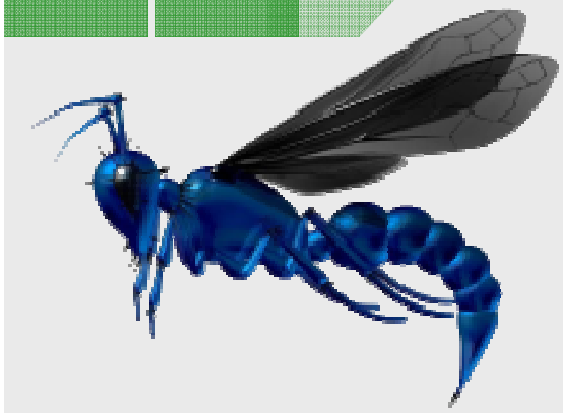


OWASP Live CD: An open environment for web application security.

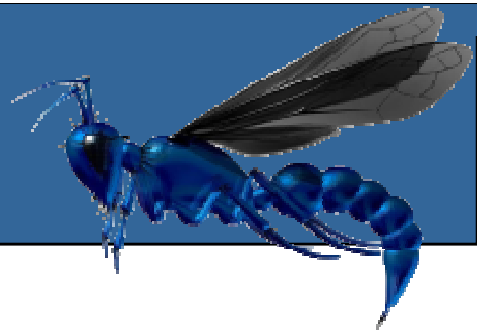
Matt Tesauro
OWASP Live CD project lead
OWASP Global Project Committee
Texas Education Agency
mtesauro@gmail.com

The OWASP Foundation
http://www.owasp.org

Presentation Overview

- Who am I and what's this OWASP Live CD thing anyway?
- Where are we now?
- Where are we going?
- How can I get involved?
- What else is out there?

About me

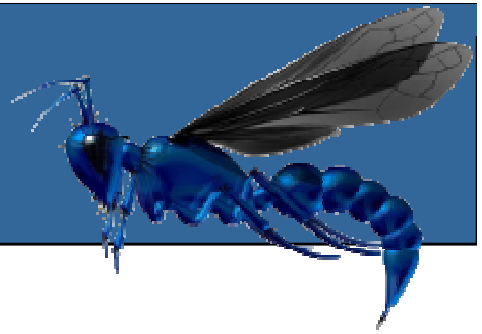


- Varried IT Background
  - Developer, DBA, Sys Admin, Pen Tester, Application Security, CISSP, CEH, RHCE, Linux+
- Long history with Linux & Open Source
  - First Linux install ~1998
  - DBA and Sys Admin was all open source
  - Last full-time commercial OS = Windows 2000
  - Contributor to many projects, leader of one

Project History

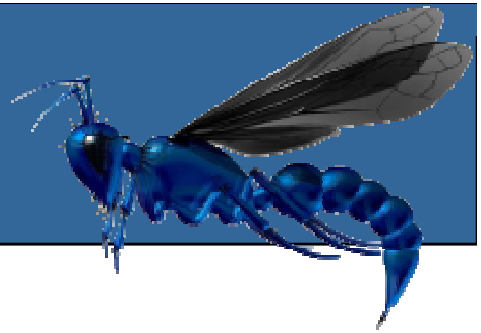
- Started as a Summer of Code 2008 project
  - SoC Project to update previous OWASP Live CD
  - Autumn of Code 2006 & Spring of Code 2007
  - Lab Rat (v 2.1)
  - Morphix (Debian derivative)
  - Appeared dormant to me
- Applied and was sponsored
  - March 25th, 2008 submitted my application
  - Sept. 15th, 2008 completed the SoC project

Project Goals (post SoC)



- 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 (maybe quarterly)
  - Focused on just application security – not general pen testing

