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

OWASP
San Antonio
Jan. 20 2010

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

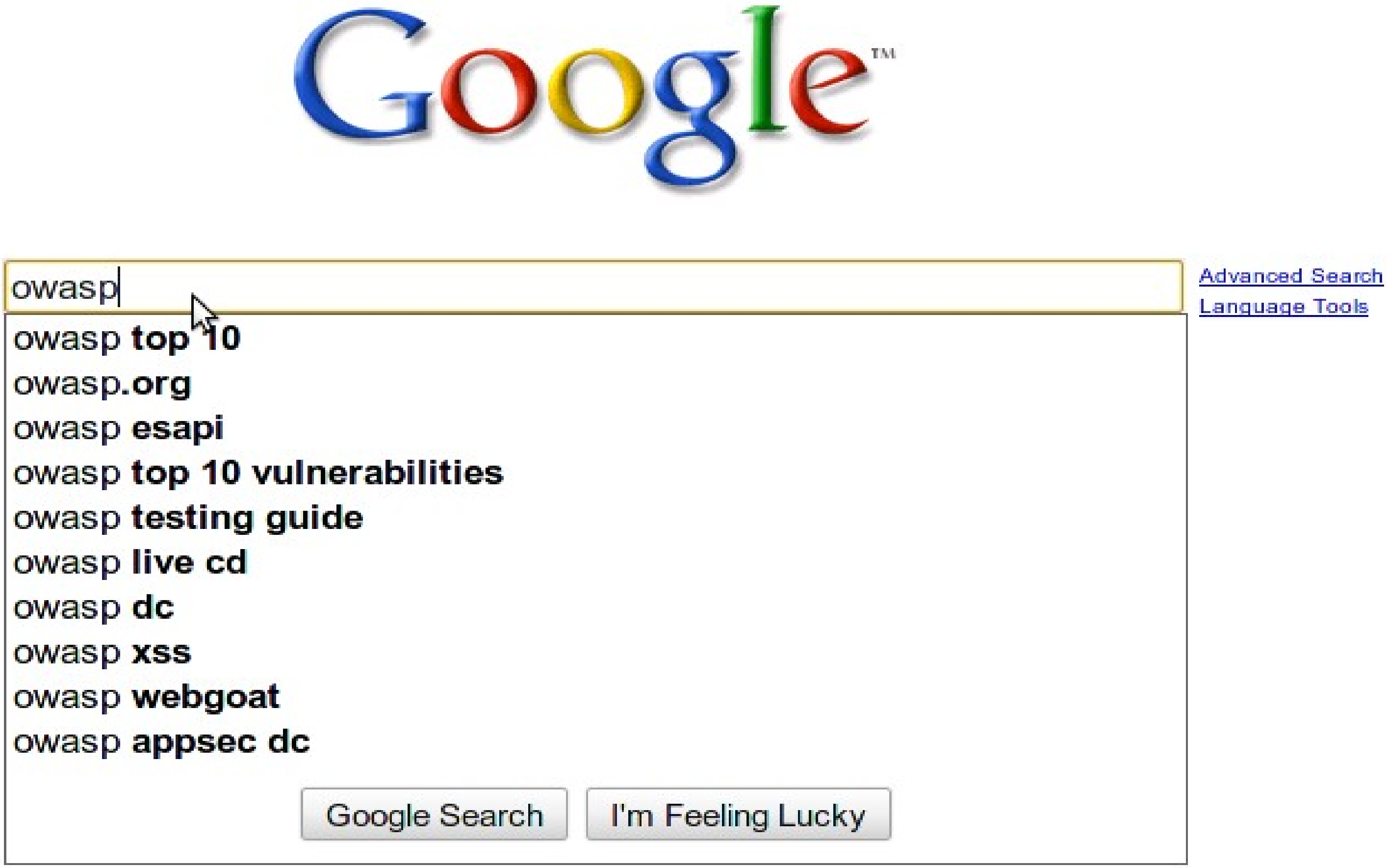
General goals going forward

- 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...



owasp

owasp top 10
owasp.org
owasp esapi
owasp top 10 vulnerabilities
owasp testing guide
owasp live cd
owasp dc
owasp xss
owasp webgoat
owasp appsec dc

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

Available Tools: 26 'Significant'

Other Proxies:

- Burp Suite
- Paros
- Spike Proxy
- Rat Proxy

Scanners:

- w3af
- Grendel Scan
- Nikto
- namp
- Zenmap
- Fierce Domain Scanner

SQL-i:

- sqlmap
- SQL Brute

Duh:

- Firefox

Others:

- Metasploit
- Httprint
- Maltego CE
- netcat
- Wireshark
- tcpdump

Its Demo time!

