Testing from the Cloud: Is the sky falling?

Matt Tesauro
OWASP Foundation Board Member, WTE Project Lead
matt.tesauro@owasp.org

“In between Jobs”
Soon to be at Rackspace
Who's this Matt guy anyway?

- **Broad IT background**
  Developer, DBA, Sys Admin, Pen Tester, Application Security professional, CISSP, CEH, RHCE, Linux+

- **Long history with Linux and Open Source**
  Contributor to many projects
  Leader of OWASP Live CD / WTE

- **OWASP Foundation Board Member**

**FUNEMPLOYED**
OWASP WTE: A History

from Paulo Coimbra <paulo.coimbra@owasp.org>  
to OWASP - ALL <owasp-all@lists.owasp.org>  
date Tue, Mar 4, 2008 at 1:33 PM  
mailing list owasp-all.lists.owasp.org Filter messages from this mailing list

OWASP Summer of Code 2008 - Sponsorship Initiative

- The OWASP Summer of Code 2008 (SoC 2008) aims to financially sponsor contributions to OWASP Projects. SoC 2008 follows the previous OWASP Spring of Code 2007, in which 21 projects were sponsored with a budget of $117,500, and the OWASP Autumn of Code 2006, in which 9 projects were sponsored with a budget of $20,000.

- The SoC 2008 is an open sponsorship program were participants/developers are paid to work on OWASP (and web security) related projects.

- The SoC 2008 is also an opportunity for external individual or company sponsors to challenge the participants/developers to work in areas in which they are willing to invest additional funding, provided that these areas are relevant and beneficial to the OWASP community.

- The initial Budget for SoC 2008 will be $100,000 and it is funded by OWASP using current membership fees and profits from past conferences. In parallel with the Request for Proposals, OWASP would like to invite individuals and companies that benefit from OWASP projects to join OWASP as a member. In addition to the current Membership benefits, the new OWASP members will be able to allocate membership fees to SoC 2008 projects they are interested in.

- There is no geographical, age or any other form of restrictions to who can apply for an "OWASP Summer of Code 2008" sponsorship. The only requirement is that the candidate shows the potential to accomplish the project’s objectives and the commitment to dedicate the time required to complete it in the allocated time frame (projects must be completed by 30th August 2008).

- Prospective candidates should visit SoC 2008 page for more information.
At all started that summer...

**OWASP Live CD 2008 Project**

- **Matt Tesauro**

**Introduction**

The previous OWASP Live CD project distributions have laid a good foundation for the 2008 Project. I'd like to take the existing Live CD and further enhance it. I see the 2008 Live CD as filling the Web App Sec niche not the more general Pen Tester niche. I'd concede general Pen Testing to Backtrack [19]. However, Backtrack has a different audience and is not specifically tailored for web application security professionals. This is the role I think this Live CD could fulfill with great success. I'd like to take the OWASP Live CD 2008 Project in that direction and see the OWASP Live CD become to Web App Sec what Backtrack is to Pen Testing.

**Proposal**

I'd like to take the existing applications and documentation in the current Live CD and add significantly more tools and documentation specifically focused on Web application security. I think OWASP's Phoenix/Tools page [20] would be a good starting point for potential tools. I'd also like to use WASC [21] and ISECON/OSSTMM [22] as sources for material.

The project would first enumerate a list of tools to include on the CD where licensing, supported OS and space will determine what is included on the Live CD. After determining a reasonable list of tools, the next phase would be to create modules for the tools and merge these modules with the Live CD. Then documentation and tutorials would be added (also as space allows) followed by any remaining OWASP branding. Additional polishing could include pre-installation (license permitting) of the VMware tools.

**Deliverables**

- April 2 to May 15, 2008
  - Enumerated tools and reference material for installation verifying that the software license allows permits distribution.
- May 16 to July 4, 2008
  - Create modules for each tool and begin to merge the modules with the base distribution.
  - Begin testing of the Live CD.
- July 5 to August 31, 2008
  - Complete the merging of modules and install any remaining documentation.
  - Further testing of the Live CD particularly installation of new/updated modules.

**Challenges / Outstanding Issues**

While the current Live CD is based on Morphix – a Knoppix derivative created to allow easy creation of custom Live CDs, I'm not sure it provides the flexibility needed to keep the CD tools updated. While I'm fine with keeping the Live CD on Morphix, I also see value in switching to another distribution: SLAX. Here's the brief pros and cons of each as I see them.