Pseudocode

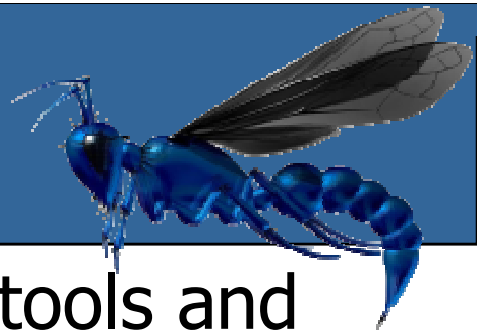



OWASP
Live CD 2008
The Open Web Application Security Project

!=

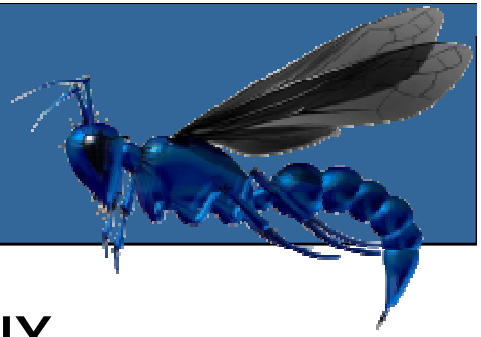

back|track

General goals going foward



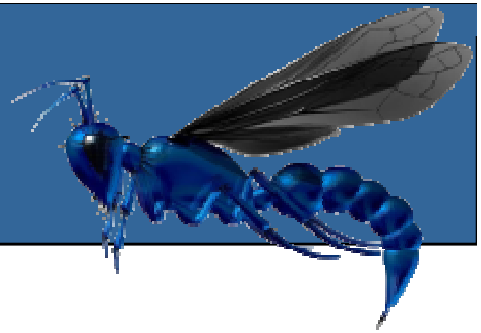
- Provide a showcase for great OWASP tools and documentation
- Provide the best, freely distributable applicaton security tools/documents in an easy to use package
- Ensure that the tools provided are easy to use as possible
- Continue to document how to use the tools and how the modules were created
- Align the tools with the OWASP Testing Guide v3

Why SLAX?



- OWASP Live CD is based on SLAX Linux
  - SLAX is a Linux distro based on Slackware specifically made for live CDs
  - Easy to make & update modules
  - Breaks creating new modules into small units
  - Comes with some great module building tools
  - Proven track record (Backtrack, Whax, DAVIX, ...)
  - Defaults to KDE – easy transition from Windows
  - Allow for some future cool stuff
    - more on this later.

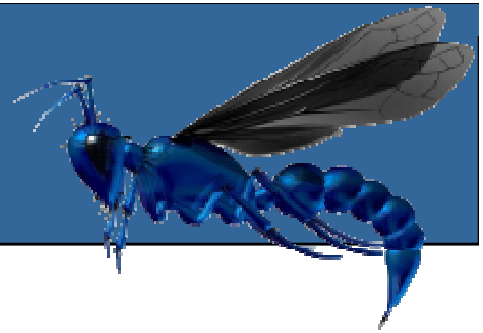
Where are we now?



- Current Release
  - AustinTerrier Feb 2009
- Previous Releases
  - Portugal Release Dec 2008
  - SoC Release Sept 2008
  - Beta1 and Beta2 releases during the SoC

- Overall downloads = 75,219 (as of 2009-03-07)
  - ~888 GB of bandwidth since launch (July 2008)
  - March downloads 6,257 (first 7 days)