DANGER

DEMO AHEAD

Watch out for explosions
and demo gremlins

OWASP WTE

There's a new kid in town

OWASP WTE

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)

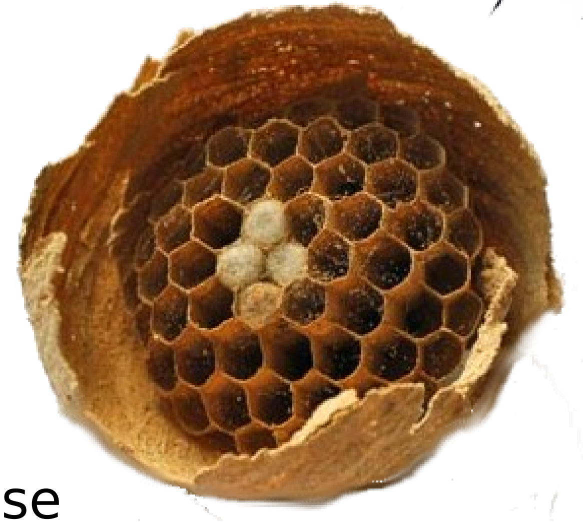
What OWASP WTE brings

- Among the new ides 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!

Documentation available

- OWASP Documents
  - Testing Guide v2 & v3
  - CLASP
  - Top 10 for 2007
  - Top 10 for Java Enterprise Edition
  - AppSec FAQ
  - Books
    - CLASP, Top 10 2007, Top 10 + Testing + Legal, WebGoat and Web Scarab, Guide 2.0, Code Review
- 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 & Paralles

- 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.

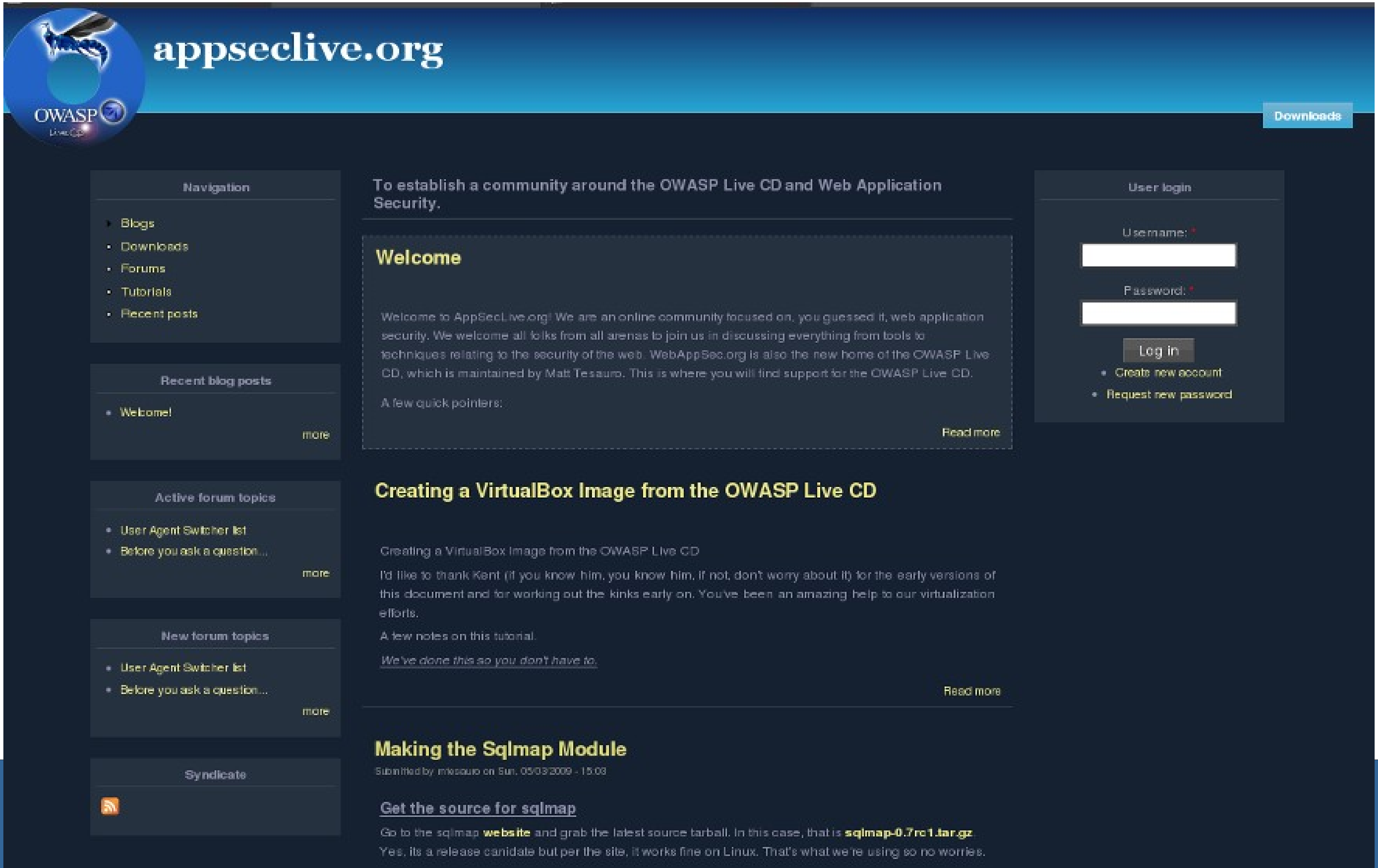
Builder tools coming in future packages.