**Pros of Morphix:**

- no change to current LiveCD - principally just updates to existing and augment.
• Current Release
  • OWASP WTE Sept 2011

• Previous Releases
  • OWASP WTE Feb 2011
  • OWASP WTE Beta Jan 2010
  • AppSecEU May 2009
  • AustinTerrier Feb 2009
  • Portugal Release Dec 2008
  • SoC Release Sept 2008
  • Beta1 and Beta2 releases during the SoC

Note: Not all of these had ISO, VirtualBox and Vmware versions
Overall downloads: 330,081 (as of 2009-10-05)

Other fun facts

- ~5,094 GB of bandwidth since launch (Jul 2008)
- Most downloads in 1 month = 81,607 (Mar 2009)
There's a new kid in town

OWASP WTE

Web Testing Environment
The project has grown to more than just a Live CD

- VMWare installs/appliances
- VirtualBox installs
- USB Installs
- Training Environments
- Cloud???

Add in the transition to Ubuntu/Debian and the possibilities are endless (plus the 26,000+ packages in the repos)
GOAL

Make application security tools and documentation easily available and easy to use

- Compliment's OWASP goal to make app security visible

Design goals

- Easy for users to keep updated
- Easy for project lead to keep updated
- Easy to produce releases (more on this later)
- Focused on just application security – not general pen testing
What's on WTE
29 “Significant” Tools Available

**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.

**EnDe**
- An amazing collection of encoding and decoding tools as well as many other utilities

**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

**WebSlayer**
- A tool designed for brute-forcing web applications such as resource discovery, GET and POST fuzzing, etc

**ZAP Proxy**
- A fork of the popular but moribund Paros Proxy
Other Proxies:
- Burp Suite
- Paros
- Spike Proxy
- Rat Proxy

Scanners:
- w3af
- Grendel Scan
- Nikto
- nmap
- Zenmap
- Fierce Domain Scanner

SQL-i:
- sqlmap
- SQL Brute
- Duh:

Others:
- Metasploit
- Httprint
- Maltego CE
- netcat
- Wireshark
- tcpdump
Why is it different?
<table>
<thead>
<tr>
<th>Add N Edit Cookies 0.2.1.3</th>
<th>No-Referer 1.3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookie Editor that allows you add and edit se</td>
<td>Lets you open a tab without sending the HTTP referer information.</td>
</tr>
<tr>
<td>CookiePie 1.0.2</td>
<td>NoScript 1.9.2.6</td>
</tr>
<tr>
<td>Use multiple Web accounts and profiles in dif</td>
<td>Extra protection for your Firefox: NoScript allows JavaScript, Java (and other plu…</td>
</tr>
<tr>
<td>DOM Inspector 2.0.3</td>
<td>POW 0.1.8</td>
</tr>
<tr>
<td>Inspects the structure and properties of a win</td>
<td>A personal Web Server</td>
</tr>
<tr>
<td>Firebug 1.3.3</td>
<td>RefControl 0.8.11</td>
</tr>
<tr>
<td>Web Development Evolved.</td>
<td>Control what gets sent as the HTTP Referer on a per-site basis.</td>
</tr>
<tr>
<td>FormFox 1.6.3</td>
<td>refspoof 0.9.5</td>
</tr>
<tr>
<td>Pops up form action when submit button is al</td>
<td>Allows easy spoofing of URL referer (referrer) w/ toolbar.</td>
</tr>
<tr>
<td>FoxyProxy 2.9</td>
<td>Server Switcher 0.5</td>
</tr>
<tr>
<td>FoxyProxy - Premier proxy management for Fi</td>
<td>Switch between your development and live servers.</td>
</tr>
<tr>
<td>Greasemonkey 0.8.20090123.1</td>
<td>SQL Injection! 1.2</td>
</tr>
<tr>
<td>A User Script Manager for Firefox</td>
<td>Set all form fields free to test SQL Injections.</td>
</tr>
<tr>
<td>HackBar 1.3.2</td>
<td>Tamper Data 10.1.0</td>
</tr>
<tr>
<td>A toolbar that helps you find and test SQL inj</td>
<td>View and modify HTTP/HTTPS headers etc. Track and time requests.</td>
</tr>
<tr>
<td>Header Spy 1.3.3.1</td>
<td>TestGen4Web - Script It All 1.0.0</td>
</tr>
<tr>
<td>Shows HTTP headers on statusbar</td>
<td>Just like your VCR - for Firefox. It records what you do, stores it, and plays it bac…</td>
</tr>
<tr>
<td>InspectThis 0.9.1</td>
<td>UrlParams 2.2.0</td>
</tr>
<tr>
<td>Inspect the current element with the DOM Ins</td>
<td>Displays GET/POST parameters in the sidebar.</td>
</tr>
<tr>
<td>JSView 2.0.5</td>
<td>User Agent Switcher 0.6.11</td>
</tr>
<tr>
<td>View the source code of external styleheets</td>
<td>Adds a menu and a toolbar button to switch the user agent of the browser.</td>
</tr>
<tr>
<td>Live HTTP headers 0.14</td>
<td>Web Developer 1.1.6</td>
</tr>
<tr>
<td>View HTTP headers of a page and while brow</td>
<td>Adds a menu and a toolbar with various web developer tools.</td>
</tr>
</tbody>
</table>
Use proxies based on their pre-defined patterns and priorities

