



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



Press Release - OWASP Summer of Code 2008

☆ from **Paulo Coimbra** <paulo.coimbra@owasp.org>

[hide details](#) 3/4/08

[Reply to all](#)

to OWASP - ALL <owasp-all@lists.owasp.org>

date Tue, Mar 4, 2008 at 1:33 PM

subject Press Release - OWASP Summer of Code 2008

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 where 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.

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 ISECOM/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 base on Morphix – a Knoppix derivative created to allow easy creation of custom Live CDs, I'm not sure it 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 Mophix:

- no change to current LiveCD - principally just updates to existing and augment.

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


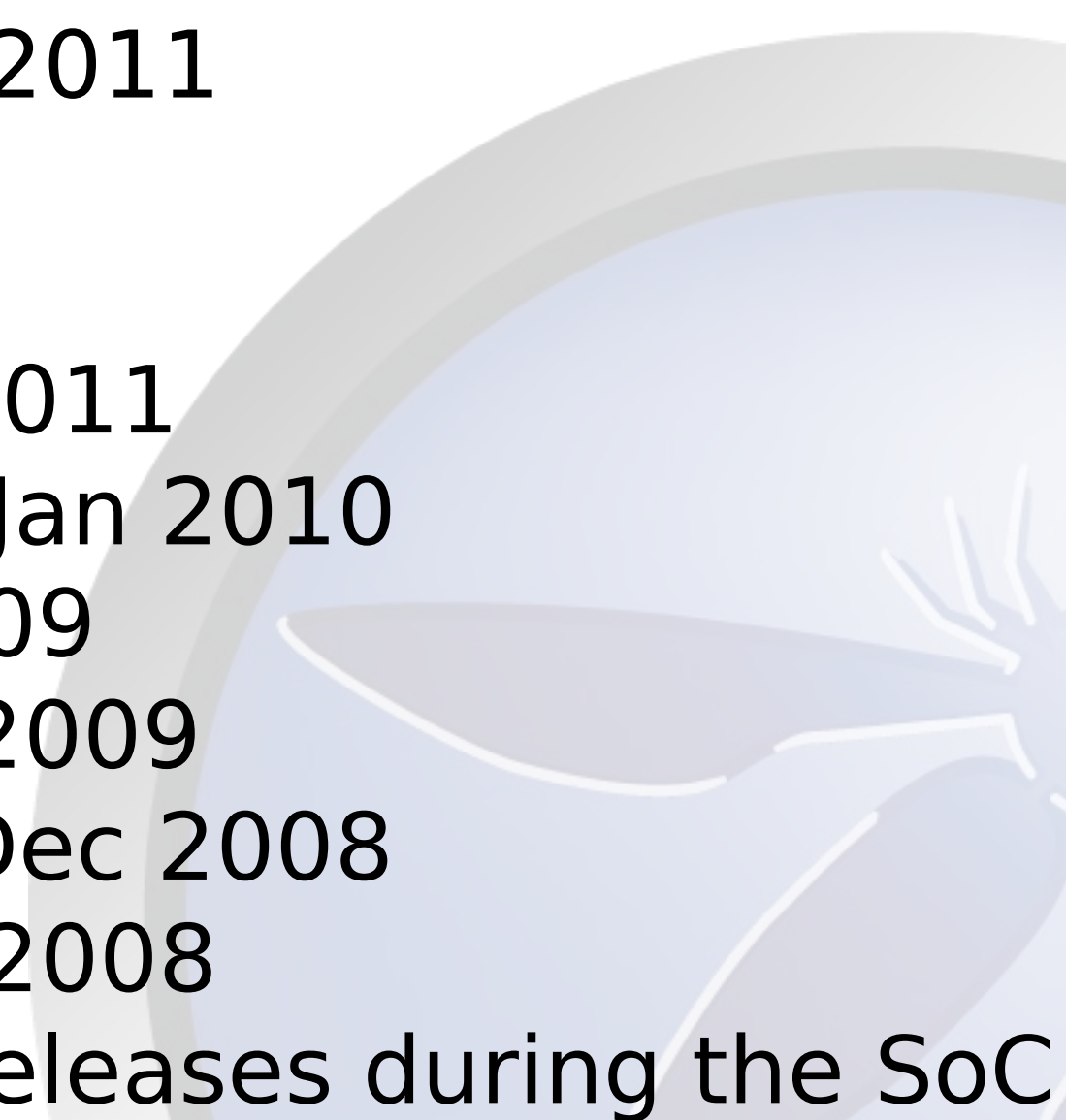
■ MAIN LINKS

- 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 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

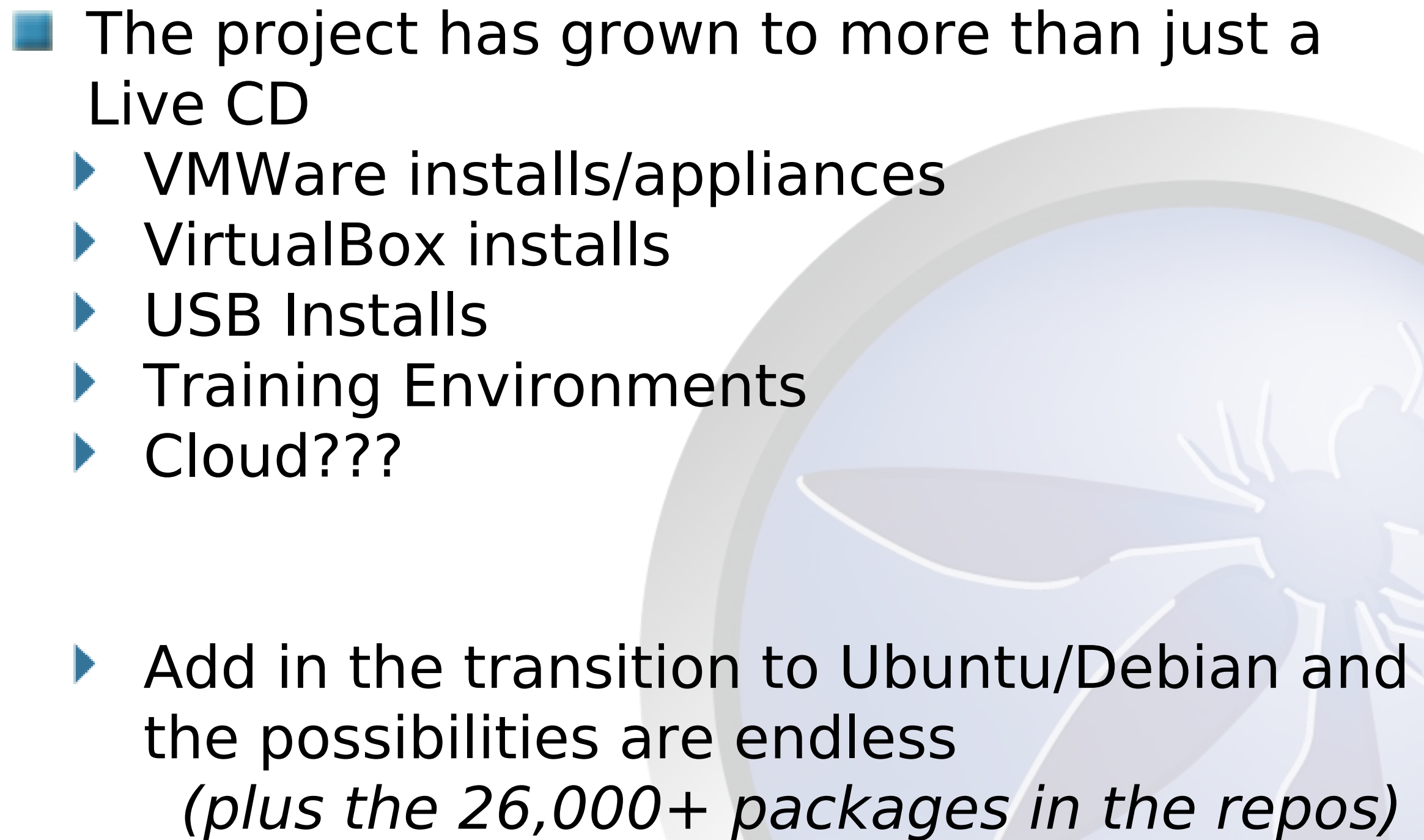
- ▶ ~5,094 GB of bandwidth since launch (Jul 2008)
- ▶ Most downloads in 1 month = 81,607 (Mar 2009)