(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

Website Update



appseclive.org

OWASP Live CD

Downloads

Navigation

- Blogs
- Downloads
- Forums
- Tutorials
- Recent posts

Recent blog posts

- Welcome!

more

Active forum topics

- User Agent Switcher list
- Before you ask a question...

more

New forum topics

- User Agent Switcher list
- Before you ask a question...

more

Syndicate

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:

Read more

Creating a VirtualBox Image from the OWASP Live CD

Creating a VirtualBox Image from the OWASP Live CD

I'd like to thank Kent (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.

Read more

Making the Sqlmap Module

Submitted by mtesauro on Sun, 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 canidate but per the site, it works fine on Linux. That's what we're using so no worries.

User login

Username: *

Password: *

Log in

- Create new account
- Request new password

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

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 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 the job your 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:
  http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project

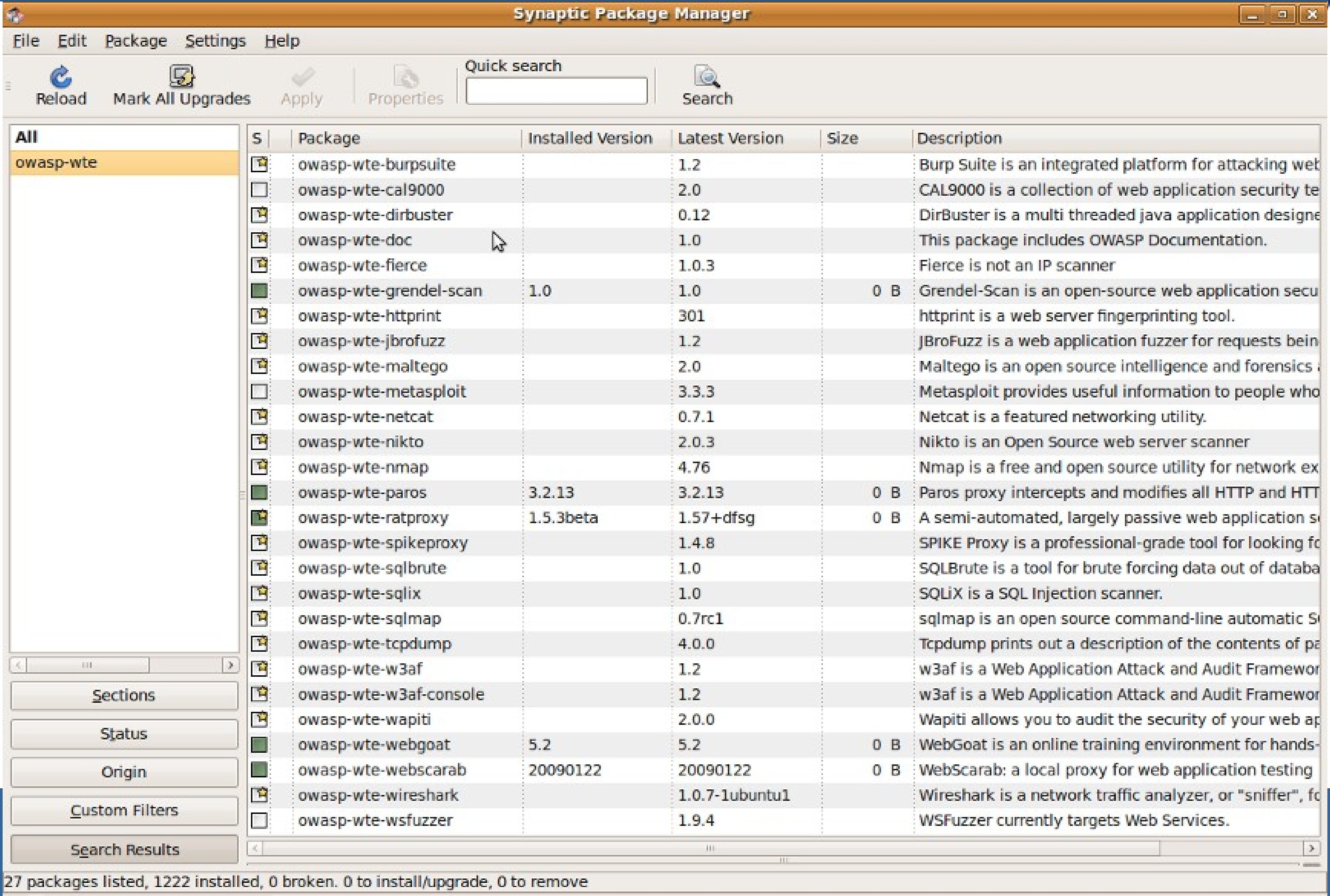
  or Google “OWASP Live CD”

- Download & Community Site:
  http://AppSecLive.org

- Google Code Site:
  http://code.google.com/p/owasp-wte/

- Original site: http://mtesauro.com/livecd/

OWASP WTE Synaptic Pride...



