OWASP WTE: Testing your way.

Matt Tesauro
OWASP Foundation Board Member, WTE Project Lead
matt.tesauro@owasp.org
Vice President, Services for Praetorian
matt.tesauro@praetorian.com
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**

- **VP, Services for Praetorian**
OWASP WTE: A History
At all started that summer...
• Current Release
  • OWASP WTE Feb 2011

• Previous Releases
  • 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)
The OWASP Live CD project was originally started to update the previous OWASP Live CD 2007. The project met the September 15th, 2008 deadline for the OWASP ...

Category:OWASP Live CD Project - OWASP

Aug 28, 2009 ... The OWASP Live CD also contains documentation and an ...

Category:OWASP Live CD 2008 Project - OWASP

Aug 28, 2009 ... Executive Summary: I am proposing a new project that will ...

Category:OWASP LiveCD Education Project - OWASP

Aug 28, 2009 ... Executive Summary: I am proposing a new project that will ...

Owasp-live-cd-2008-project Info Page

The OWASP Live CD 2008 project is focused on creating a Linux-based live CD ...

AppSecLive.org

A community around the OWASP Live CD and Web Application Security. ... AppSecLive.org is also the new home of the OWASP Live CD, which is maintained by Matt ...
owasp wte - Google Search

About 4,400 results (0.28 seconds)

OWASP Web Testing Environment (WTE) Preview - Part 1 | AppSecLive.org
Jan 4, 2010 ... So, we're finalizing some stuff for the OWASP Live CD (which is now being renamed to the OWASP Web Testing Environment (WTE)) and I wanted ...
appseclive.org/owasp-web-testing-environment-wte-preview-part-1 - Cached

AppSecLive.org
So, we're finalizing some stuff for the OWASP Live CD (which is now being ...
appseclive.org - Cached

owasp-wte - Project Hosting on Google Code
Continue to add documentation and tools to the OWASP WTE; Continue to document how to use the tools and how the tool modules where created. ...
code.google.com/p/owasp-wte - Similar

OWASP DHS SWA Day 2010 OWASP WTE - OWASP
Oct 22, 2010 ... The OWASP Web Testing Environment (WTE) is the new name of the DVD which includes 26 significant tools. WTE also includes Firefox security ...
www.owasp.org/owasp_dhs_swa_day_2010_owasp_wte - Cached

Dallas - OWASP
Title: OWASP WTE: Application Pen Testing your way. ... In this talk I will ...
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 Environment
- ....

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

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

- Compliment's OWASP goal to make application 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
20 “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:
- Firefox

Others:
- Metasploit
- Httprint
- Maltego CE
- netcat
- Wireshark
- tcpdump
Why is it different?
<table>
<thead>
<tr>
<th>Extension</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No-Referer</td>
<td>1.3.1</td>
<td>Lets you open a tab without sending the HTTP referer information.</td>
</tr>
<tr>
<td>NoScript</td>
<td>1.9.2.6</td>
<td>Extra protection for your Firefox: NoScript allows JavaScript, Java (and other plu...</td>
</tr>
<tr>
<td>POW</td>
<td>0.1.8</td>
<td>A personal Web Server</td>
</tr>
<tr>
<td>RefControl</td>
<td>0.8.11</td>
<td>Control what gets sent as the HTTP Referer on a per-site basis.</td>
</tr>
<tr>
<td>refsSpoof</td>
<td>0.9.5</td>
<td>Allows easy spoofing of URL referer (referrer) w/ toolbar.</td>
</tr>
<tr>
<td>Server Switcher</td>
<td>0.5</td>
<td>Switch between your development and live servers.</td>
</tr>
<tr>
<td>SQL Injection!</td>
<td>1.2</td>
<td>Set all form fields free to test SQL Injections.</td>
</tr>
<tr>
<td>Tamper Data</td>
<td>10.1.0</td>
<td>View and modify HTTP/HTTPS headers etc. Track and time requests.</td>
</tr>
<tr>
<td>TestGen4Web - Script It All</td>
<td>1.0.0</td>
<td>Just like your VCR - for Firefox. It records what you do, stores it, and plays it back...</td>
</tr>
<tr>
<td>UrlParams</td>
<td>2.2.0</td>
<td>Displays GET/POST parameters in the sidebar.</td>
</tr>
<tr>
<td>User Agent Switcher</td>
<td>0.6.11</td>
<td>Adds a menu and a toolbar button to switch the user agent of the browser.</td>
</tr>
<tr>
<td>Web Developer</td>
<td>1.1.6</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