- Use proxy "Spike Proxy" for all URLs
- Use proxy "Paros Proxy" for all URLs
- Use proxy "Grendel Scan" for all URLs
- Use proxy "w3af spiderman discovery plugin" for all URLs
- Use proxy "Ratproxy" for all URLs
- Use proxy "Burp Suite" for all URLs
- **Use proxy "WebScarab" for all URLs**
- Use proxy "Default" for all URLs
- Completely disable FoxyProxy
- OWASP Documents
  - Testing Guide v2 & v3
  - CLASP and OpenSamm
  - Top 10 for 2010
  - Top 10 for Java Enterprise Edition
  - AppSec FAQ
  - Books – tried to get all of them
- Others
  - WASC Threat Classification, OSTTMM 3.0 & 2.2
Index of /apt/stable

- Parent Directory
- Packages.gz
- README
- owasp-wte-burpsuite-1.3.03-1_all.deb
- owasp-wte-cal9000-2.0-1_all.deb
- owasp-wte-ende-1.0rc3-1_all.deb
- owasp-wte-fierce-1.0.3-1_all.deb
- owasp-wte-firefox-3.6-1_i386.deb
- owasp-wte-grendel-scan-1.0-1_all.deb
- owasp-wte-httpprint-301-1_all.deb
- owasp-wte-jbrofuzz-2.4-1_all.deb
- owasp-wte-maltego-3.0-1_all.deb
- owasp-wte-metasploit-3.5.1-1_all.deb
- owasp-wte-netcat-0.7.1-1_all.deb
- owasp-wte-nikto-2.1.2-1_all.deb
- owasp-wte-nmap-5.00-1_all.deb
- owasp-wte-paros-3.2.13-1_all.deb
- owasp-wte-ratproxy-1.58-1_all.deb
- owasp-wte-spikeproxy-1.4.8-1_all.deb
- owasp-wte-sqlbrute-1.0-1_all.deb
- owasp-wte-sqlmap-0.8-1_all.deb
- owasp-wte-tcpdump-4.0.0-1_all.deb
- owasp-wte-w3af-1.0~rc2svn3180-1_all.deb
- owasp-wte-w3af-console-1.0~rc2svn3180-1_all.deb
- owasp-wte-w3af-svn-3909-1_all.deb
- -
Index of /apt/testing

- Parent Directory
- Packages.gz
- README
- owasp-wte-sqlix-1.0-1_all.deb

Apache Server at appseclive.org Port 80
<table>
<thead>
<tr>
<th>S</th>
<th>Package</th>
<th>Installed Version</th>
<th>Latest Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>owasp-wte-netcat</td>
<td>0.7.1</td>
<td></td>
<td>Netcat is a featured networking utili...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-nikto</td>
<td>2.1.2</td>
<td>2.1.2</td>
<td>Nikto is an Open Source web server...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-nmap</td>
<td>5.00</td>
<td></td>
<td>Nmap is a free and open source utili...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-paros</td>
<td>3.2.13</td>
<td></td>
<td>Paros proxy intercepts and modifies</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-ratproxy</td>
<td>1.58</td>
<td></td>
<td>A semi-automated, largely passive w...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-spikeproxy</td>
<td>1.4.8</td>
<td></td>
<td>SPIKE Proxy is a professional-grade...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-sqlbrute</td>
<td>1.0</td>
<td></td>
<td>SQLBrute is a tool for brute forcing</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-sqlmap</td>
<td>0.8</td>
<td></td>
<td>sqlmap is an open source command...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-tcpdump</td>
<td>4.0.0</td>
<td></td>
<td>Tcpdump prints out a description of...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-w3af</td>
<td>svn-4041</td>
<td></td>
<td>w3af is a Web Application Attack an...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-wapiti</td>
<td>2.2.1</td>
<td></td>
<td>Wapiti allows you to audit the securi...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-webgoat</td>
<td>5.3-RC1</td>
<td></td>
<td>WebGoat is an online training environ...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-webscarab</td>
<td>20090122</td>
<td></td>
<td>WebScarab: a local proxy for web ap...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-webslayer</td>
<td>svn-r4</td>
<td>svn-r4</td>
<td>WebSlayer is a tool designed for brute...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-wireshark</td>
<td>1.2.7</td>
<td></td>
<td>Wireshark is a network traffic analyz...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-wsfuzzer</td>
<td>1.9.4</td>
<td></td>
<td>WSFuzzer currently targets Web Ser...</td>
</tr>
<tr>
<td></td>
<td>owasp-wte-zap</td>
<td>1.2.0</td>
<td>1.2.0</td>
<td>The OWASP Zed Attack Proxy (ZAP)</td>
</tr>
</tbody>
</table>