S	Package	Installed Version	Latest Version	Size	Description
☆	owasp-wte-burpsuite		1.2		Burp Suite is an integrated platform for attacking we
□	owasp-wte-cal9000		2.0		CAL9000 is a collection of web application security te
☆	owasp-wte-dirbuster		0.12		DirBuster is a multi threaded java application designe
☆	owasp-wte-doc		1.0		This package includes OWASP Documentation.
☆	owasp-wte-fierce		1.0.3		Fierce is not an IP scanner
🟩	owasp-wte-grendel-scan	1.0	1.0	0 B	Grendel-Scan is an open-source web application secu
☆	owasp-wte-httprint		301		httprint is a web server fingerprinting tool.
☆	owasp-wte-jbrofuzz		1.2		JBroFuzz is a web application fuzzer for requests bein
☆	owasp-wte-maltego		2.0		Maltego is an open source intelligence and forensics a
□	owasp-wte-metasploit		3.3.3		Metasploit provides useful information to people who
☆	owasp-wte-netcat		0.7.1		Netcat is a featured networking utility.
☆	owasp-wte-nikto		2.0.3		Nikto is an Open Source web server scanner
☆	owasp-wte-nmap		4.76		Nmap is a free and open source utility for network ex
🟩	owasp-wte-paros	3.2.13	3.2.13	0 B	Paros proxy intercepts and modifies all HTTP and HTT
🟩	owasp-wte-ratproxy	1.5.3beta	1.57+dfsg	0 B	A semi-automated, largely passive web application s
☆	owasp-wte-spikeproxy		1.4.8		SPIKE Proxy is a professional-grade tool for looking fo
☆	owasp-wte-sqlbrute		1.0		SQLBrute is a tool for brute forcing data out of databa
☆	owasp-wte-sqlix		1.0		SQLiX is a SQL Injection scanner.
☆	owasp-wte-sqlmap		0.7rc1		sqlmap is an open source command-line automatic S
☆	owasp-wte-tcpdump		4.0.0		Tcpdump prints out a description of the contents of pa
☆	owasp-wte-w3af		1.2		w3af is a Web Application Attack and Audit Framewor
☆	owasp-wte-w3af-console		1.2		w3af is a Web Application Attack and Audit Framewor
☆	owasp-wte-wapiti		2.0.0		Wapiti allows you to audit the security of your web ap
🟩	owasp-wte-webgoat	5.2	5.2	0 B	WebGoat is an online training environment for hands-
🟩	owasp-wte-webscarab	20090122	20090122	0 B	WebScarab: a local proxy for web application testing
☆	owasp-wte-wireshark		1.0.7-1ubuntu1		Wireshark is a network traffic analyzer, or "sniffer", fo
□	owasp-wte-wsfuzzer		1.9.4		WSFuzzer currently targets Web Services.