Options

QuickAdd

Use Advanced Menus

Apache/2.2.9...  FoxyProxy: Disabled
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-httprint-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
- owasp-wte-w3af-svn-3914-1_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
## WebSlayer

WebSlayer is a tool designed for brute forcing Web Applications.

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 WILLST..
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 scanner aimed at aiding manual penetration tests.
owasp-wte-grendel-scan

JBroFuzz is a web application fuzzing tool 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 automating the process of attacking an application.
owasp-wte-burpsuite

CAL9000 is a collection of web application security testing tools
owasp-wte-c9000

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

Utilita is an Open Source web server manager.
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 where 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 &lt;matt.tesauro@owasp.org&gt;
# as part of the OWASP Live CD project

# This file, webscarb, is part of the .deb package created for use
# on the OWASP Live CD.

# webscarb is free software: you can redistribute it and/or modify
# 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.

# webscarb 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 webscarb. If not, see &lt;http://www.gnu.org/licenses/&gt;.

# Tue, 12 Jan 2010 21:40:21 -0600

# This script was written with help from:
# &lt;http://www.linuxjournal.com/article/10495
# &lt;http://tldp.org/LDP/abs/html/extmisc.html
# &lt;http://www.linuxquestions.org/questions/programming-9/bash-how-to-handle-options-490759-and-the-zenity-man-page

# Set some sane defaults
RAM="64"
PROMPT="false"
SAVE="false"

# Setup command line option parsing

What is next?
root@wte-appsec-us-2010:~# du -h -s /opt/owasp
732M /opt/owasp
Among the new ideas for WTE are

- Live CDs & Live DVDs
- Virtual installs/appliances
- A package repository
  - Can add 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
- USB and Kiosk version
OWASP Education Project

Natural ties between these projects

- Already being used for training classes
- Need to coordinate efforts to make sure critical pieces aren't missing from the OWASP WTE
- Training environment could be customized for a particular class thanks to the individual modules
  - Student gets to take the environment home
- As more modules come online, even more potential for cross pollination
- Builder tools/docs only expand its reach
Builder vs Breaker

Builder is where the ROI is

But darn it, breaking is really fun.

Builder tools coming in future releases.

(Thanks Top Gear!)
Crazy “Pie in the Sky” idea

- .deb package + auto update + categories = CD profiles
  - Allows someone to customize the OWASP WTE to their needs
  - Example profiles
    - Whitebox testing
    - Blackbox testing
    - Static Analysis
    - Target specific (Java, .Net, ...)
  - Profile + VM = custom persistent environment
Goals going forward

- Showcase great OWASP projects
- Provide the best, freely distributable application security tools/documents in an easy to use package
- Ensure that tools provided are easy to use as possible
Goals going forward

- 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
- Add more developer focused tools
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 docs or links
- Do a screencast of one of the tools being used on the OWASP WTE
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/
A bit about OWASP
OWASP Meritocracy

OWASP Users and Participants

OWASP Members

OWASP Leaders (Chapters and Project)

Projects
Membership
Education
Conferences
Industry
Chapters
Connections

OWASP Foundation (OWASP Board)
Security Vulnerabilities

- Change Control
- Source Code Mgmt
- Strategy & Metrics
- Policy & Compliance
- Education & Training
- Threat Assessment
- Security Requirements
- Secure Architecture
- Design Review
- Code Review
- Remediation
- Hardening
- ...

...
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