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

OWASP Summer of Cod...

www.owasp.org/index.php/OWASP_Summer_of_Code_2008

Page Discussion View source History

Navigation

- Home
- News
- OWASP Projects
- Downloads
- Local Chapters
- Global Committees
- AppSec Job Board
- AppSec Conferences
- Presentations
- Video
- Press
- Get OWASP Books
- Get OWASP Gear
- Mailing Lists
- About OWASP
- Membership

Reference

- How To...
- Principles
- Threat Agents
- Attacks
- Vulnerabilities
- Controls
- Activities
- Technologies
- Glossary
- Code Snippets
- .NET Project
- Java Project

Language

OWASP Summer of Code 2008

OWASP Summer of Code 2008

- **MAIN LINKS**
- Press Release
- OWASP Summer of Code 2008 Blog
- Request for Proposal List
- Applications
- Jury's evaluation/selection of applications
- Approved projects, authors, status target and reviewers
- Half term payments
- Project completion payments
- OWASP EU Summit Portugal 2008
- Project's current status

Projects | Historical Information

100% Completion Projects	Author
OWASP Testing Guide v3	Matteo Meucci
OWASP Ruby on Rails Security Guide v2	Heiko Webers
OWASP Live CD 2008 Project	Matt Tesauro
OWASP Code review guide, V1.1	Eoin Keary
OWASP AntiSamy .NET	Arshan Dabirsiaghi
OWASP .NET Project Leader	Mark Roxberry

- 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)

File Edit View History Bookmarks Tools Help

http://www.google.com/#hl=en&sugexp=ldymls&xhr=t&q=owasp+live+cd&cp=

Google

owasp live cd - Google Search

Web Images Videos Maps News Shopping Gmail more Sign in

Google

owasp live cd

Search

Instant is on

owasp live cd
owasp lisbon
owasp library
owasp linux
owasp li

Everything
Images
Videos
News
Shopping
More

Austin, TX
Change location

Any time
Latest
Past 24 hours
Past week
Past 2 weeks
Past month
Past year
Custom range...

More search tools

About 189,000 results (0.42 seconds) Advanced search

Category:**OWASP Live CD** Project - OWASP
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 ...
www.**owasp**.org/index.../Category:**OWASP_Live_CD**_Project - Cached - Similar

Category:**OWASP Live CD** 2008 Project - OWASP
Aug 28, 2009 ... The **OWASP Live CD** also contains documentation and an ...
www.**owasp**.org/.../Category:**OWASP_Live_CD**_2008_Project - Cached - Similar

Category:**OWASP LiveCD** Education Project - OWASP
Aug 28, 2009 ... Executive Summary: I am proposing a new project that will ...
www.**owasp**.org/.../Category:**OWASP_LiveCD**_Education_Project - Cached - Similar

Owasp-live-cd-2008-project Info Page
The **OWASP Live CD** 2008 project is focused on creating a Linux-based live CD ...
https://lists.**owasp**.org/mailman/.../**owasp-live-cd**-2008-project - Cached - Similar

Show more results from owasp.org

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 ...
appsec**live**.org/ - Cached

File Edit View History Bookmarks Tools Help

http://www.google.com/#hl=en&sugexp=ldymls&xhr=t&q=owasp+wte&cp=7&f

Google

owasp wte - Google Search

Web Images Videos Maps News Shopping Gmail more Sign in

Google

owasp wte

Search

Instant is on

- owasp **wte**
- owasp **webgoat**
- owasp **wiki**
- owasp **webscarab**
- owasp **w**

Everything
Images
Videos
News
Shopping
More

Austin, TX
Change location

All results
Wonder wheel
More search tools

About 45,400 results (0.28 seconds) Advanced search

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

Show more results from appseclive.org

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 ...

Done

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)