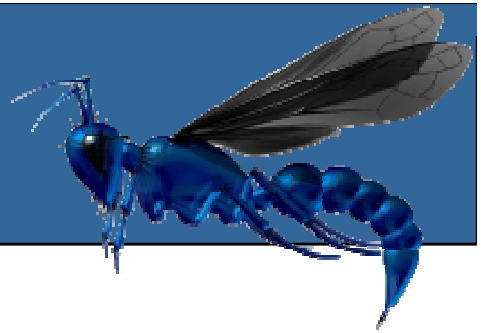
Available Tools



25 “significant” tools

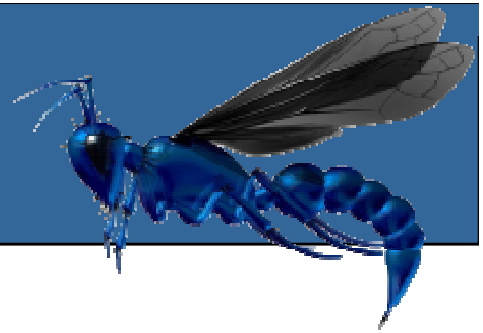
OWASP WebScarab v20090122	OWASP WebGoat v5.2	OWASP CAL9000 v2.0	OWASP JBroFuzz v1.2	OWASP DirBuster v0.12
OWASP SQLiX v1.0	OWASP WSFuzzer v1.9.4	OWASP Wapiti v2.0.0-beta	Paros Proxy v3.2.13	nmap & Zenmap v 4.76
Wireshark v1.0.5	tcpdump v4.0.0	Firefox 3.06 + 25 addons	Burp Suite v1.2	Grendel Scan v1.0
Metasploit v3.2 (svn)	w3af + GUI svn r2161	Netcats – original + GNU	Nikto v2.03	Firece Domain Scanner v1.0.3
Maltego CE v2-210	Httprint v301	SQLBrute v1.0	Spike Proxy v1.4.8-4	Rat Proxy v1.53-beta

Documentation available



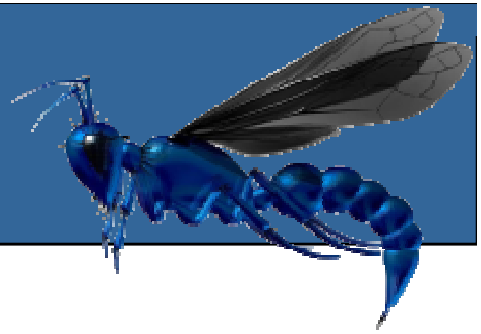
- OWASP Documents
  - Testing Guide v2 & v3
  - CLASP
  - Top 10 for 2007
  - Top 10 for Java Enterprise Edition
  - AppSec FAQ
  - Books
    - CLASP, Top 10 2007, Top 10 + Testing + Legal, WebGoat and Web Scarab, Guide 2.0, Code Review
- Others
  - WASC Threat Classification, OSTTMM 3.0 & 2.2

Support Modules



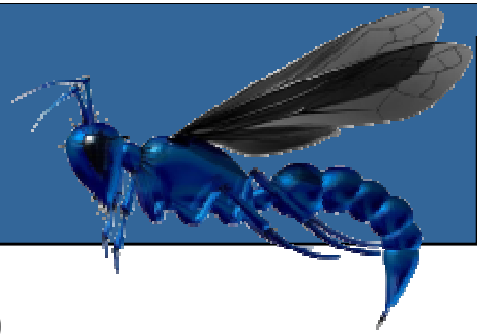
- OWASP Branding Module
- Subversion client
- JRE 6 update 6
- Python 2.5.2
- Ruby 1.8.1
- Graphviz
- tidy
- GnuTLS
- wget, host, dig, openssl, grep, whois

Bonus Features



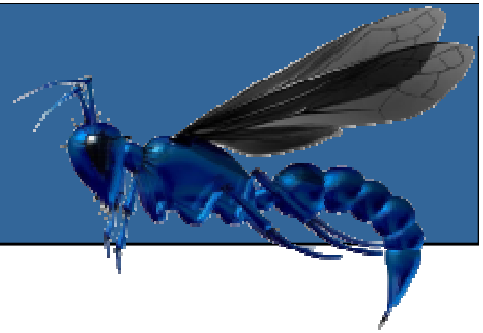
- 331 tools enumerated & documented
  - Potential Tool list
  - Name, website, License, Installation source, OWASP Tool?, Notes, Page numbers for tools in OWASP testing guide v2
- Each addition to SLAX created as a seperate module – 37 total
  - Downloadable at the Google Code site
  - Download counts vary from 3014 to 2
  - Use on other SLAX installs or extract (.lzm)

In the News...