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

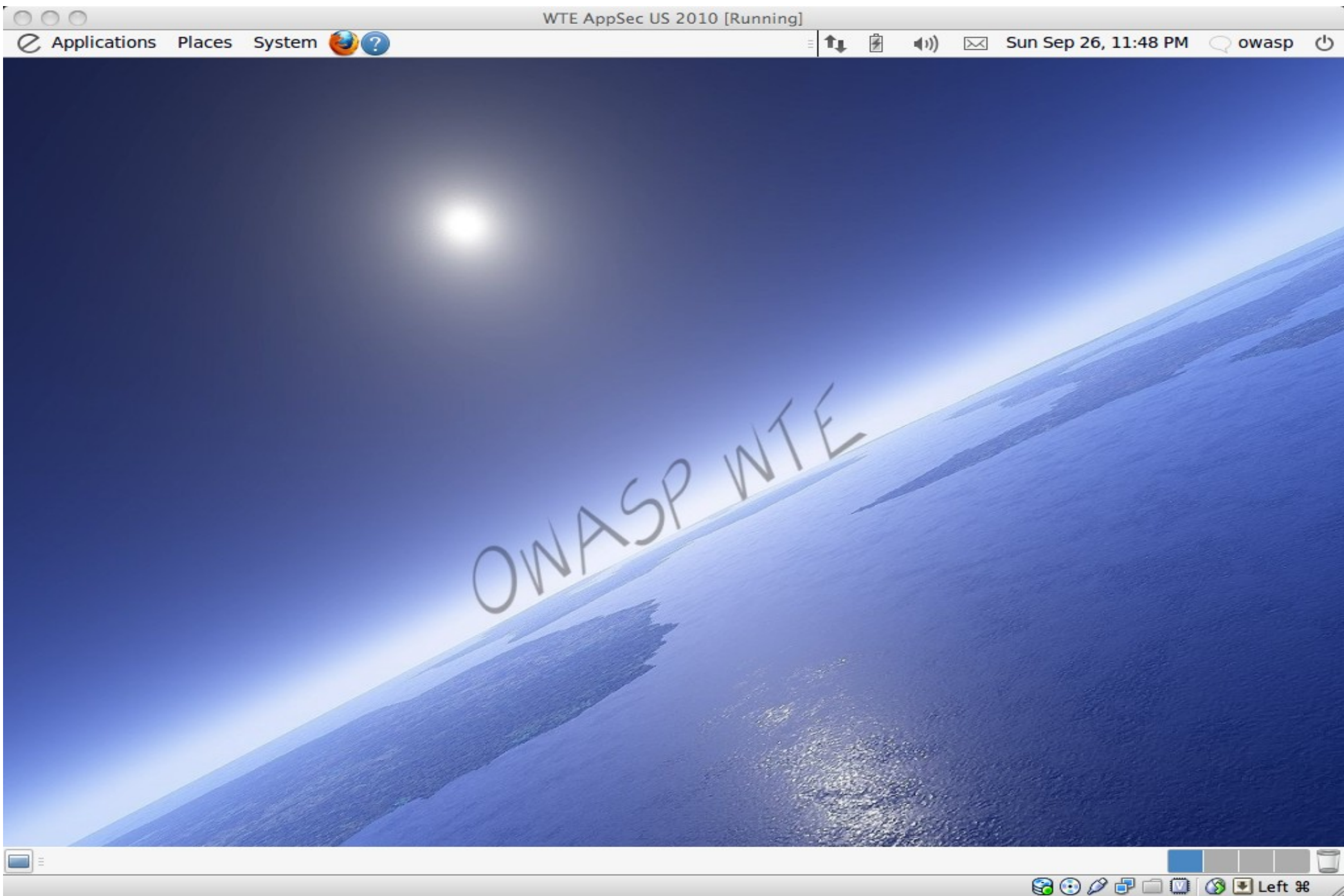
■ Design goals

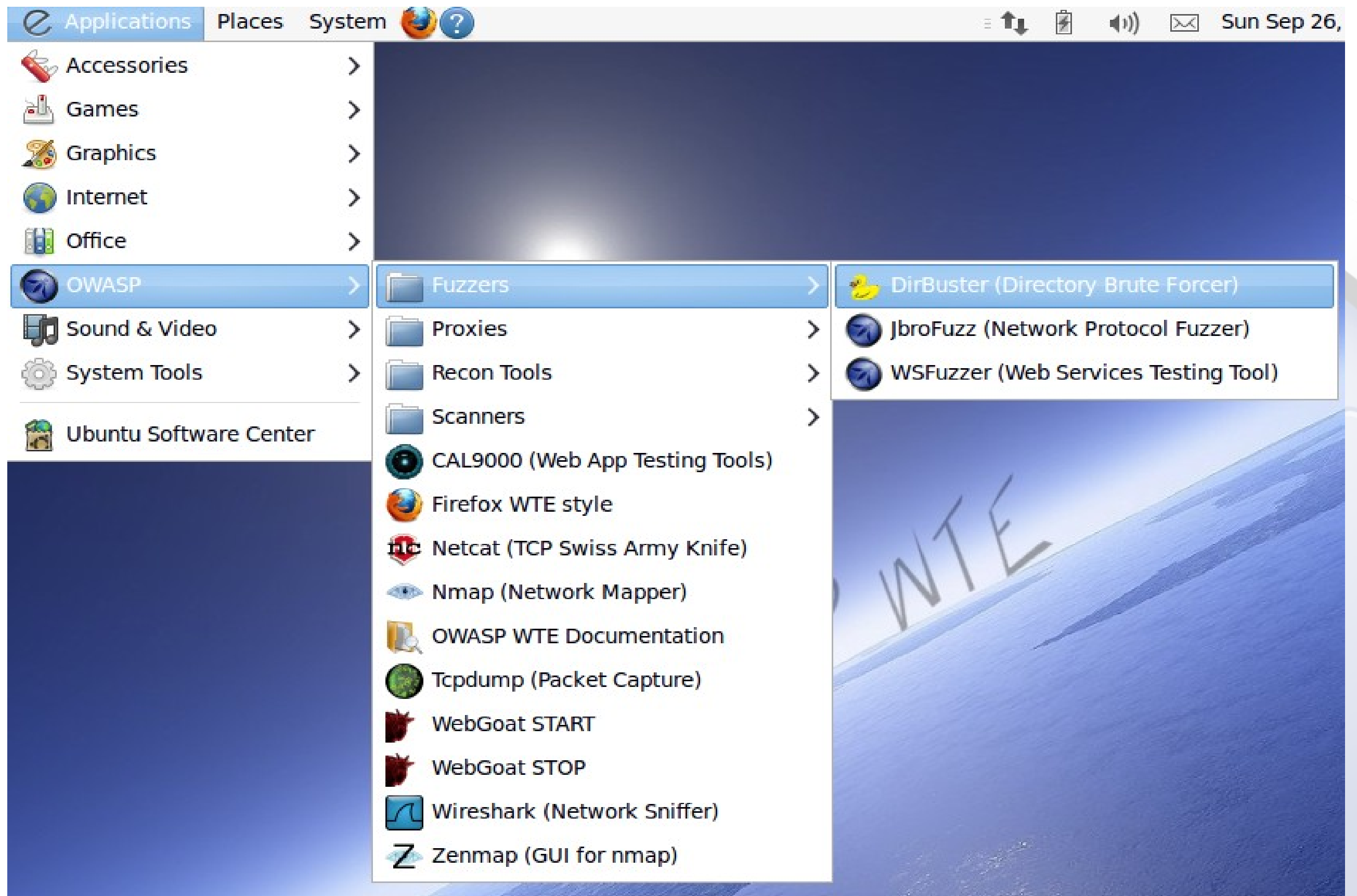
- ▶ Easy for users to keep updated
 - ▶ Easy for project lead to keep updated
 - ▶ Easy to produce releases (more on this later)
 - ▶ Focused on just application security – not general pen testing
- 



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:



Firefox

Others:



Metasploit



Httpprint



Maltego CE



netcat



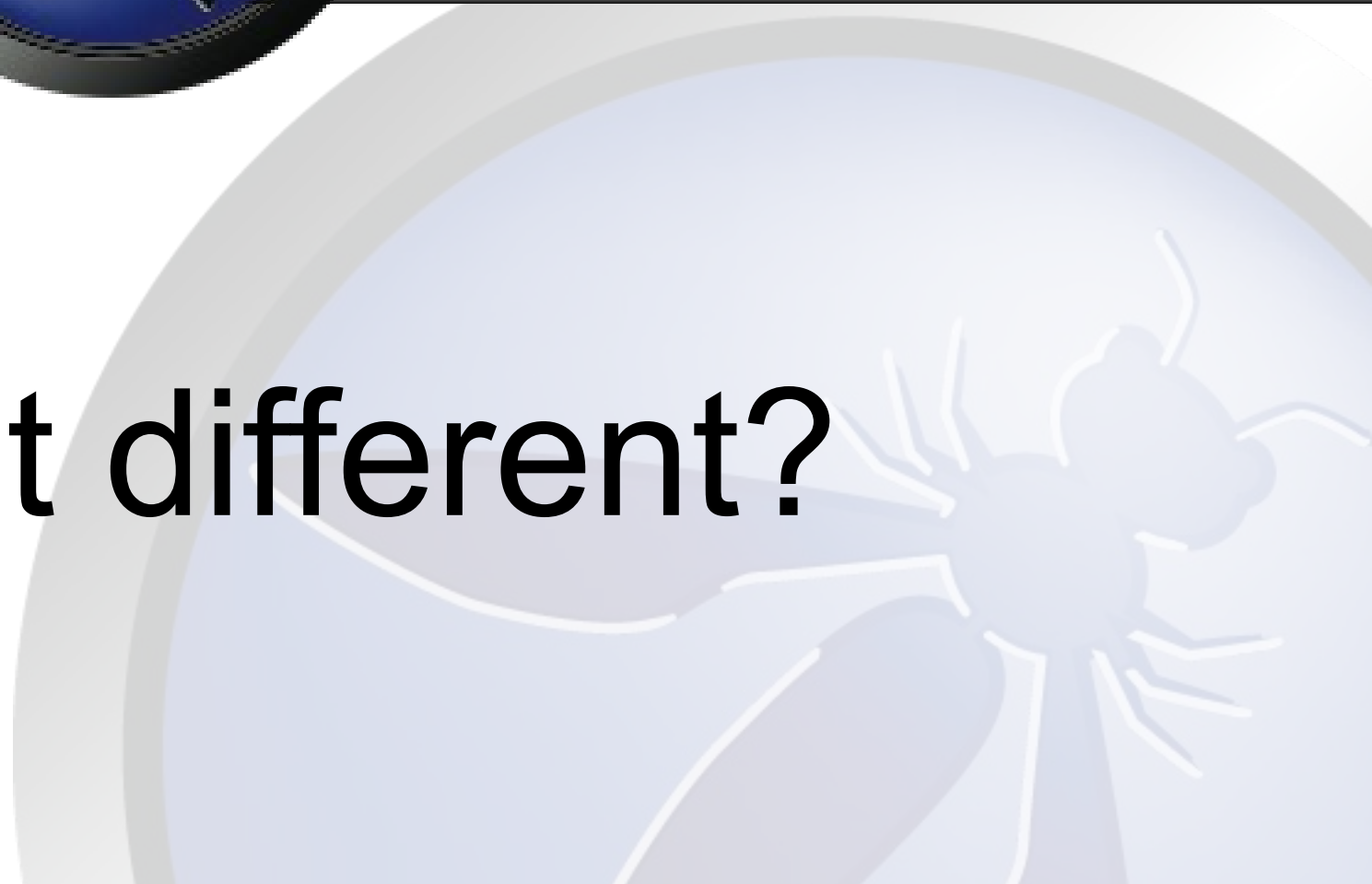
Wireshark







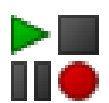


tcpdump



Why is it different?