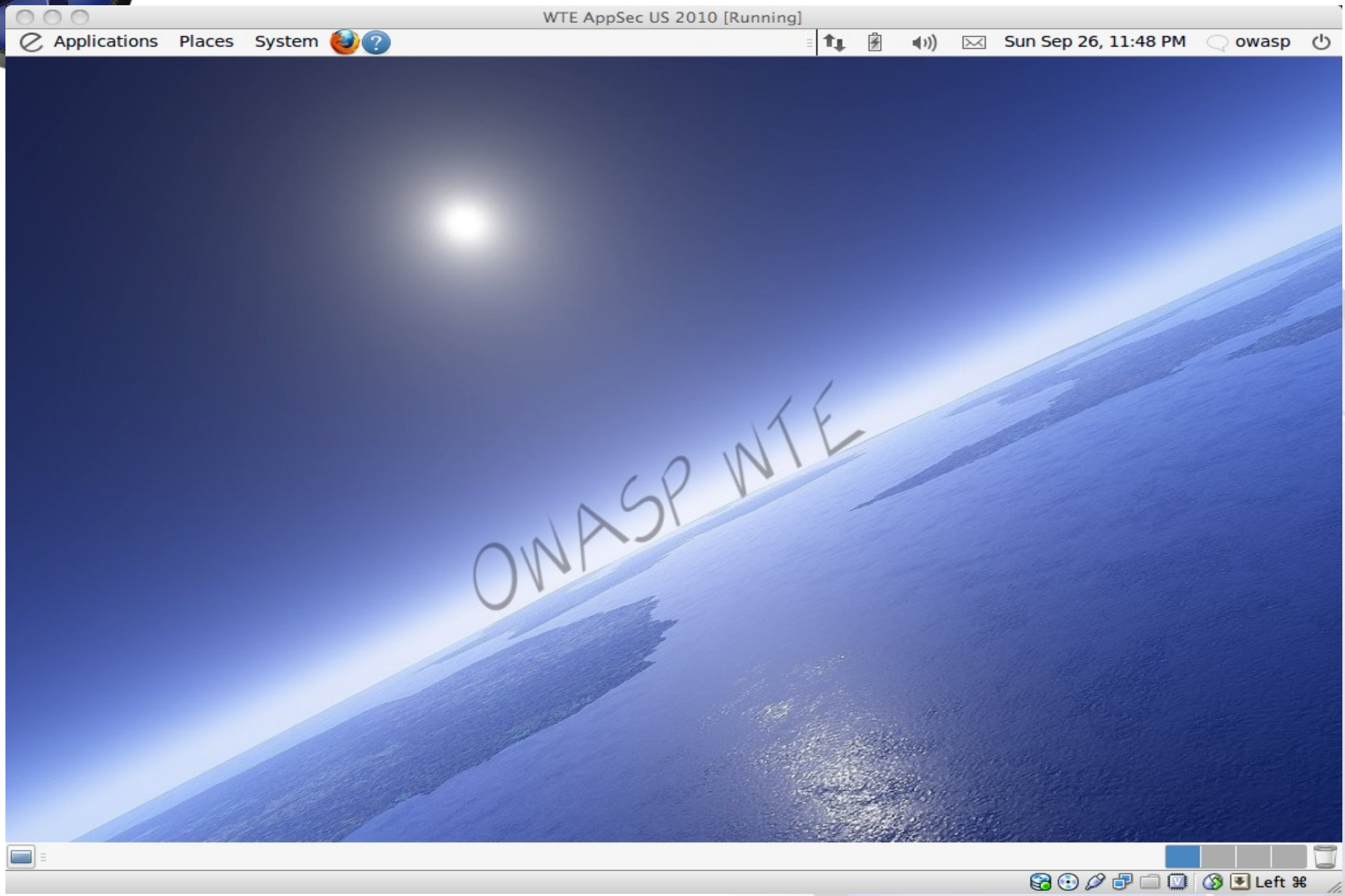
- GOAL

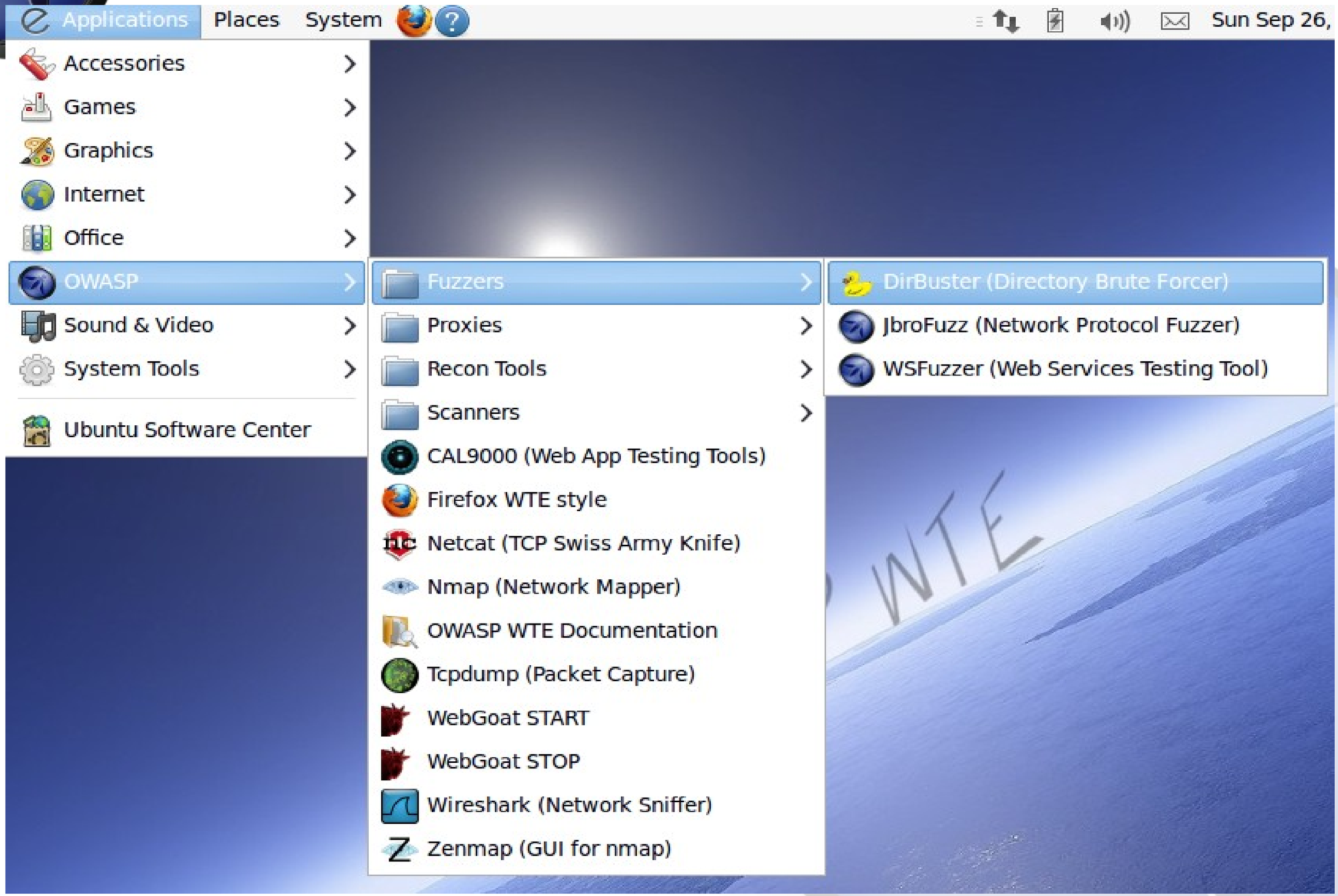
  Make application security tools and documentation easily available and easy to use

  - 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


WTE AppSec US 2010 [Running]
Applications
Places
System
Sun Sep 26, 11:48 PM
owasp
OWASP WTE
Left ⌘


Applications
Places
System
Sun Sep 26,
Accessories
Games
Graphics
Internet
Office
OWASP
Sound & Video
System Tools
Ubuntu Software Center
Fuzzers
Proxies
Recon Tools
Scanners
CAL9000 (Web App Testing Tools)
Firefox WTE style
Netcat (TCP Swiss Army Knife)
Nmap (Network Mapper)
OWASP WTE Documentation
Tcpdump (Packet Capture)
WebGoat START
WebGoat STOP
Wireshark (Network Sniffer)
Zenmap (GUI for nmap)
DirBuster (Directory Brute Forcer)
JbroFuzz (Network Protocol Fuzzer)
WSFuzzer (Web Services Testing Tool)

26 “Significant” Tools Available

OWASP Tools:

Web Scarab

a tool for performing all types of security testing on web apps and web services

WSFuzzer

a fuzzer with HTTP based SOAP services as its main target

Web Goat

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

Wapiti

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

CAL9000

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

DirBuster

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

JBroFuzz

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

WebSlayer

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

EnDe

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

ZAP Proxy

A fork of the popular but moribund Paros Proxy

Other Proxies:


Burp Suite


Paros


Spike Proxy


Rat Proxy

Scanners:

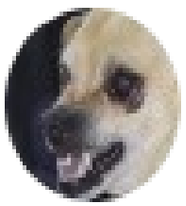

w3af


Grendel Scan


Nikto


nmap


Zenmap


Fierce Domain Scanner

SQL-i:


sqlmap


SQL Brute

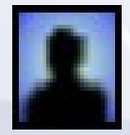
Duh:


Firefox

Others:

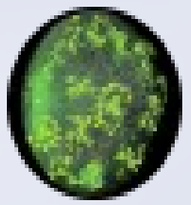

Metasploit


Httprint


Maltego CE


netcat


Wireshark


tcpdump

Why is it different?