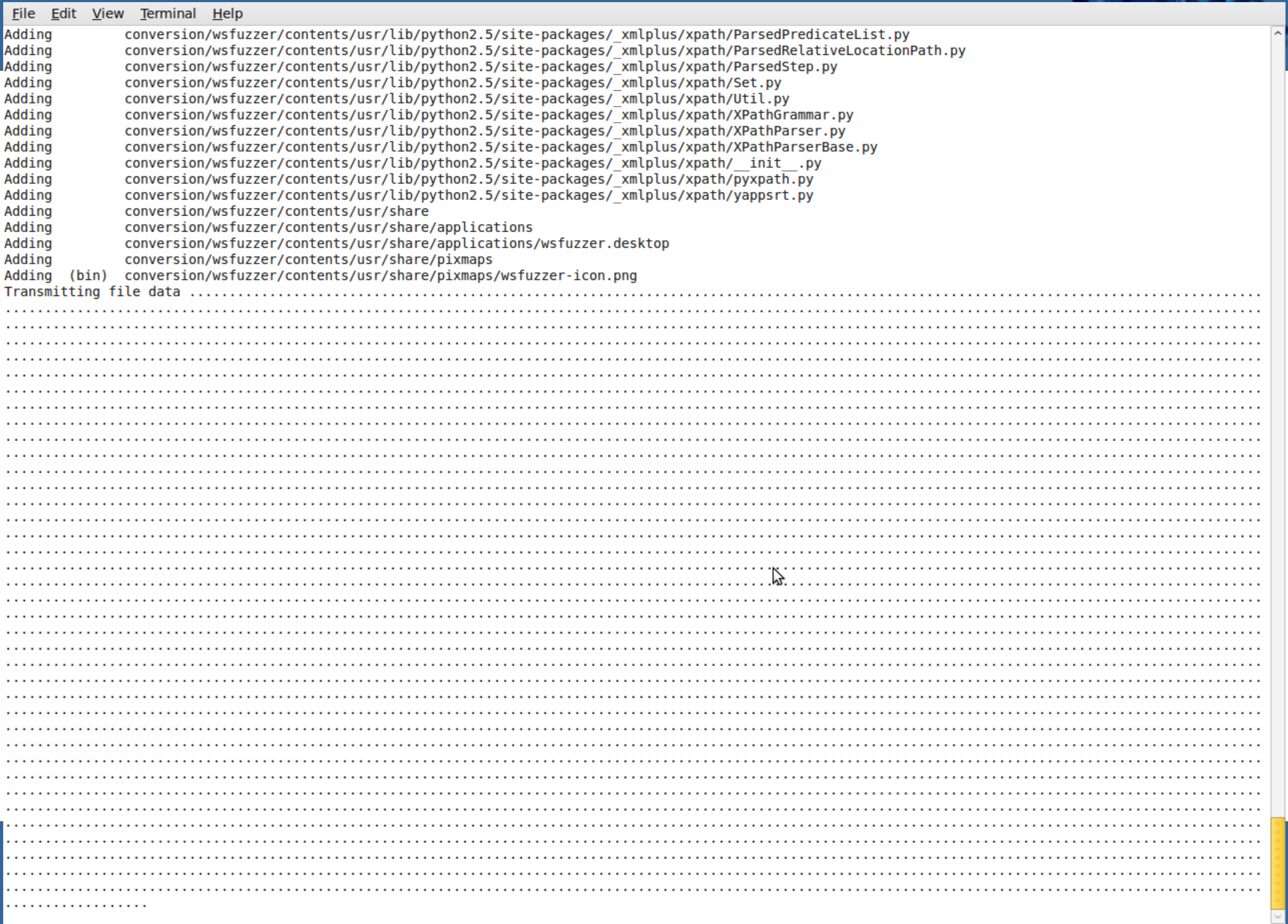
27 packages listed, 1222 installed, 0 broken. 0 to install/upgrade, 0 to remove