 Add N Edit Cookies 0.2.1.3 Cookie Editor that allows you add and edit se	 No-Referer 1.3.1 Lets you open a tab without sending the HTTP referer information.
 CookiePie 1.0.2 Use multiple Web accounts and profiles in difi	 NoScript 1.9.2.6 Extra protection for your Firefox: NoScript allows JavaScript, Java (and other plu...
 DOM Inspector 2.0.3 Inspects the structure and properties of a win	 POW 0.1.8 A personal Web Server
 Firebug 1.3.3 Web Development Evolved.	 RefControl 0.8.11 Control what gets sent as the HTTP Referer on a per-site basis.
 FormFox 1.6.3 Pops up form action when submit button is at	 refspoof 0.9.5 Allows easy spoofing of URL referer (referrer) w/ toolbar.
 FoxyProxy 2.9 FoxyProxy - Premier proxy management for Fi	 Server Switcher 0.5 Switch between your development and live servers.
 Greasemonkey 0.8.20090123.1 A User Script Manager for Firefox	 SQL Injection! 1.2 Set all form fields free to test SQL Injections.
 HackBar 1.3.2 A toolbar that helps you find and test SQL inje	 Tamper Data 10.1.0 View and modify HTTP/HTTPS headers etc. Track and time requests.
 Header Spy 1.3.3.1 Shows HTTP headers on statusbar	 TestGen4Web - Script It All 1.0.0 Just like your VCR - for Firefox. It records what you do, stores it, and plays it bac...
 InspectThis 0.9.1 Inspect the current element with the DOM Ins	 UriParams 2.2.0 Displays GET/POST parameters in the sidebar.
 JSView 2.0.5 View the source code of external stylesheets	 User Agent Switcher 0.6.11 Adds a menu and a toolbar button to switch the user agent of the browser.
 Live HTTP headers 0.14 View HTTP headers of a page and while brow	 Web Developer 1.1.6 Adds a menu and a toolbar with various web developer tools.
 Modify Headers 0.6.6 Add, modify and filter http request headers	

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

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

Ctrl+F2

QuickAdd

Alt+F2

☐ Use Advanced Menus

categories

SP) is a
improving
s to make

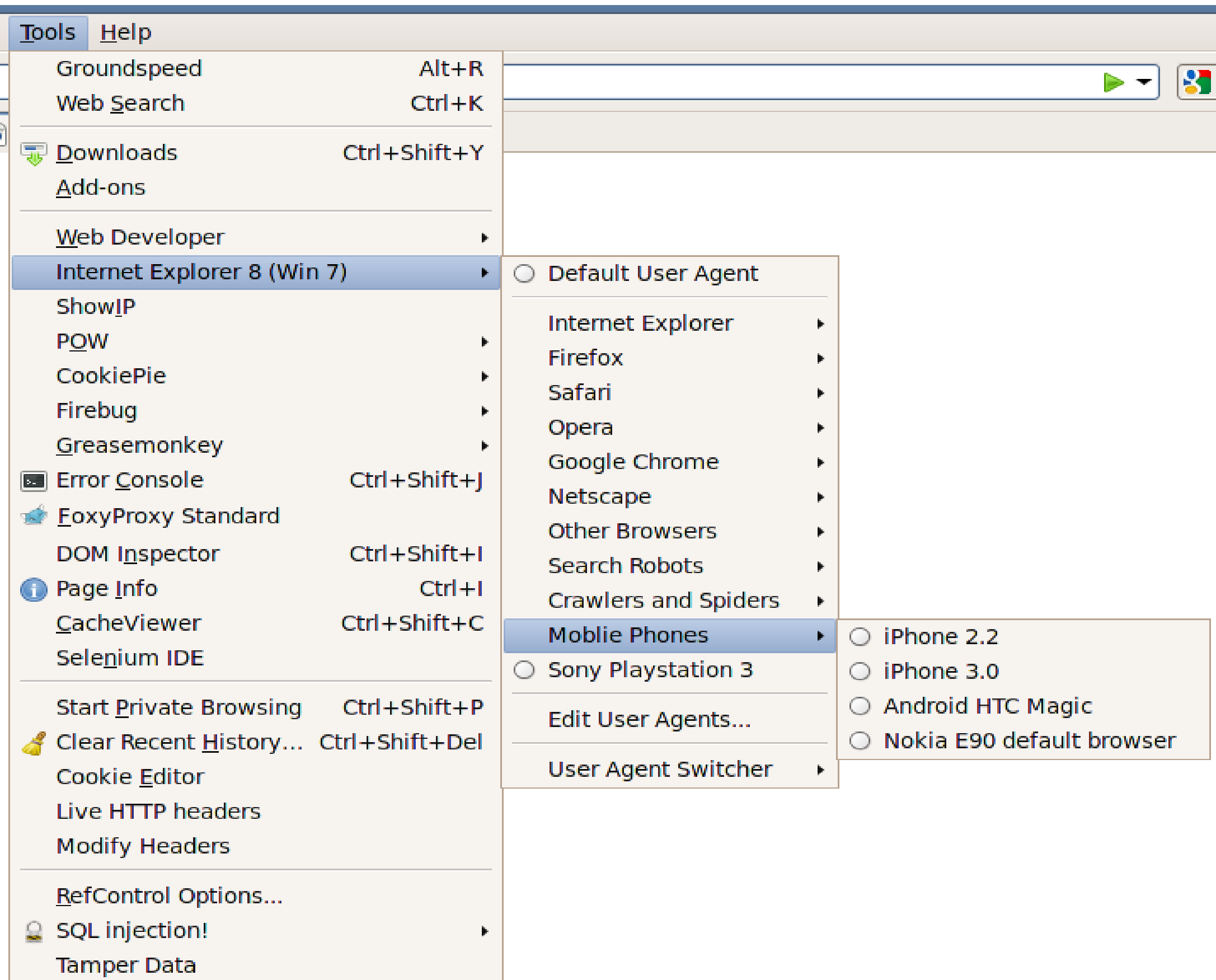
t true
icipate in
er a free

Apache/2.2.9...