Add N Edit Cookies 0.2.1.3
Cookie Editor that allows you add and edit se

CookiePie 1.0.2
Use multiple Web accounts and profiles in diff

DOM Inspector 2.0.3
Inspects the structure and properties of a win

Firebug 1.3.3
Web Development Evolved.

FormFox 1.6.3
Pops up form action when submit button is at

FoxyProxy 2.9
FoxyProxy - Premier proxy management for Fi

Greasemonkey 0.8.20090123.1
A User Script Manager for Firefox

HackBar 1.3.2
A toolbar that helps you find and test SQL inje

Header Spy 1.3.3.1
Shows HTTP headers on statusbar

InspectThis 0.9.1
Inspect the current element with the DOM Ins

JSView 2.0.5
View the source code of external stylesheets

Live HTTP headers 0.14
View HTTP headers of a page and while brow

Modify Headers 0.6.6
Add, modify and filter http request headers

No-Referer 1.3.1
Lets you open a tab without sending the HTTP referer information.

NoScript 1.9.2.6
Extra protection for your Firefox: NoScript allows JavaScript, Java (and other plu...

POW 0.1.8
A personal Web Server

RefControl 0.8.11
Control what gets sent as the HTTP Referer on a per-site basis.

refspoof 0.9.5
Allows easy spoofing of URL referer (referrer) w/ toolbar.

Server Switcher 0.5
Switch between your development and live servers.

SQL Injection! 1.2
Set all form fields free to test SQL Injections.

Tamper Data 10.1.0
View and modify HTTP/HTTPS headers etc. Track and time requests.

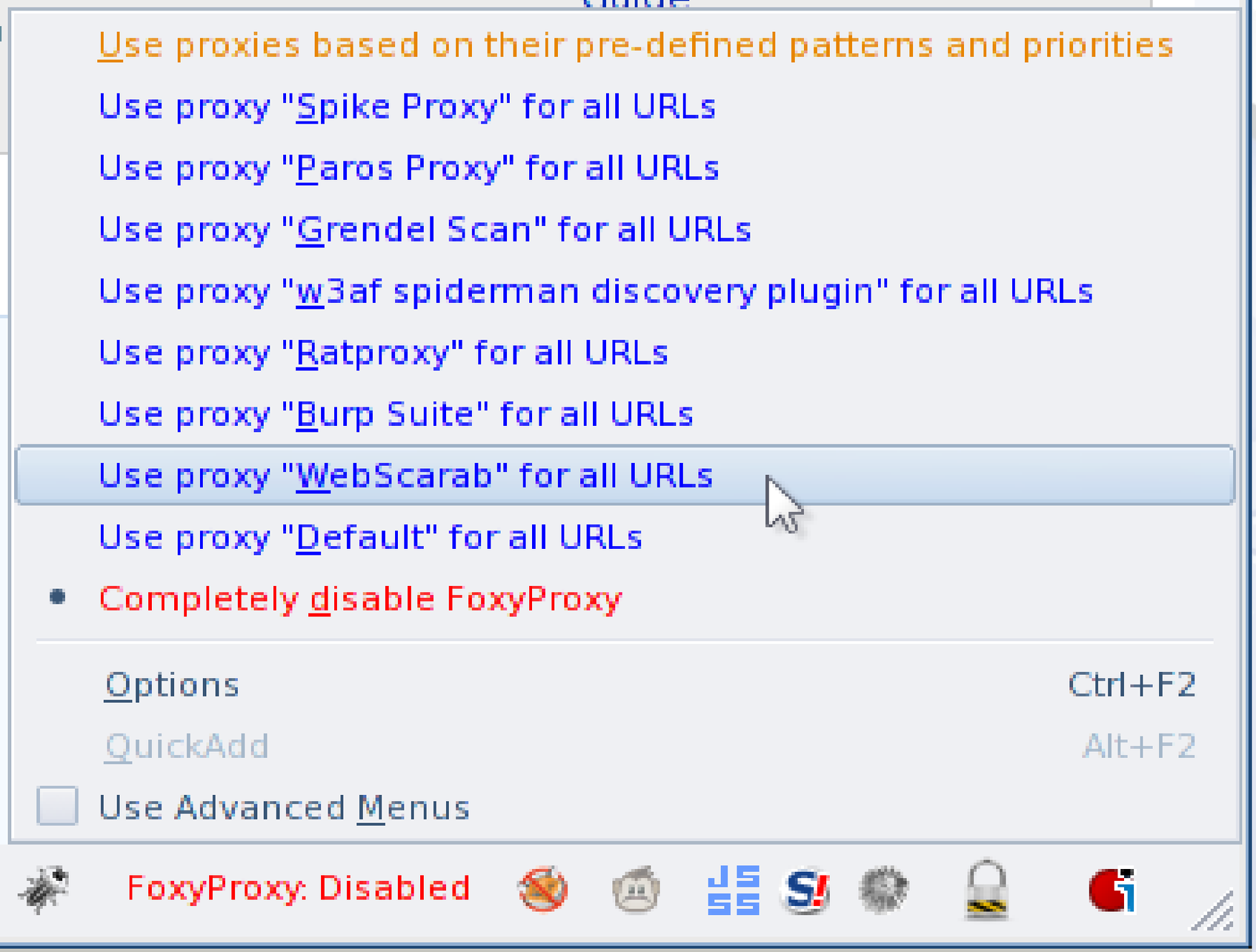
TestGen4Web - Script It All 1.0.0
Just like your VCR - for Firefox. It records what you do, stores it, and plays it bac...

