-sqlbrute</td>
<td>1.0</td>
<td></td>
<td></td>
<td>SQLiX is a SQL injection scanner.</td>
</tr>
<tr>
<td>owasp-wte-sqldump</td>
<td>0.7rc1</td>
<td></td>
<td></td>
<td>sqldump is an open-source command-line automatic SQL injection tool.</td>
</tr>
<tr>
<td>owasp-wte-sqmap</td>
<td>4.0.0</td>
<td></td>
<td></td>
<td>Tcpdump prints out a description of the contents of packets.</td>
</tr>
<tr>
<td>owasp-wte-w3af</td>
<td>1.2</td>
<td></td>
<td></td>
<td>w3af is a Web Application Attack and Audit Framework.</td>
</tr>
<tr>
<td>owasp-wte-w3af-console</td>
<td>1.2</td>
<td></td>
<td></td>
<td>w3af is a Web Application Attack and Audit Framework.</td>
</tr>
<tr>
<td>owasp-wte-wapiti</td>
<td>2.0.0</td>
<td></td>
<td></td>
<td>Wapiti allows you to audit the security of your web applications.</td>
</tr>
<tr>
<td>owasp-wte-webgoat</td>
<td>5.2</td>
<td></td>
<td>0 B</td>
<td>WebGoat is an online training environment for hands-on practice.</td>
</tr>
<tr>
<td>owasp-wte-webscarab</td>
<td>20090122</td>
<td>20090122</td>
<td></td>
<td>WebScarab is a local proxy for web application testing.</td>
</tr>
<tr>
<td>owasp-wte-wireshark</td>
<td>1.0.7-1ubuntu1</td>
<td></td>
<td></td>
<td>Wireshark is a network traffic analyzer, or “sniffer”, for protocol analysis.</td>
</tr>
<tr>
<td>owasp-wte-ws fuzzer</td>
<td>1.9.4</td>
<td></td>
<td></td>
<td>WSFuzzer currently targets Web Services.</td>
</tr>
</tbody>
</table>
OWASP WTE is OPEN

Add will always be...
Questions?
the BIG commit

<table>
<thead>
<tr>
<th>File</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/parseLocationPath.py</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/parsePredicateList.py</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/parseStep.py</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/parseSet.py</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/parseUtil.py</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/xpathGrammar.py</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/xpathParser.py</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/xpathParserBase.py</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/share/layouts/wsfuzzr.desktop</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/share/applications/wsfuzzr.desktop</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/share/applications/wsfuzzr.web ordinances</td>
</tr>
<tr>
<td>Adding</td>
<td>conversion/wsuzer/contents/usr/share/applications/wsfuzzr-xmap</td>
</tr>
<tr>
<td>Adding (bin)</td>
<td>conversion/wsuzer/contents/usr/share/applications/wsfuzzr-icon.png</td>
</tr>
</tbody>
</table>

Transmitting file data...
First package test install

Unpacking unixodbc (from .../unixodbc_2.2.11-16build3_i386.deb) ...
Selecting previously deselected package sun-java6-bin.
Unpacking sun-java6-bin (from .../sun-java6-bin_6-16-0ubuntu1.9.04_i386.deb) ...
sun-dlj-v1.1 license has already been accepted
Selecting previously deselected package gsfonts-x11.
Unpacking gsfonts-x11 (from .../gsfonts-x11_0.21_all.deb) ...
Selecting previously deselected package owasp-wte-paros.
Unpacking owasp-wte-paros (from .../owasp-wte-paros-3.2.13-1_all.deb) ...
Processing triggers for doc-base ...
Processing 2 added doc-base file(s)...
Registering documents with scrollkeeper...
Processing triggers for man-db ...
Processing triggers for shared-mime-info ...
Setting up java-common (0.39ubuntu4) ...
Setting up odbcinst1debian1 (2.2.11-16build3) ...
Setting up unixodbc (2.2.11-16build3) ...
Setting up gsfonts-x11 (0.21) ...
Setting up sun-java6-jre (6-16-0ubuntu1.9.04) ...
Setting up owasp-wte-paros (3.2.13) ...
Setting up sun-java6-bin (6-16-0ubuntu1.9.04) ...
Processing triggers for libc6 ...
lviewconfig deferred processing now taking place
root@owasp-wte:/var/owasp/apt# apt-get install owasp-wte-paros
First package fail

```
root@owasp-wte: /var/owasp/apt

Unpacking unixodbc (from .../unixodbc_2.2.11-16build3_i386.deb) ...
Selecting previously deselected package sun-java6-bin.
Unpacking sun-java6-bin (from .../sun-java6-bin_6.16-0ubuntu1.9.04_i386.deb)
sun-dlj-v1-1 license has already been.
Selecting previously deselected package gsfonts-x11.
Unpacking gsfonts-x11 (from .../gsfonts-x11_0.21)
Selecting previously deselected package sun-java6-jre.
Processing triggers for libc6 ...
```

Could not launch 'Paros'

Text was empty (or contained only whitespace)
Yeah, genuine alright