**WebSlayer** is a tool designed for brute forcing Web Applications.

Get Screenshot

it can be used to discover not linked resources (directories, servlets, scripts, etc), brute force GET and POST parameters, brute force forms parameters (User/Password), fuzzing, etc. The tool has a powerful payload generator and a easy and flexible results analyzer.

27 packages listed, 1695 installed, 0 broken. 0 to install/upgrade, 0 to remove
The WTE version of Firefox comes packed with App Sec addons.
owasp-wte-firefox

The OWASP Zed Attack Proxy (ZAP) is an easy to use integrated
owasp-wte-zap

EnDe - Encoder, Decoder, Converter, Calculator, TU WAS DU WILST..
owasp-wte-ende

Nmap is a free and open source utility for network exploration or security auditing.
owasp-wte-nmap

Paros proxy intercepts and modifies all HTTP and HTTPS data between server and client.
owasp-wte-paros

Tcpdump prints out a description of the contents of packets on a network interface.
owasp-wte-tcpdump

WebGoat is an online training environment for hands-on learning
owasp-wte-webgoat

WSFuzzer currently targets Web Services.
owasp-wte-wsfuzzer

Grendel-Scan is an open-source web application打架 at aiding manual penetration tests.
owasp-wte-grendel-scan

JBroFuzz is a web application fuzzer for requests being made over HTTP or HTTPS.
owasp-wte-jbrofuzz

w3af is a Web Application Attack and Audit Framework. The project's
owasp-wte-w3af

Burp Suite is an integrated platform for attacking and auditing an application.
owasp-wte-burpsuite

CAL9000 is a collection of web application security testing tools
owasp-wte-cal9000

Wireshark is a network traffic analyzer, or ... for Unix and Unix-like operating systems.
owasp-wte-wireshark

Nikto is an Open Source web server scanner.
owasp-wte-nikto
The overarching goal for this project is to make application security tools and documentation easily available. I see this as a great complement to OWASP’s goal to make application security visible.

The project has several other goals going forward:

1. Provide a showcase for great OWASP tools and documentation
2. Provide the best, freely distributable application security tools in an easy to use package
3. Ensure that the tools provided are as easy to use as possible.
4. Continue to add documentation and tools to the OWASP WTE
5. Continue to document how to use the tools and how the tool modules were created.
6. Align the tools provided with the OWASP Testing Guide

This project will create several versions of the Testing Environment: A Live CD, VMs (VMware & Virtualbox), a Live DVD, etc.

Additionally, all the tools will be packaged as .deb packages.
#!/bin/bash
#
# Script written by Matt Tesauro <matt.tesauro@owasp.org>
# as part of the OWASP Live CD project
#
# This file, webscarab, is part of the .deb package created for use
# on the OWASP Live CD.
#
# webscarab is free software: you can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation, either version 3 of the License, or
# (at your option) any later version.
#
# webscarab is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with webscarab. If not, see <http://www.gnu.org/licenses/>.
#
# Tue, 12 Jan 2010 21:40:21 -0600
#
# This script was written with help from:
# http://www.linuxjournal.com/article/10495
# http://www.linuxquestions.org/questions/programming-9/bash-how-to-handle-options-480081.html
# and the zenity man page
#
# Set some sane defaults
# RAM="64"
# PROMPT="false"
# SAVE="false"
#
# Setup command line option parsing
#
What is next?
Cloud-ifying WTE

- Cloud Provider
- Ubuntu / Debian Install
- WTE Repository
- Fun ensues
WTE Cloud - The 12 Step Program