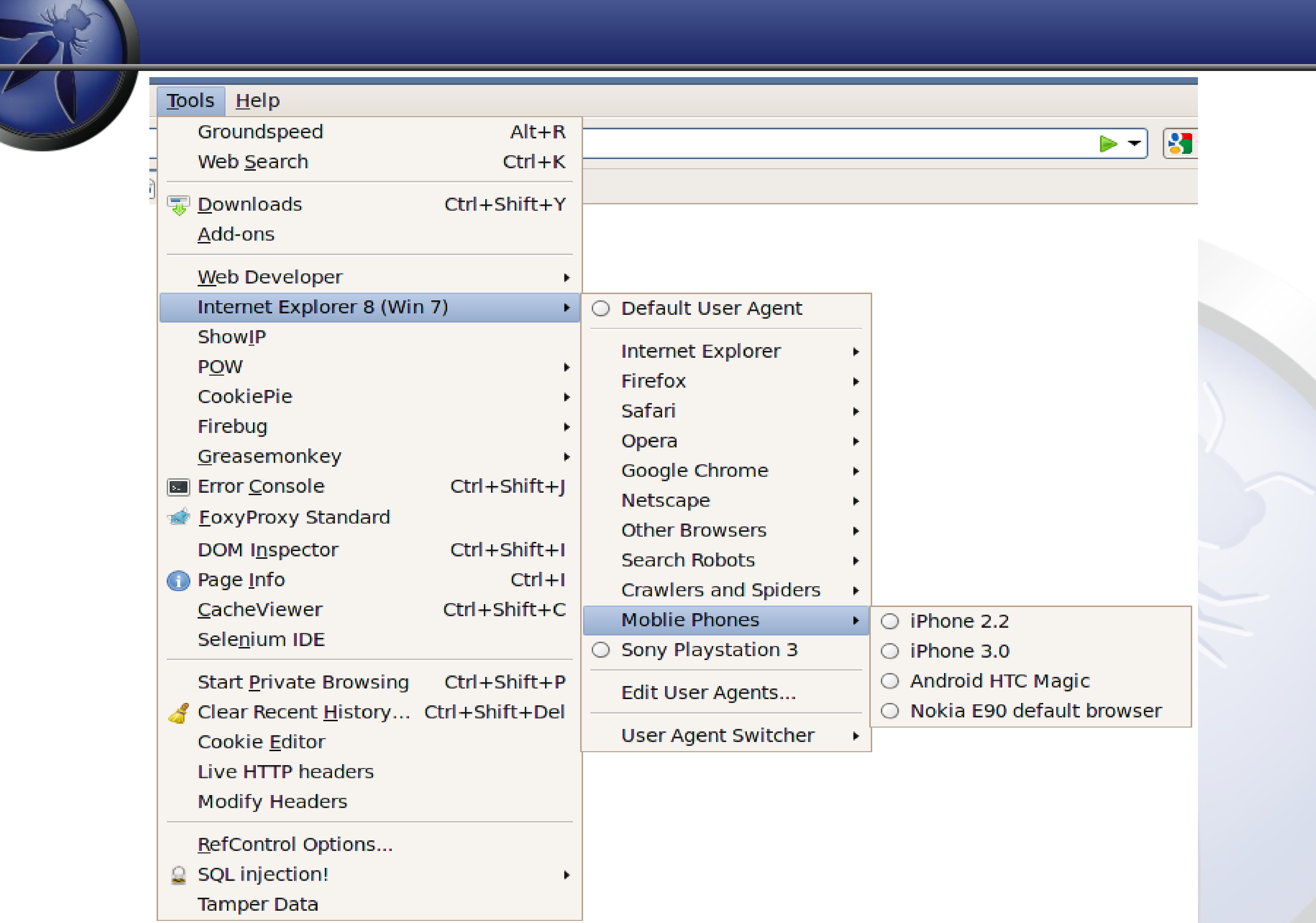
UrlParams 2.2.0
Displays GET/POST parameters in the sidebar.