OWASP WTE is OPEN

- Add will always be...

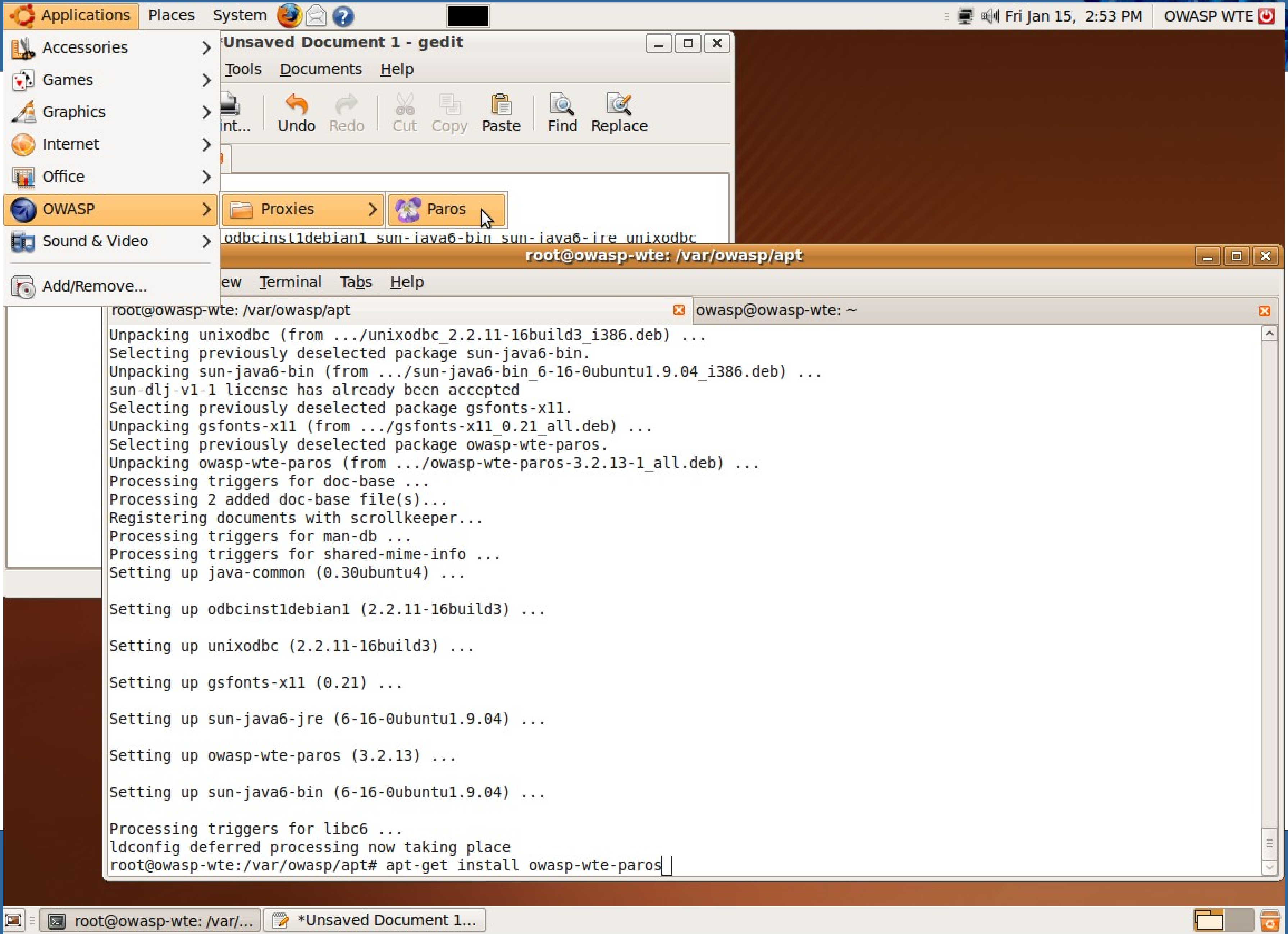
Questions?