- Release party in Austin February 2009
- Presentations
  - Austin OWASP meeting, August 2008
  - ISSA Austin Meeting, February 2009
  - DHS Software Assurance Workshop, March 2009
  - TRISC, March 2009
  - AppSec EU 2009, May 2009
- Training using OWASP Live CD
  - OWASP AppSec Australia 2009
  - SecAppDev Belguim
  - OWASP AppSec EU 2009

Where are we going?



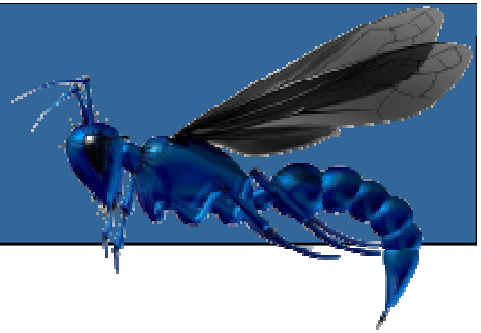
- The cool fun stuff ahead
  - Project Tindy
  - Project Aqua Dog
  - Builder vs Breaker
  - Auto-update installed tools
  - Website update
  - OWASP Education Project
  - Minor release tweaks
  - Crazy Pie in the Sky idea

Project Tindy & Aqua Dog

- Project Tindy
  - OWASP Live CD installed to a virtual hard drive
  - Persistance!
  - 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

(Thanks Top Gear!)

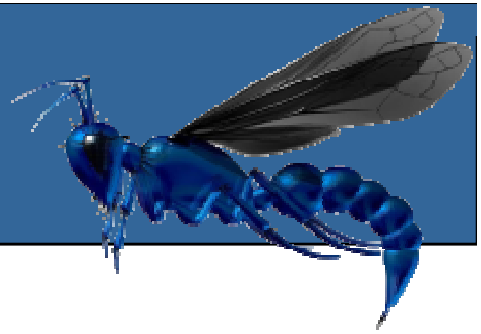
But darn it,
breaking is really fun.

Builder tools coming in future releases.

Auto-update installed tools

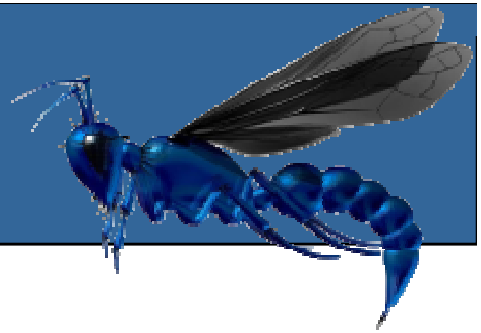
- In theory, SLAX modules can be added to a running system – booted CD or virtual install
  - SLAX packages aren't all that smart
    - No pre-install or post-install scripting capabilities
    - No idea of dependencies
  - Program to check installed modules against those available via Google Code site
  - Lots of bolt-on engineering to get us there
  - Currently lots of human interaction
- Alternatives...

Website Update



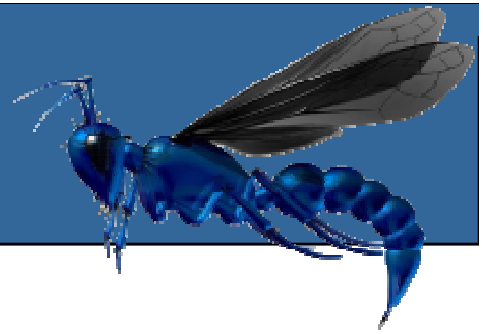
- Quick, spell my last name
  - FAIL!
- Need a much easier URL – AppSecLive.org
  - Community site around OWASP Live CD
    - Forums, articles, screen casts, etc
  - Online Tool database
    - Seeded with the 331 I've already got
  - Articles and HowTo's published by users
  - www.owasp.org will ***always*** be its home
  - Content from AppSecLive -> OWASP site
  - Current site -> OWASP site