User Agent Switcher 0.6.11
Adds a menu and a toolbar button to switch the user agent of the browser.

Web Developer 1.1.6
Adds a menu and a toolbar with various web developer tools.

- Top Ten
- WebGoat
- ESAPI
- ASVS
- Development Guide
- Code Review Guide
- CLASP
- Contracting




Tools
Help
Groundspeed Alt+R
Web Search Ctrl+K
Downloads Ctrl+Shift+Y
Add-ons
Web Developer
Internet Explorer 8 (Win 7)
ShowIP
POW
CookiePie
Firebug
Greasemonkey
Error Console Ctrl+Shift+J
FoxyProxy Standard
DOM Inspector Ctrl+Shift+I
Page Info Ctrl+I
CacheViewer Ctrl+Shift+C
Selenium IDE
Start Private Browsing Ctrl+Shift+P
Clear Recent History... Ctrl+Shift+Del
Cookie Editor
Live HTTP headers
Modify Headers
RefControl Options...
SQL injection!
Tamper Data
Default User Agent
Internet Explorer
Firefox
Safari
Opera
Google Chrome
Netscape
Other Browsers
Search Robots
Crawlers and Spiders
Moblie Phones
Sony Playstation 3
Edit User Agents...
User Agent Switcher
iPhone 2.2
iPhone 3.0
Android HTC Magic
Nokia E90 default browser

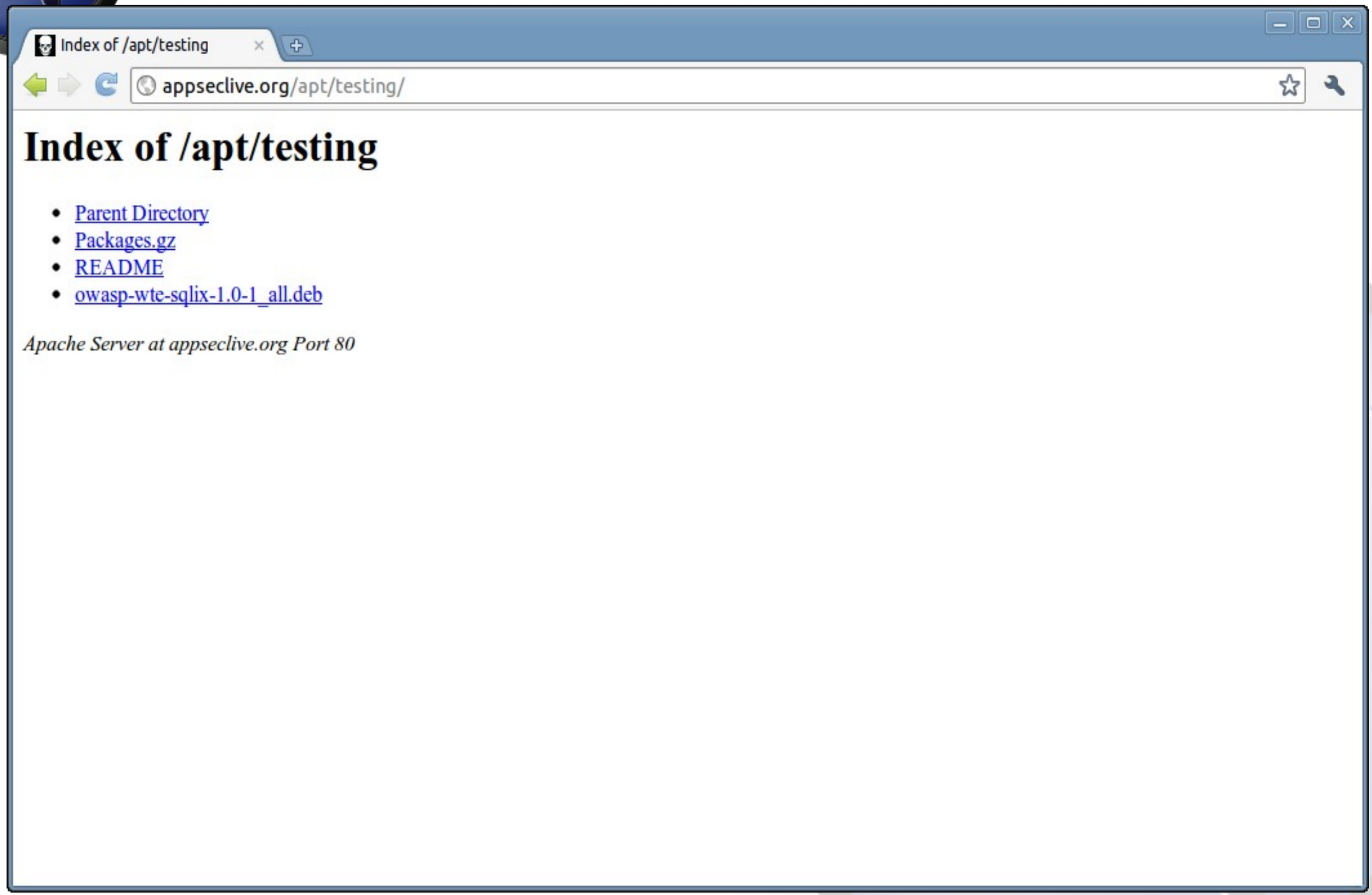
- OWASP Documents
  - Testing Guide v2 & v3
  - CLASP and OpenSamm
  - Top 10 for 2010
  - Top 10 for Java Enterprise Edition
  - AppSec FAQ
  - Books – tried to get all of them
    - CLASP, Top 10 2010, Top 10 + Testing + Legal, WebGoat and Web Scarab, Guide 2.0, Code Review
- Others
  - WASC Threat Classification, OSTTMM 3.0 & 2.2