the BIG commit



```
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/ParsedPredicateList.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/ParsedRelativeLocationPath.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/ParsedStep.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/Set.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/Util.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/XPathGrammar.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/XPathParser.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/XPathParserBase.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/__init__.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/pyxpath.py
Adding         conversion/wsfuzzer/contents/usr/lib/python2.5/site-packages/_xmlplus/xpath/yappsrt.py
Adding         conversion/wsfuzzer/contents/usr/share
Adding         conversion/wsfuzzer/contents/usr/share/applications
Adding         conversion/wsfuzzer/contents/usr/share/applications/wsfuzzer.desktop
Adding         conversion/wsfuzzer/contents/usr/share/pixmaps
Adding  (bin)  conversion/wsfuzzer/contents/usr/share/pixmaps/wsfuzzer-icon.png
Transmitting file data ......................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
.............................................................................................................................................................
..................
```

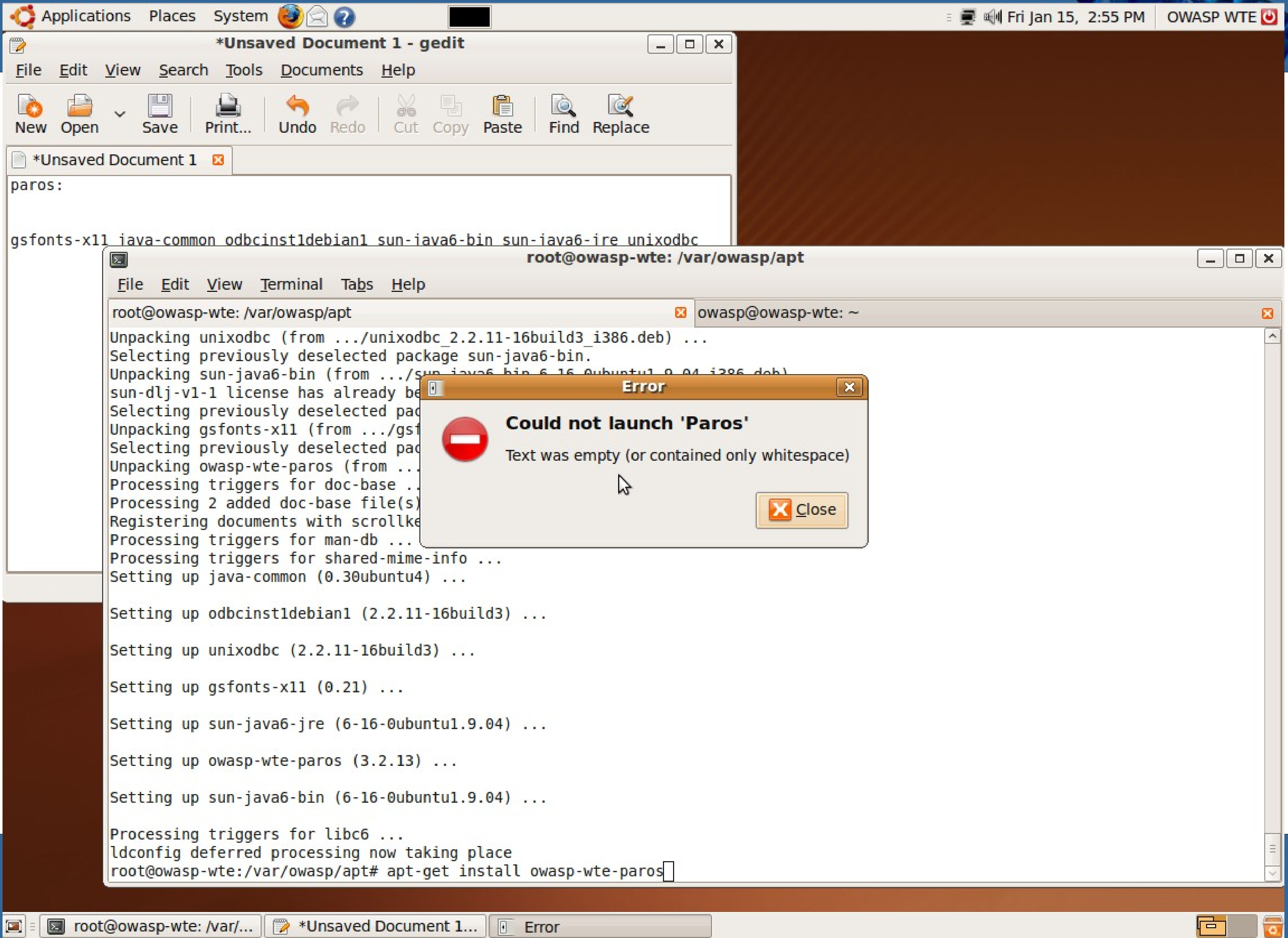
First package test install



```
odbcinst1debian1 sun-java6-bin sun-java6-jre unixodbc
```

```
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 (0.30ubuntu4) ...

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 ...
ldconfig deferred processing now taking place
root@owasp-wte:/var/owasp/apt# apt-get install owasp-wte-paros
```