- Currently this is all manual
- 12 steps to get a fully-functional WTE
- ~30 minutes until you are logged in
Step 1: Get a cloud account
Step 2: Select Ubuntu/Debian
Step 3: Choose Name & RAM
Step 4: Start your server
Step 5: Install Desktop + WTE

```
```

Step 6: More installs

- Add Repos & apt-get update
  - Ubuntu partners & WTE
- Add a NX Server
  - ppa:freenx-team (plus a fix)
- Add OWASP user
- Start GDM
Step 7: NX Client setup
Step 8: Connect to WTE
Step 9: WTE ala Cloud
Step 10: Test Connectivity
Step 11: Test the Tools
Turn Cats into Dogs

Dog

From Wikipedia, the free encyclopedia

Redirected from Dogs

For other uses, see Dog (disambiguation).

The domestic dog (Canis lupus familiaris) and Canis lupus dirigo is a domesticated form of the gray wolf, a member of the Canidae family of the order Carnivora. The term is used for both feral and pet varieties. The dog may have been the first animal to be domesticated, and has been the most widely kept working, hunting, and companion animal in human history. The word "dog" may also mean the male of a canine species, as opposed to the word "bitch" for the female of the species.

Dogs were domesticated from gray wolves about 15,000 years ago. They must have been very valuable to early human settlements, for they quickly became ubiquitous across world cultures. Dogs perform many roles for people, such as hunting, herding, pulling loads, protection, assisting police and military, companionship, and, more recently, aiding handicapped individuals.
Step 12: Check your bill

Cloud Servers Usage Summary

Total Uptime uses the following format: Days Hours:Minutes:Seconds

<table>
<thead>
<tr>
<th>1 Servers (Showing 1 to 1)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Disk Space (GB)</td>
<td>Bandwidth In (GB)</td>
<td>Bandwidth Out (GB)</td>
<td>Total Uptime</td>
<td>Running Charges</td>
<td></td>
</tr>
<tr>
<td>wte-test</td>
<td>80</td>
<td>1.13</td>
<td>0.02</td>
<td>0 Day(s) 01:53:54</td>
<td>$0.23</td>
<td></td>
</tr>
</tbody>
</table>
Cost Estimates

Operating System:
- Linux
- Windows (Minimum size of 1024MB for Windows)

Add Managed Service Level (What is this?)
(Adds $0.12 per hour per server plus a flat $100/month account fee)

Server Size (Memory in Megabytes)

Number of Servers: 1
Monthly Hours of Service: 40 hr
Number of Red Hat Servers: 0
Outgoing Bandwidth: 1 GB
Estimated Monthly Total: $4.98
Cost Estimates

- Estimated for 40 hours + 1 GB transfer = $4.98
- Estimated for M-F by 24 hours + 1 GB transfer = $15.48
- Estimated 30 days by 24 hours + 4 GB transfer = $88.32
Now what?
More Automation

- Create a wte-cloud package
  - Wraps up all tools into 1 package
- Make configuration steps into a script
  - Add to postinst for wte-cloud package
- Get setup down to a single step
  - Ideally all in the wte-cloud package
Even More Automation

Apache Libcloud

- Python library to abstract away differences between multiple cloud provider APIs
  - Cloud Servers
  - Cloud Storage
  - Cloud Load balancers
- Supports 24 different providers
More Options

- Different desktop installs
  - Minimal
  - Baseline
- Instant WebGoat in the sky
- Internal Clouds
  - OpenStack, Vmware, VirtualBox (headless)
Document, Document, Document

- Document and post the current manual process (next week)

- Create then document the Libcloud process

- Tutorials for various providers
Problems
Current Issues

- Yikes AMD64 CPU
  - sqlmap is missing a dependency
  - WTE Firefox is for i386
  - NX server is a bit tricky
- The WTE theme gets lost
How can you get involved?

- Join the OWASP mail list
  - Announcements are there – low traffic

- Download an ISO or VM or Cloud instance
  - Complain or praise, suggest improvements
  - Submit a bug to the Google Code site
How can you get involved?

- Suggest missing doc or links
- Do a screencast of one of the tools
- Suggest some cool new tool
- Create a .deb package
Learn More...

**OWASP Site**


or just look on the OWASP project page (release quality)

http://www.owasp.org/index.php/Category:OWASP_Project

or Google “OWASP Live CD”

**Download & Community Site**

http://AppSecLive.org

Previously:  http://mtesauro.com/livecd/
Why do I do this?
Questions?

Download it free at:

http://www.sintel.org

Sintel

Independent film produced by the Blender Foundation using free and open software