Index of /apt/stable

appseclive.org/apt/stable/

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


Index of /apt/testing
appseclive.org/apt/testing/
Index of /apt/testing
Parent Directory
Packages.gz
README
owasp-wte-sqlix-1.0-1_all.deb
Apache Server at appseclive.org Port 80

File Edit Package Settings Help

Reload | Mark All Upgrades | Apply | Properties | Quick search | Search

All
owasp-wte

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

Sections
Status
Origin
Custom Filters
Search Results

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

File Edit View Help

- Get Software
- Installed Software
- History

Get Software > Search Results

owasp-wte

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 H…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 applic…eared 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 at…p the process of attacking 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

27 matching items

owasp-wte - Project Ho...

code.google.com/p/owasp-wte/

My favorites ▼ | Sign in

owasp-wte

OWASP Web Testing Environment (WTE)

Search projects

Project Home | Downloads | Wiki | Issues | Source

Summary Updates People

Project Information

Activity High
Project feeds

Code license
GNU GPL v3

Content license
Creative Commons 3.0 BY-SA

Labels
security, OWASP, livecd, Linux, Ubuntu, ApplicationSecurity

Members
mtesa...@gmail.com
2 committers

Links

Blogs
AppSecLive

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.

webscarab - owasp-wte ...

code.google.com/p/owasp-wte/source/browse/conversion/webscarab/contents/usr/bin/webscarab

Project Home | Downloads | Wiki | Issues | **Source**

Checkout **Browse** Changes | Search Trunk

Source path: svn/ conversion/ webscarab/ contents/ usr/ bin/ webscarab

‹ r165 **r283**

Hide details

```
1  #!/bin/bash
2  #
3  # Script written by Matt Tesauro <matt.tesauro@owasp.org>
4  # as part of the OWASP Live CD project
5  #
6  # This file, webscarab, is part of the .deb package created for use
7  # on the OWASP Live CD.
8  #
9  # webscarab is free software: you can redistribute it and/or modify
10 # it under the terms of the GNU General Public License as published by
11 # the Free Software Foundation, either version 3 of the License, or
12 # (at your option) any later version.
13 #
14 # webscarab is distributed in the hope that it will be useful,
15 # but WITHOUT ANY WARRANTY; without even the implied warranty of
16 # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
17 # GNU General Public License for more details.
18 #
19 # You should have received a copy of the GNU General Public License
20 # along with webscarab.  If not, see <http://www.gnu.org/licenses/>.
21 #
22 # Tue, 12 Jan 2010 21:40:21 -0600
23
24 # This script was written with help from:
25 # http://www.linuxjournal.com/article/10495
26 # http://tldp.org/LDP/abs/html/extmisc.html
27 # http://www.linuxquestions.org/questions/programming-9/bash-how-to-handle-options-4
28 # and the zenity man page
29
30 # Set some sane defaults
31 RAM="64"
32 PROMPT="false"
33 SAVE="false"
34
35 # Setup command line option parsing
```

Change log

r209 by mtesauro on Aug 29, 2010 Diff

Fixed bugs in WebScarab launching script and updated postinst

Go to: ...carab/contents/usr/bin/webscarab

Project members, sign in to write a code review

Older revisions

⊞ r165 by mtesauro on Mar 04, 2010 Diff

⊞ r83 by mtesauro on Jan 16, 2010 Diff

⊞ r2 by mtesauro on Jan 13, 2010 Diff

All revisions of this file

File info

Size: 4123 bytes, 127 lines

View raw file

File properties

svn:executable

*

What is next?


```
root@wte-appsec-us-2010:~# du -h -s /opt/owasp
732M    /opt/owasp
```

- Among the new ides 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

(Thanks Top Gear!)