First package fail


Applications Places System
Fri Jan 15, 2:55 PM
OWASP WTE
*Unsaved Document 1 - gedit
File Edit View Search Tools Documents Help
New Open Save Print... Undo Redo Cut Copy Paste Find Replace
*Unsaved Document 1

```
paros:


gsfonts-x11 java-common odbcinst1debian1 sun-java6-bin sun-java6-jre unixodbc
```

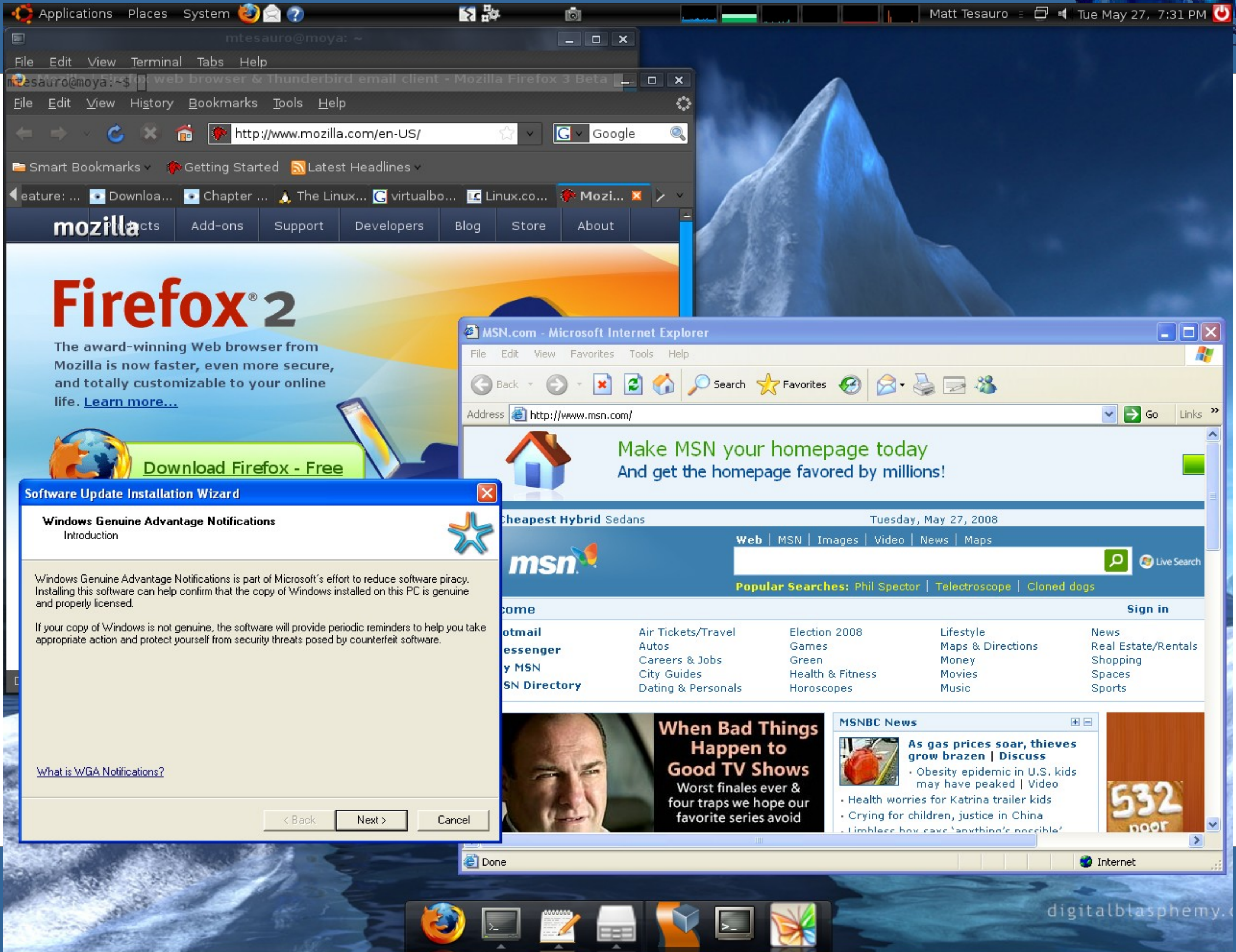
root@owasp-wte: /var/owasp/apt
File Edit View Terminal Tabs Help
root@owasp-wte: /var/owasp/apt
owasp@owasp-wte: ~

```
Unpacking unixodbc (from .../unixodbc_2.2.11-16build3_i386.deb) ...
Selecting previously deselected package sun-java6-bin.
Unpacking sun-java6-bin (from .../s
sun-dlj-v1-1 license has already be
Selecting previously deselected pac
Unpacking gsfonts-x11 (from .../gsf
Selecting previously deselected pac
Unpacking owasp-wte-paros (from ...
Processing triggers for doc-base ..
Processing 2 added doc-base file(s)
Registering documents with scrollke
Processing triggers for man-db ...
Processing triggers for shared-mime-info ...
Setting up java-common (0.30ubuntu4) ...

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 ...
ldconfig deferred processing now taking place
root@owasp-wte:/var/owasp/apt# apt-get install owasp-wte-paros
```

Could not launch 'Paros'

Text was empty (or contained only whitespace)

Yeah, genuine alright


Applications Places System
Matt Tesauro
Tue May 27, 7:31 PM
mtesauro@moya: ~
File Edit View Terminal Tabs Help
mtesauro@moya:~$
Mozilla Firefox web browser & Thunderbird email client - Mozilla Firefox 3 Beta
File Edit View History Bookmarks Tools Help
http://www.mozilla.com/en-US/
Google
Smart Bookmarks
Getting Started
Latest Headlines
eature: ...
Downloa...
Chapter ...
The Linux...
virtualbo...
Linux.co...
Mozi...
mozilla
Products
Add-ons
Support
Developers
Blog
Store
About
Firefox 2
Download Firefox - Free
MSN.com - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.msn.com/
Go
Links
Make MSN your homepage today
And get the homepage favored by millions!
Cheapest Hybrid Sedans
Tuesday, May 27, 2008
Web | MSN | Images | Video | News | Maps
msn
Live Search
Popular Searches: Phil Spector | Telectroscope | Cloned dogs
come
Sign in
otmail
essenger
y MSN
SN Directory
Air Tickets/Travel
Autos
Careers &amp; Jobs
City Guides
Dating &amp; Personals
Election 2008
Games
Green
Health &amp; Fitness
Horoscopes
Lifestyle
Maps &amp; Directions
Money
Movies
Music
News
Real Estate/Rentals
Shopping
Spaces
Sports
When Bad Things Happen to Good TV Shows
Worst finales ever &amp; four traps we hope our favorite series avoid
MSNBC News
As gas prices soar, thieves grow brazen | Discuss
· Obesity epidemic in U.S. kids may have peaked | Video
· Health worries for Katrina trailer kids
· Crying for children, justice in China
532 poor
Done
Internet
Software Update Installation Wizard
Windows Genuine Advantage Notifications
Introduction
What is WGA Notifications?
&lt; Back
Next &gt;
Cancel
digitalblasphemy.c

The award-winning Web browser from Mozilla is now faster, even more secure, and totally customizable to your online life. Learn more...

Windows Genuine Advantage Notifications is part of Microsoft's effort to reduce software piracy. Installing this software can help confirm that the copy of Windows installed on this PC is genuine and properly licensed.

If your copy of Windows is not genuine, the software will provide periodic reminders to help you take appropriate action and protect yourself from security threats posed by counterfeit software.