FoxyProxy: Disabled





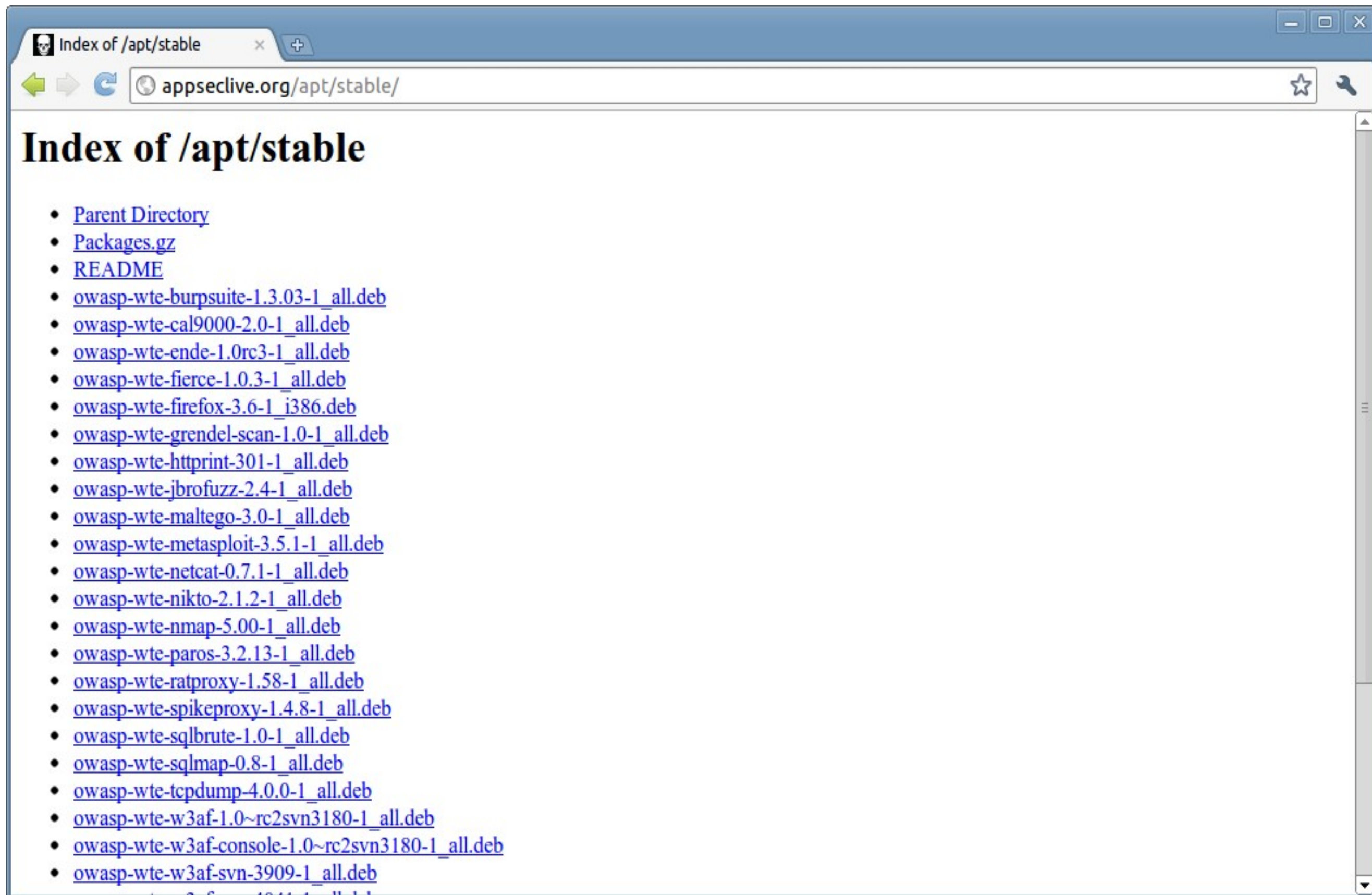
■ OWASP Documents

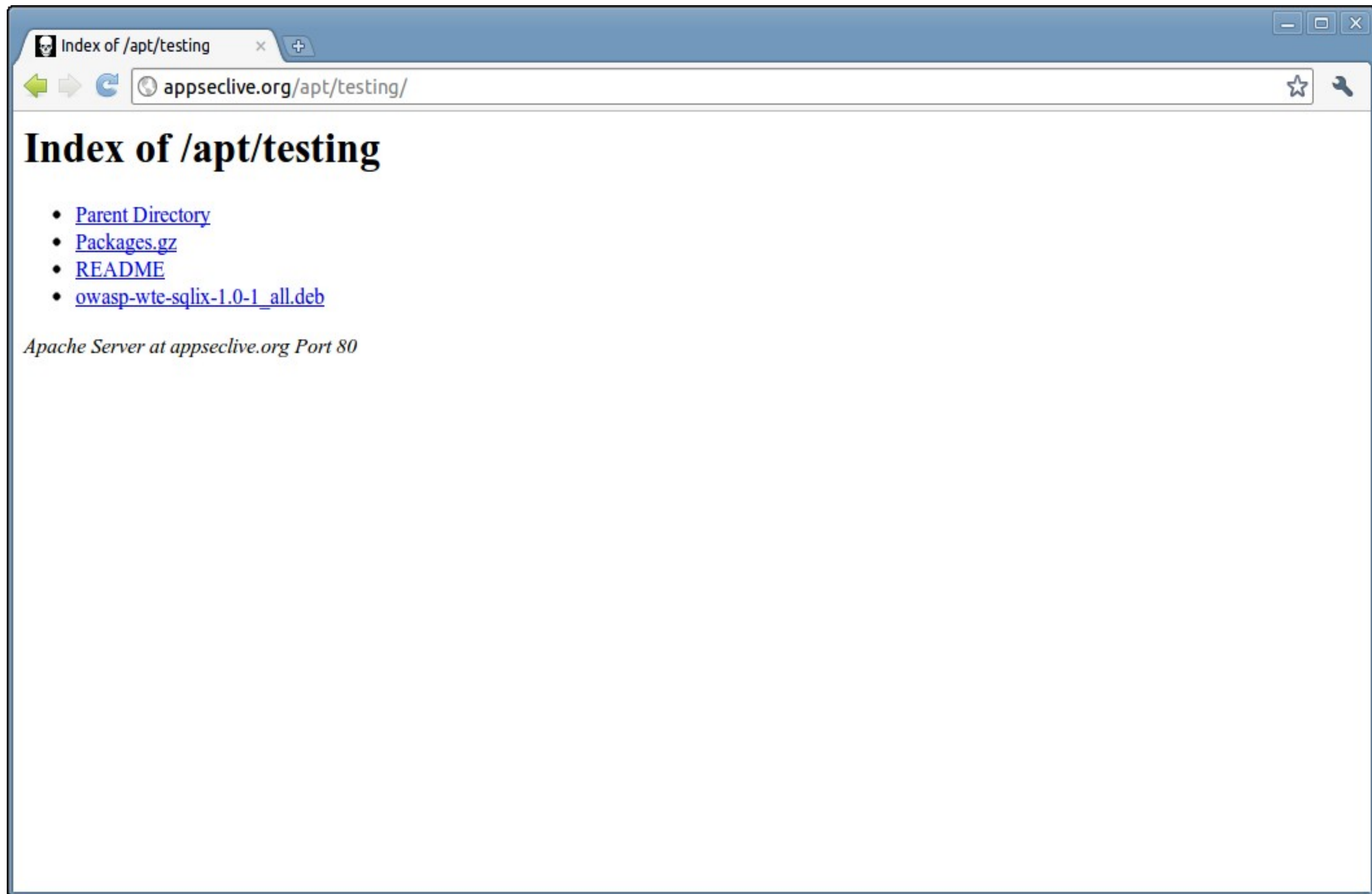
- ▶ Testing Guide v2 & v3
- ▶ CLASP and OpenSamm
- ▶ Top 10 for 2010
- ▶ Top 10 for Java Enterprise Edition
- ▶ AppSec FAQ
- ▶ Books – tried to get all of them
 - CLASP, Top 10 2010, Top 10 + Testing + Legal, WebGoat and Web Scarab, Guide 2.0, Code Review

■ Others

- ▶ WASC Threat Classification, OSTTMM 3.0 & 2.2







File

Edit

Package

Settings

Help

Reload

Mark All Upgrades

Apply

Properties

Quick search

Search

All

owasp-wte

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





Nikto is a...
owasp-wte-nikto

27 matching items

owasp-wte - Project Ho... x

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

My favorites | Sign in



owasp-wte

OWASP Web Testing Environment (WTE)

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 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.

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:

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

*

27



What is next?



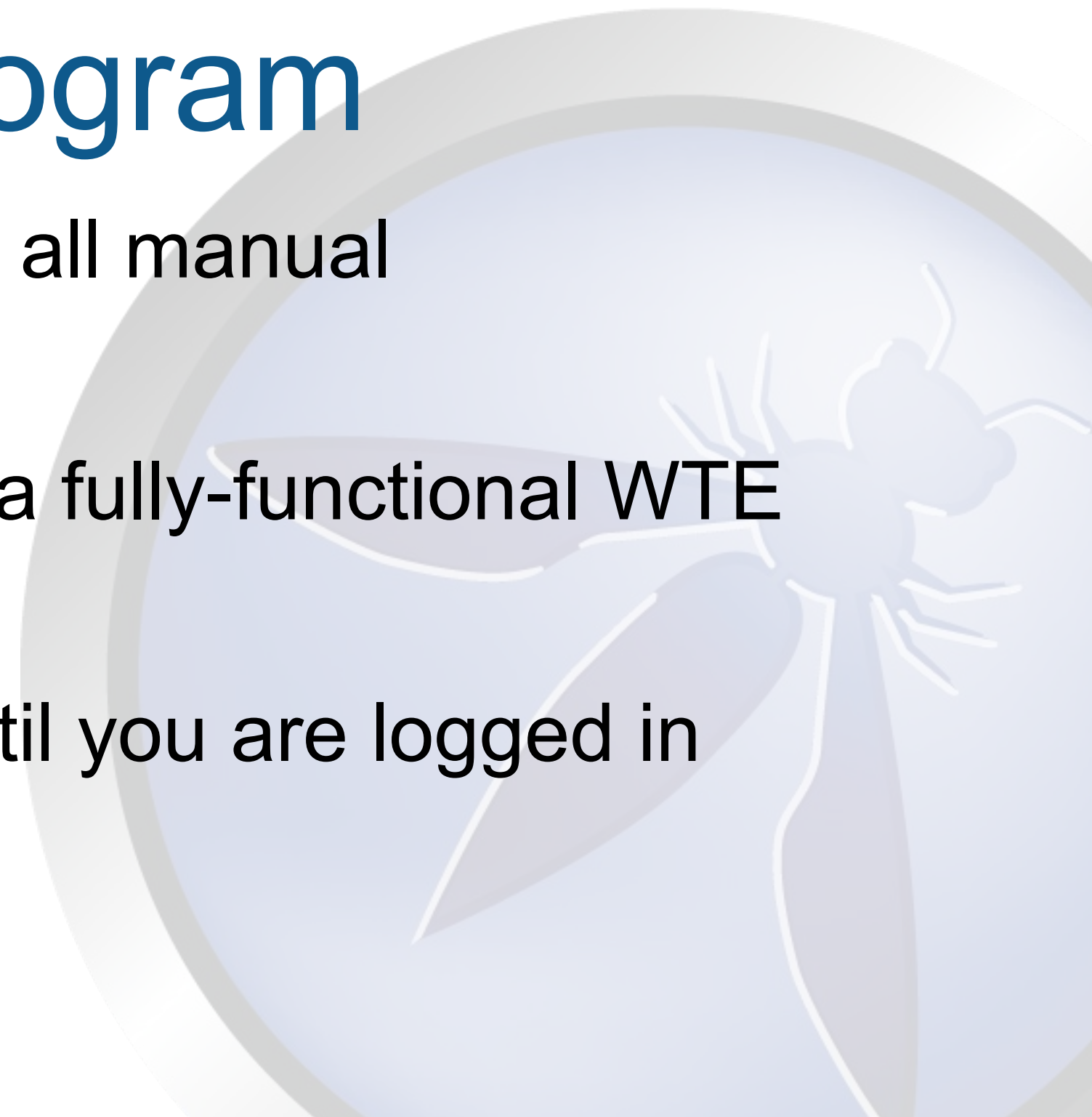


Cloud-ifying WTE

- 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

The screenshot shows a web browser window titled "Hosting - Cloud Servers - Mozilla Firefox". The address bar displays "Rackspace US, Inc. (US)" and the URL "https://manage.rackspacecloud.com/CloudServers/ServerList". The page header includes the Rackspace Cloud logo and support links: "Support: Cloud Status, Knowledge Base, Forums, Tickets, Live Chat", along with phone numbers "1-877-934-0407" and "0800-083-3012".

The left sidebar contains navigation links: Home, Hosting (selected), Cloud Files, Cloud Servers, Load Balancers, Your Account, Support, and Logout.

The main content area is titled "Cloud Servers" and contains a blue informational box stating: "The cloud servers in your account are listed below. Click on the link in the Server Name column to manage the server and its settings. Please note that servers in this list accumulate usage fees regardless of their operational status. If you no longer wish to be billed for a server you must delete the server from your account."

Below the box are two tabs: "Server Instances" (selected) and "My Server Images". The "Server Instances" tab shows "0 Server(s)" and includes "Add Server" and "Delete Selected" buttons. A search bar is also present.

A table with the following headers is shown: Status, Server Name, RAM Amount, Primary IP, Distribution, and Datacenter. The table body contains the message: "There is currently no data to display in this table."

The footer includes the text: "For helpful apps and tools check out Cloud Tools and the Rackspace Cloud iPhone page." and "Control Panel Version 2.2.2 - Release Notes".

Step 2: Select Ubuntu/Debian

The screenshot shows the Rackspace Cloud management interface in a Mozilla Firefox browser window. The page title is "Hosting - Select an image from one of the tabs below. - Mozilla Firefox". The address bar shows the URL "https://manage.rackspacecloud.com/CloudServers/AddNew". The Rackspace Cloud logo is in the top left, and support links are in the top right. A left sidebar contains navigation links: Home, Hosting, Cloud Files, Cloud Servers, Load Balancers, Your Account, Support, and Logout. The main content area has tabs for "Linux", "Windows", and "My Server Images". Below the tabs, it says "19 Linux Images (Showing 1 to 19)". A table lists the images:

OS	Image	Select
ubuntu	Ubuntu 10.04 LTS (Lucid Lynx)	Select
ubuntu	Ubuntu 10.10 (Maverick Meerkat)	Select
ubuntu	Ubuntu 11.04 (Natty Narwhal)	Select
ubuntu	Ubuntu 8.04.2 LTS (Hardy Heron)	Select

The "Ubuntu 10.10 (Maverick Meerkat)" row is highlighted with a red box. At the bottom, there is a footer with links to "Cloud Tools" and "Rackspace Cloud iPhone page", and a version note "Control Panel Version 2.2.2 - Release Notes".

Step 3: Choose Name & RAM

Support: Cloud Status Knowledge Base Forums Tickets Live Chat

Server Configuration

Required items are marked with a red square (■).

Image: Ubuntu 10.10 (Maverick Meerkat)

Server Name

■ wte-test

Only alphanumeric characters, periods, and hyphens are valid. Server Name cannot start or end with a period or hyphen.