But darn it,
breaking is really fun.

Builder tools coming in future releases.

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

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

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)

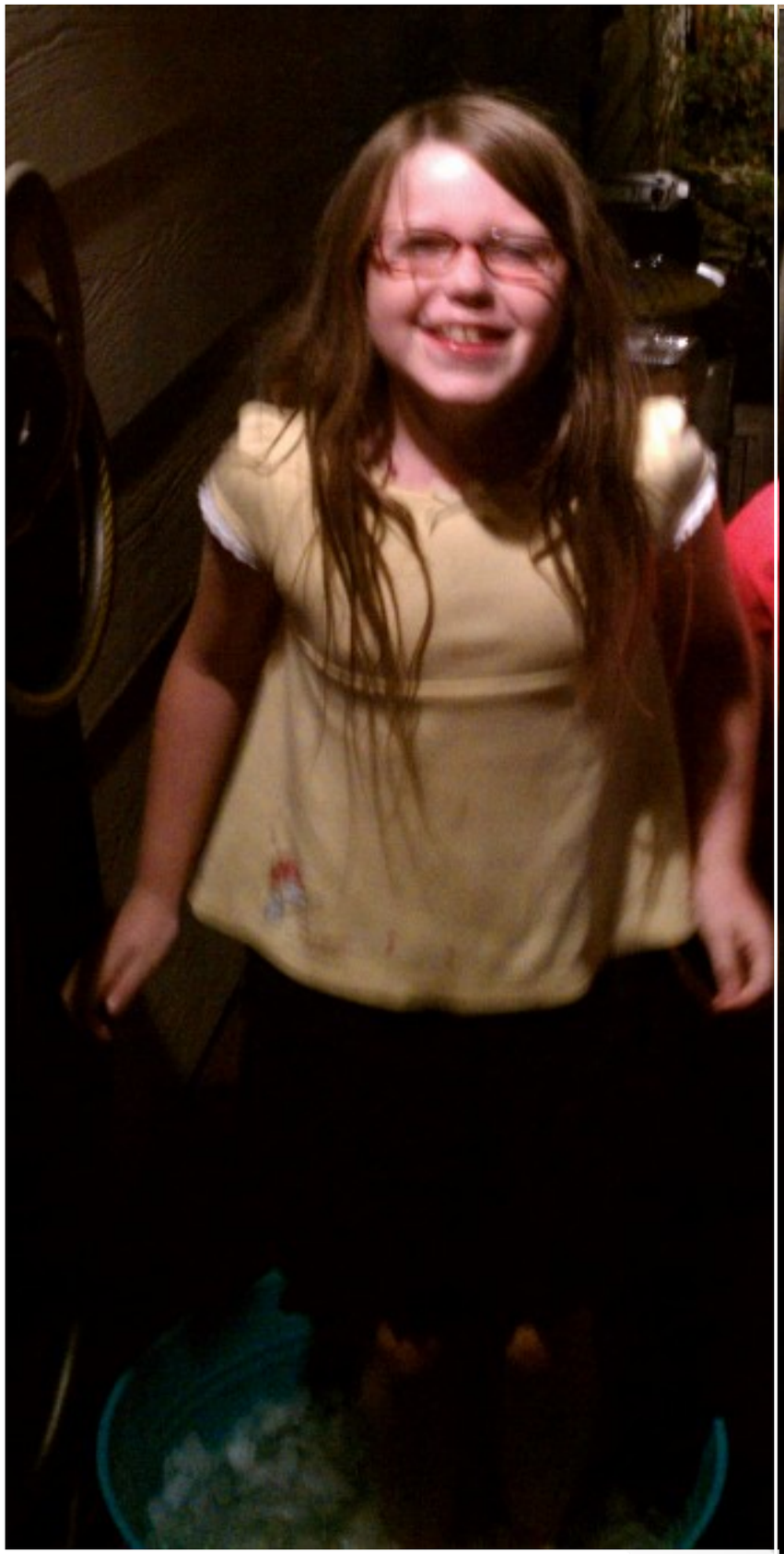
Projects | Membership | Education | Conferences | Industry | Chapters | Connections

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