OWASP Education Project



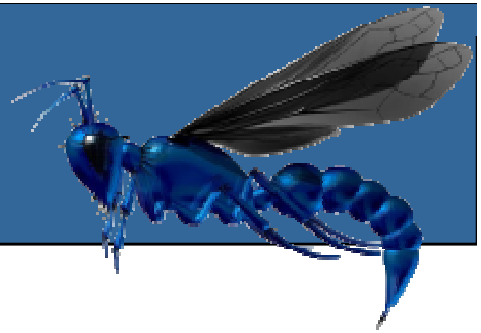
- Natural ties between these projects
  - Already being used for training classes
  - Need to coordinate efforts to make sure critical pieces aren't missing from the OWASP Live CD
  - Training environment could be customized for a particular class thanks to the individual modules
    - Student gets to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

Minor Release Tweaks



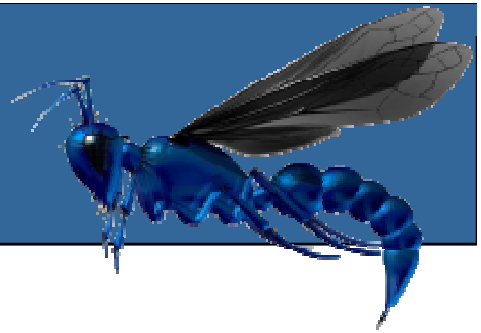
- Sign the release files
  - Establish a project GPG key (Open PGP)
  - At least sign the hash file (MD5/SHA1)
  - Both at the module level and ISO/VM disk files
- New & better repository for development
  - Likely will be git, currently mostly ad-hock
  - Better method to track upstream updates
- Release schedule
  - Probably quarterly or bi-annual releases
- Add TrueCrypt / file encryption to VMs

Crazy Pie in the Sky idea



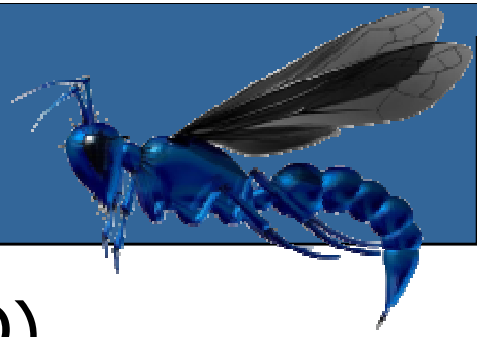
- Modules + auto update + categories = CD profiles
  - Allows someone to customize the OWASP Live CD to their needs
  - Example profiles
    - Whitebox testing
    - Blackbox testing
    - Static Analysis
    - Target specific (Java, .Net, ...)
  - Profile + VM = custom persistent work environment
  - There's room (461.7 MB vs 700 MB CD)

How can you get involved?



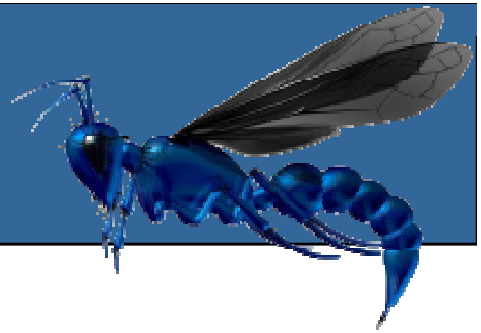
- Join the mail list
  - Announcements are there – low traffic
- Download an ISO or VM
  - Complain or praise
  - Suggest improvements
  - Submit a bug to the Google Code site
- Create a modules
  - How I created modules is documented, command by command and I'll answer questions gladly
- Suggest missing docs or links
- Do a screencast of one of the tools being used on the OWASP Live CD

What else is out there?



- LabRat v2.1 (Previous OWASP Live CD)
  - 404 for ISO link
- Samurai WTF (Web Testing Framework)
  - Slighly fewer tools overall
    - Unique to Samurai: WebShag & MoinMoin Wiki
  - Ubuntu based live CD, looks really nice
  - No .deb packages for most of the tools
  - Currently development release
  - http://samurai.intelguardians.com/
    - Login info is samurai / samurai
- Backtrack – has some web app tools

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 & Documentation Site:
  http://mtesauro.com/livecd/

- Commin soon: http://AppSecLive.org

Questions?