Server Size

■

	RAM	Disk	Price Per Hour
<input type="radio"/>	256 MB	10 GB	\$0.015
<input type="radio"/>	512 MB	20 GB	\$0.03
<input type="radio"/>	1024 MB	40 GB	\$0.06
<input checked="" type="radio"/>	2048 MB	80 GB	\$0.12
<input type="radio"/>	4096 MB	160 GB	\$0.24
<input type="radio"/>	8192 MB	320 GB	\$0.48
<input type="radio"/>	15872 MB	620 GB	\$0.96

Cancel Create Server

Step 4: Start your server

The screenshot shows the Rackspace Cloud Servers Overview page in a Mozilla Firefox browser. The browser's address bar displays the URL <https://manage.rackspacecloud.com/CloudServers/Overview>. The page features a sidebar with navigation links: Home, Hosting, Cloud Files, Cloud Servers, Load Balancers, Your Account, Support, and Logout. The main content area is titled "wte-test" and includes tabs for Overview, DNS, Images, and Diagnostics. The "Overview" tab is selected, showing "Cloud Server Details" for a server named "wte-test". The server's status is "Active", and its current action is "None". Technical details listed include 2048 MB of RAM, 80 GB of disk space, and 0.00 GB of bandwidth in and out. A "Change Name" link is visible next to the server name. The footer of the page provides links to Cloud Tools and the Rackspace Cloud iPhone page, along with the Control Panel Version 2.2.2 and Release Notes.

Hosting - Overview - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Hosting - Overview

Rackspace US, Inc. (US) <https://manage.rackspacecloud.com/CloudServers/Overview> Google

the rackspacecloud

Support: [Cloud Status](#) [Knowledge Base](#) [Forums](#) [Tickets](#) [Live Chat](#) [1-877-934-0407](#) [0800-083-3012](#)

Home

Hosting

Cloud Files

Cloud Servers

Load Balancers

Your Account

Support

Logout

Cloud Servers Overview

wte-test

Overview DNS Images Diagnostics

Cloud Server Details

Name & Status

Name: wte-test [Change Name](#)

Status: Active

Current Action: None

Age: 0 Days

Technical Details

RAM: 2048 MB

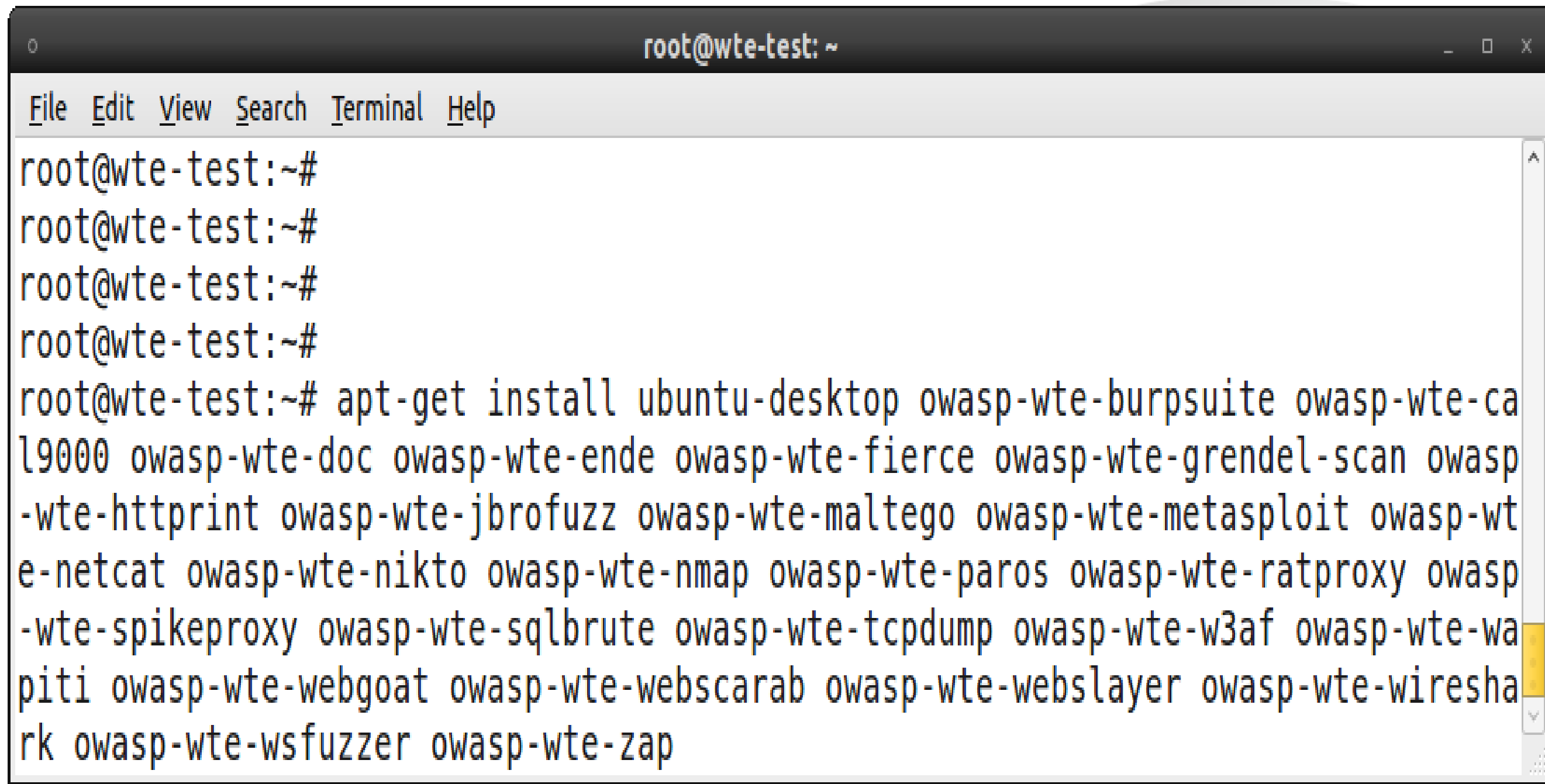
Disk Space: 80 GB

Bandwidth In: 0.00 GB

Bandwidth Out: 0.00 GB

For helpful apps and tools check out [Cloud Tools](#) and the [Rackspace Cloud iPhone page](#). Control Panel Version 2.2.2 - [Release Notes](#)

Step 5: Install Desktop + WTE

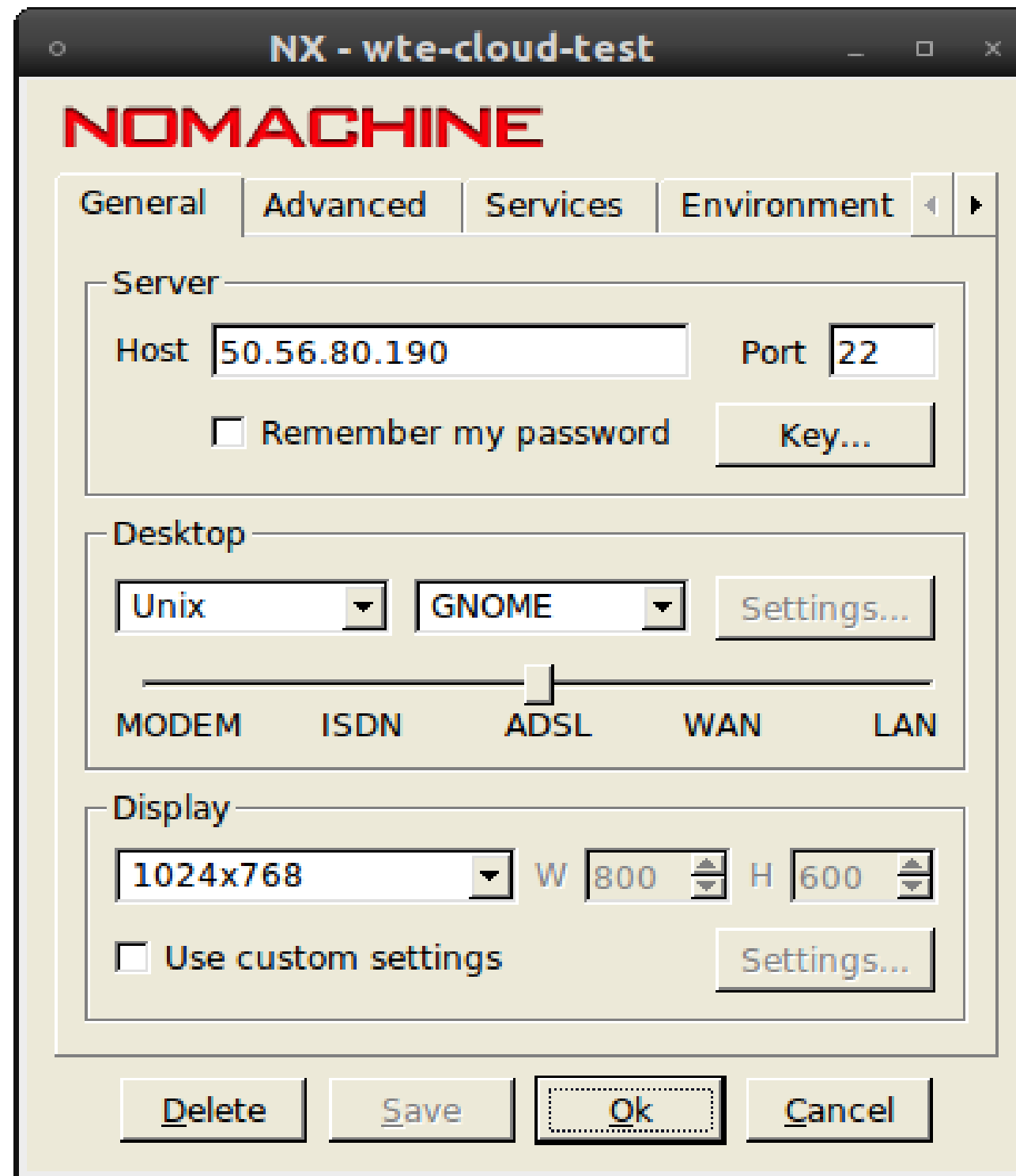


```
root@wte-test: ~  
File Edit View Search Terminal Help  
root@wte-test:~#  
root@wte-test:~#  
root@wte-test:~#  
root@wte-test:~#  
root@wte-test:~# apt-get install ubuntu-desktop owasp-wte-burpsuite owasp-wte-ca  
l9000 owasp-wte-doc owasp-wte-ende owasp-wte-fierce owasp-wte-grendel-scan owasp  
-wte-httpprint owasp-wte-jbrofuzz owasp-wte-maltego owasp-wte-metasploit owasp-wt  
e-netcat owasp-wte-nikto owasp-wte-nmap owasp-wte-paros owasp-wte-ratproxy owasp  
-wte-spikeproxy owasp-wte-sqlbrute owasp-wte-tcpdump owasp-wte-w3af owasp-wte-wa  
piti owasp-wte-webgoat owasp-wte-webscarab owasp-wte-webslayer owasp-wte-wiresha  
rk owasp-wte-wsfuzzer owasp-wte-zap
```

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



The image shows a screenshot of the 'NX - wte-cloud-test' window. The window has a title bar with standard window controls. Below the title bar, the text 'NOMACHINE' is displayed in red. There are four tabs: 'General', 'Advanced', 'Services', and 'Environment'. The 'General' tab is selected. The 'Server' section contains a 'Host' field with the value '50.56.80.190', a 'Port' field with the value '22', a checkbox for 'Remember my password' which is unchecked, and a 'Key...' button. The 'Desktop' section contains two dropdown menus: 'Unix' and 'GNOME', a 'Settings...' button, and a horizontal slider with labels 'MODEM', 'ISDN', 'ADSL', 'WAN', and 'LAN'. The 'Display' section contains a dropdown menu with '1024x768', 'W' and 'H' labels with '800' and '600' respectively, a checkbox for 'Use custom settings' which is unchecked, and a 'Settings...' button. At the bottom of the window are four buttons: 'Delete', 'Save', 'Ok', and 'Cancel'.

NOMACHINE

General Advanced Services Environment

Server

Host 50.56.80.190 Port 22

☐ Remember my password Key...

Desktop

Unix GNOME Settings...

MODEM ISDN ADSL WAN LAN

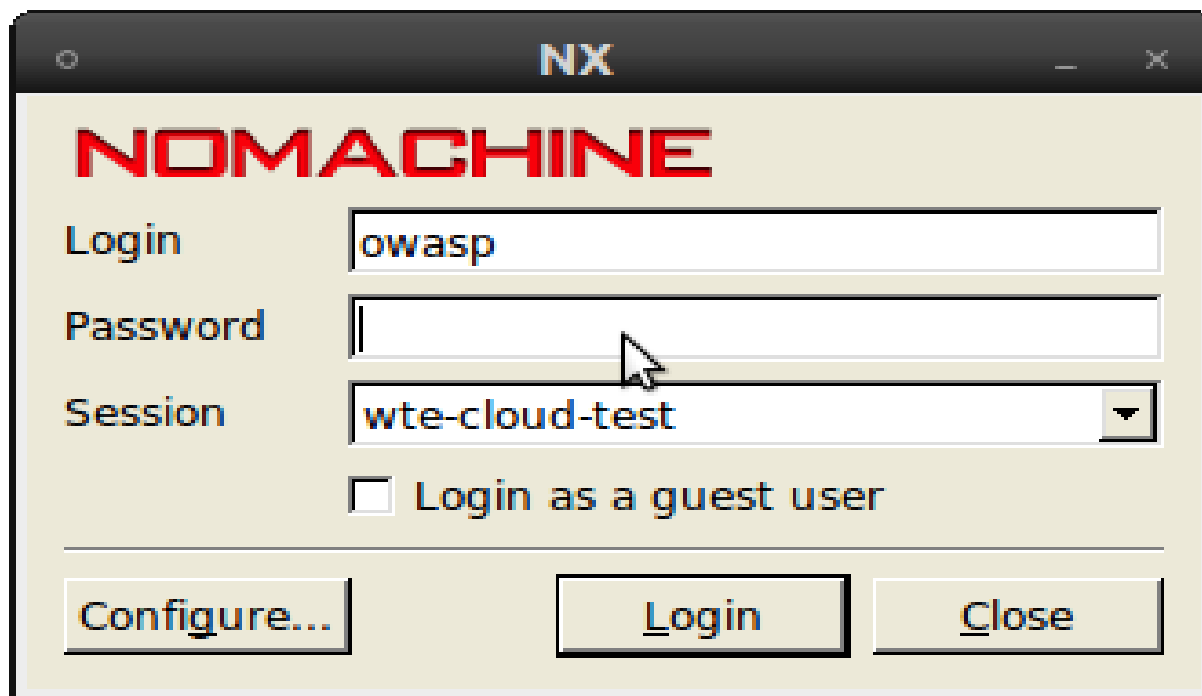
Display

1024x768 W 800 H 600

☐ Use custom settings Settings...

Delete Save Ok Cancel

Step 8: Connect to WTE



The image shows a window titled "NX" with a light beige background. At the top, the word "NOMACHINE" is written in large, bold, red letters. Below this, there are three input fields: "Login" with the text "owasp", "Password" which is empty, and "Session" with a dropdown menu showing "wte-cloud-test". Below the input fields is a checkbox labeled "Login as a guest user" which is unchecked. At the bottom of the window are three buttons: "Configure...", "Login", and "Close".

NX

NOMACHINE

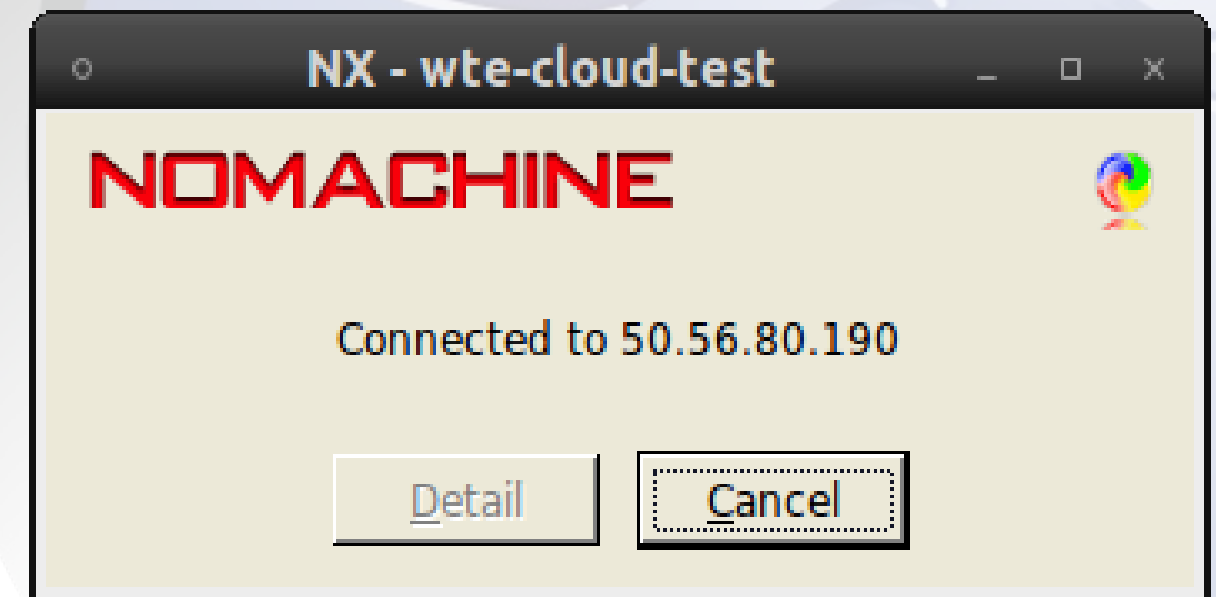
Login: owasp

Password:

Session: wte-cloud-test

☐ Login as a guest user

Configure... Login Close



The image shows a window titled "NX - wte-cloud-test" with a light beige background. At the top, the word "NOMACHINE" is written in large, bold, red letters. To the right of the text is a small, colorful circular icon. Below the text, it says "Connected to 50.56.80.190". At the bottom of the window are two buttons: "Detail" and "Cancel".

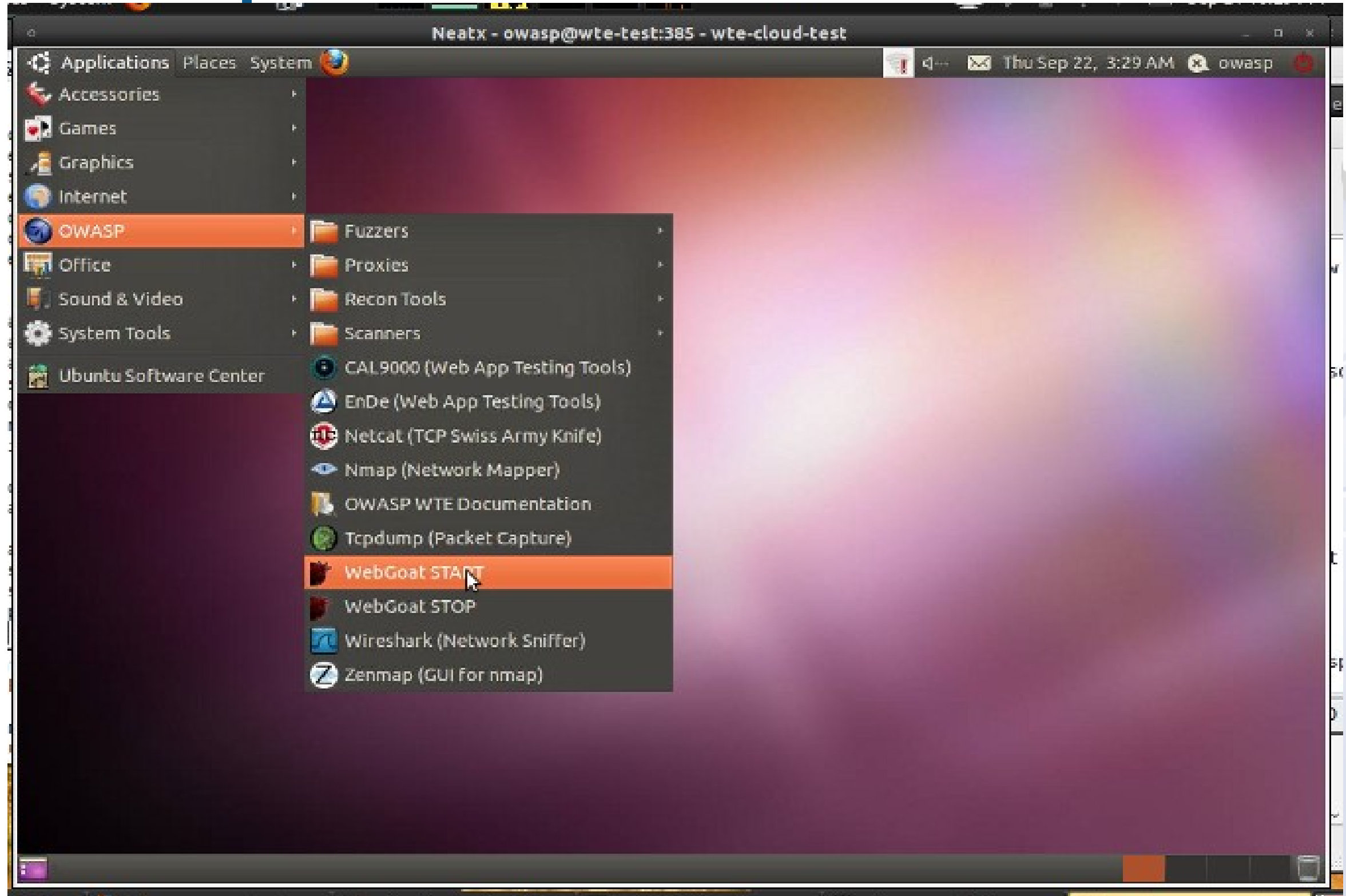
NX - wte-cloud-test

NOMACHINE

Connected to 50.56.80.190

Detail Cancel

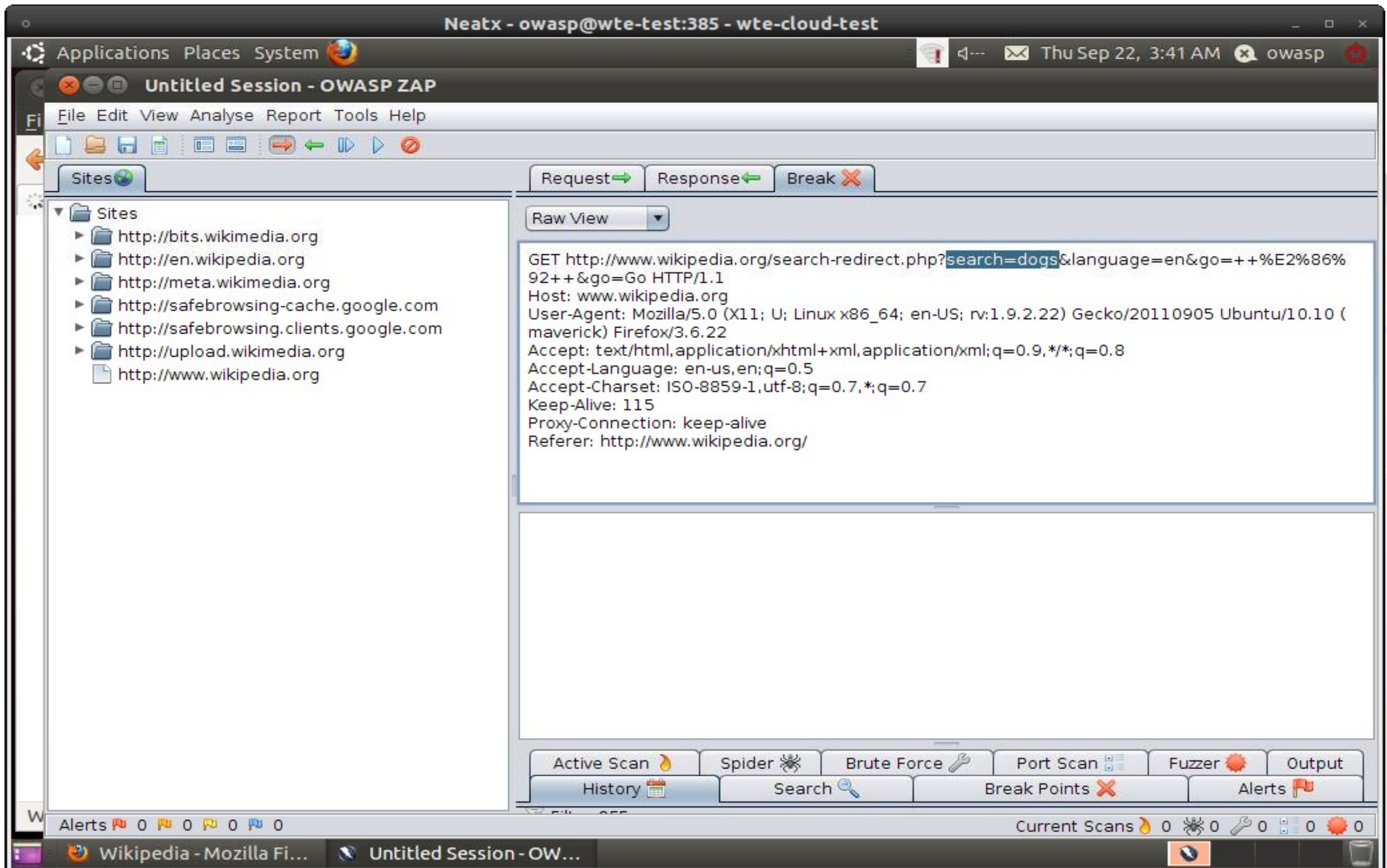
Step 9: WTE ala Cloud



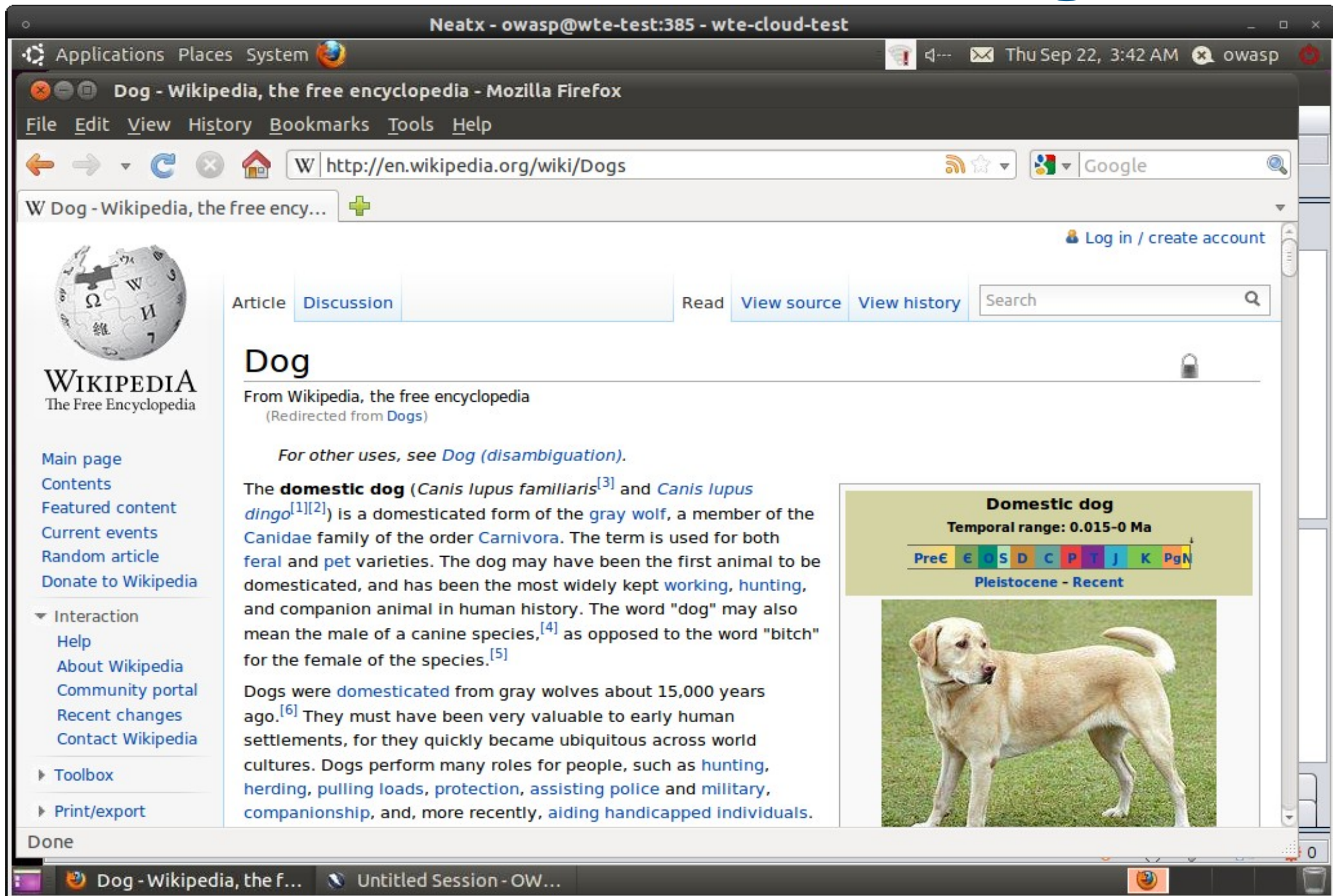
Step 10: Test Connectivity



Step 11: Test the Tools



Turn Cats into Dogs



Step 12: Check your bill

+ Cloud Servers Usage Summary

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

1 Servers (Showing 1 to 1)						<input type="text"/>
Server Name	Disk Space (GB)	Bandwidth In (GB)	Bandwidth Out (GB)	Total Uptime	Running Charges	
wte-test	80	1.13	0.02	0 Day(s) 01:53:54	\$0.23	

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:
(average time per server)

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

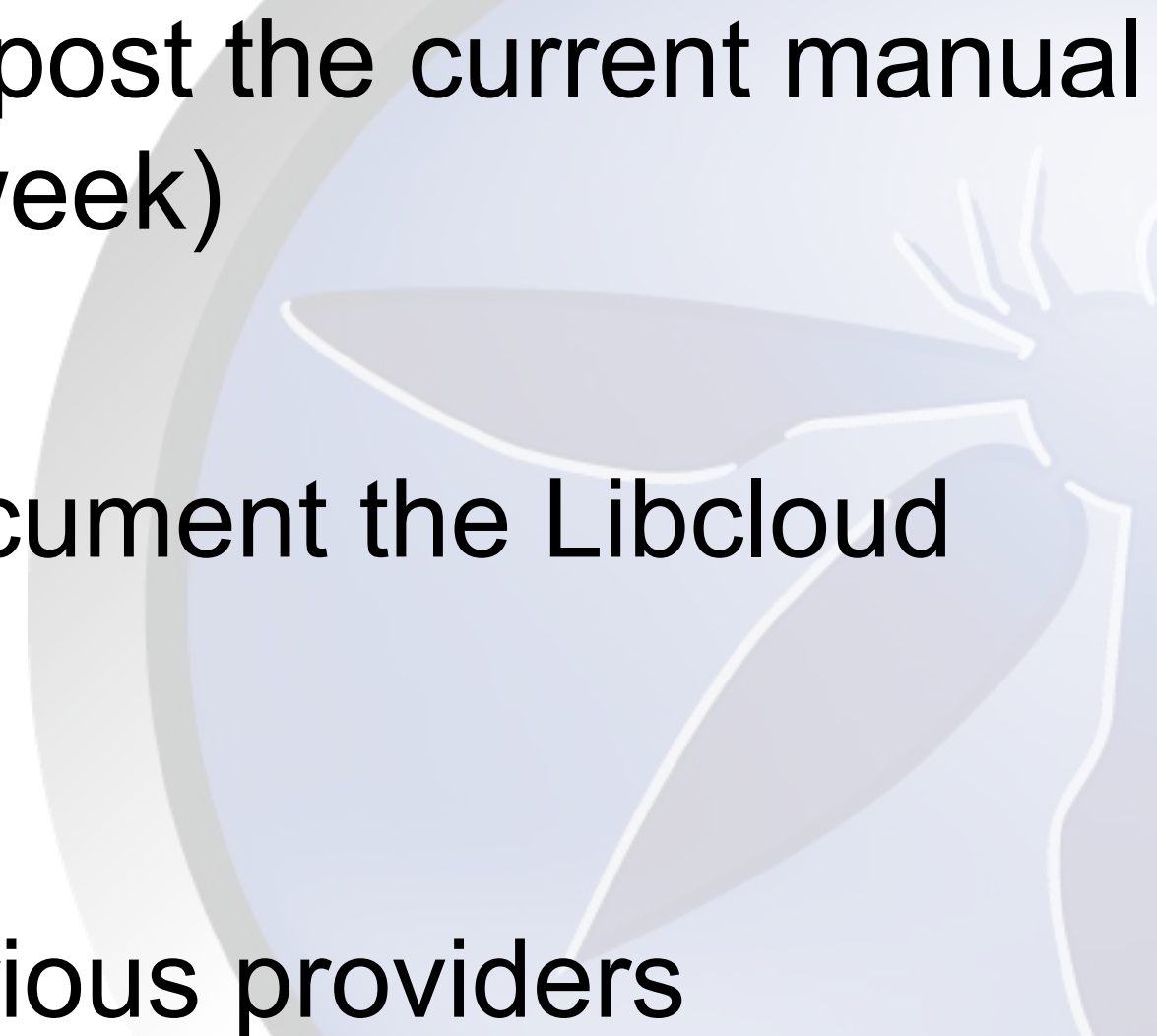
- Python library to abstract away differences between multiple cloud provider APIs
 - ▶ Cloud Servers
 - ▶ Cloud Storage
 - ▶ Cloud Load balancers
- Supports 24 different providers

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

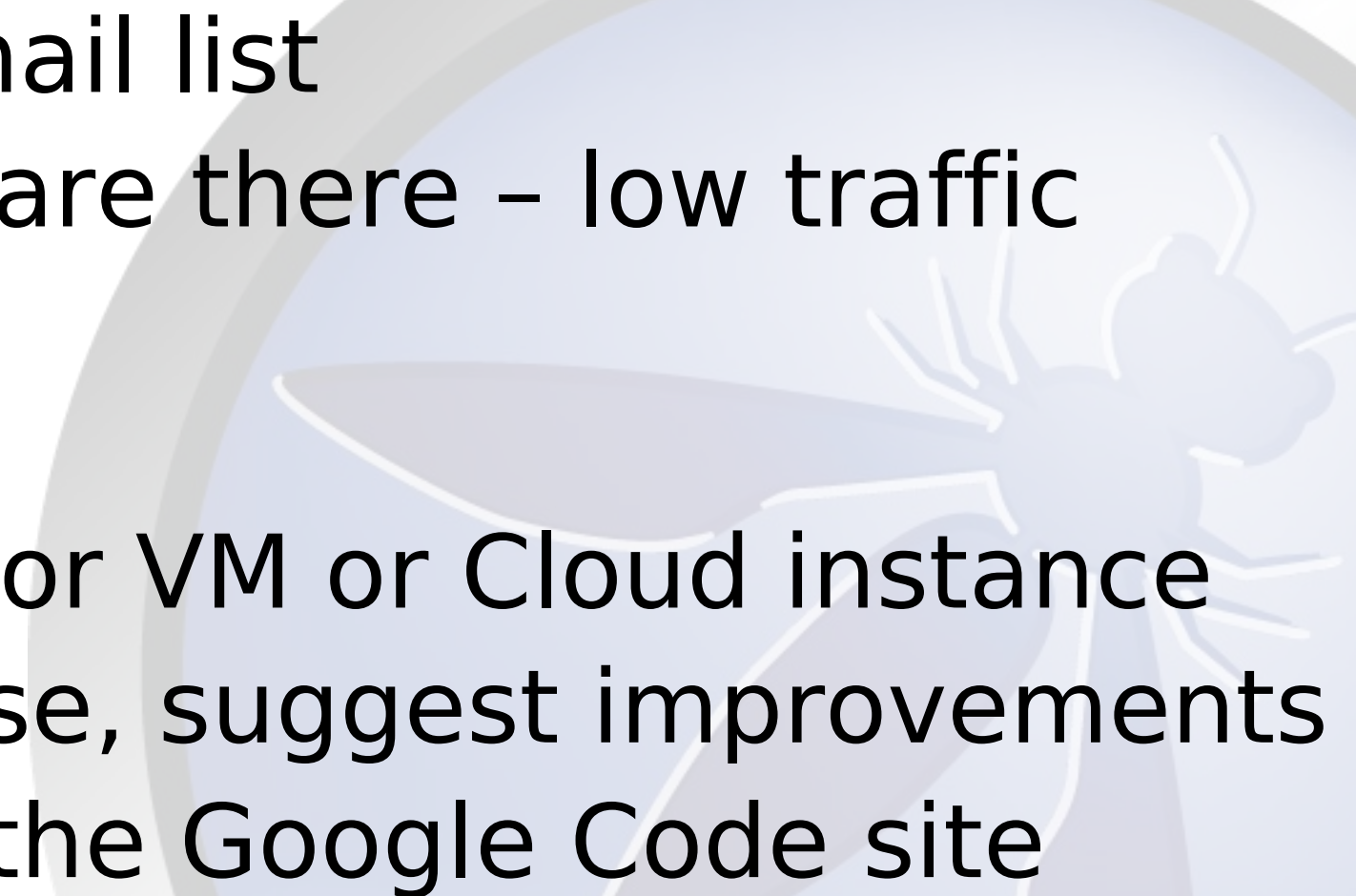


Current Issues

- Yikes AMD64 CPU
 - ▶ sqlmap is missing a dependency
 - ▶ WTE Firefox is for i386
 - ▶ NX server is a bit tricky
- The WTE theme gets lost

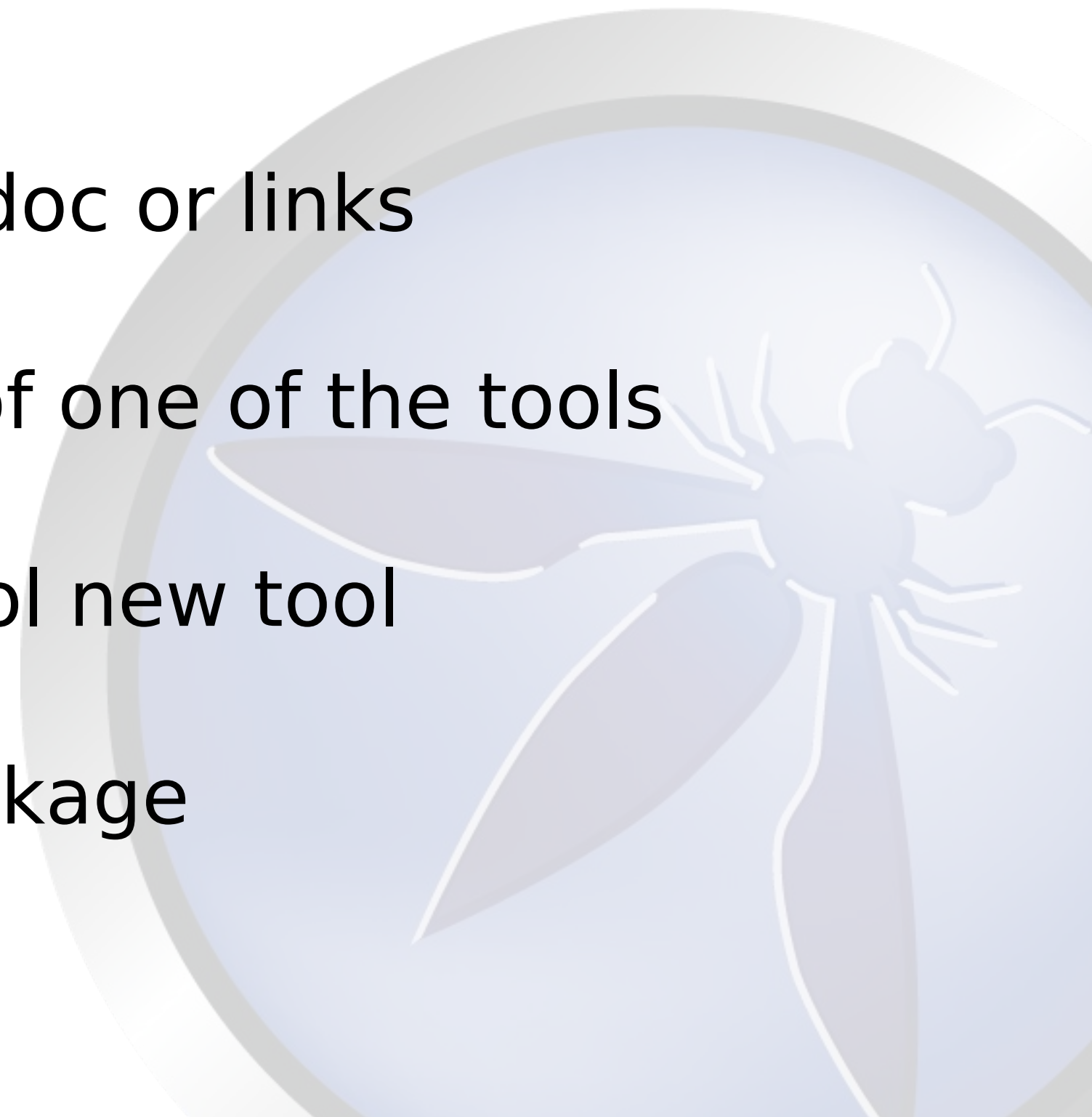


How can you get involved?

- ▶ 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

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/>



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

