

OWASP 广州 2012



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



# OWASP **live CD**

-- The most simple topics

何伊圣

[akast@ngsst.com](mailto:akast@ngsst.com)

# Who's this **Akast** guy anyway?

## ■ My work

White hat, Web security engineer, Pen Tester, Vulnerability mining, Security services manager

IT民工，无证从业人士

## ■ Linux and Open Source projects

Backtrack、Radiowar、Open Web Application Security Project ( Live CD / WTE )

## ■ External teachers

清远职业技术学院、南华工商学院、现代信息工程职业技术学院

Who's this **Matt** guy anyway? — **OWASP live CD负责人!**

■ **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**

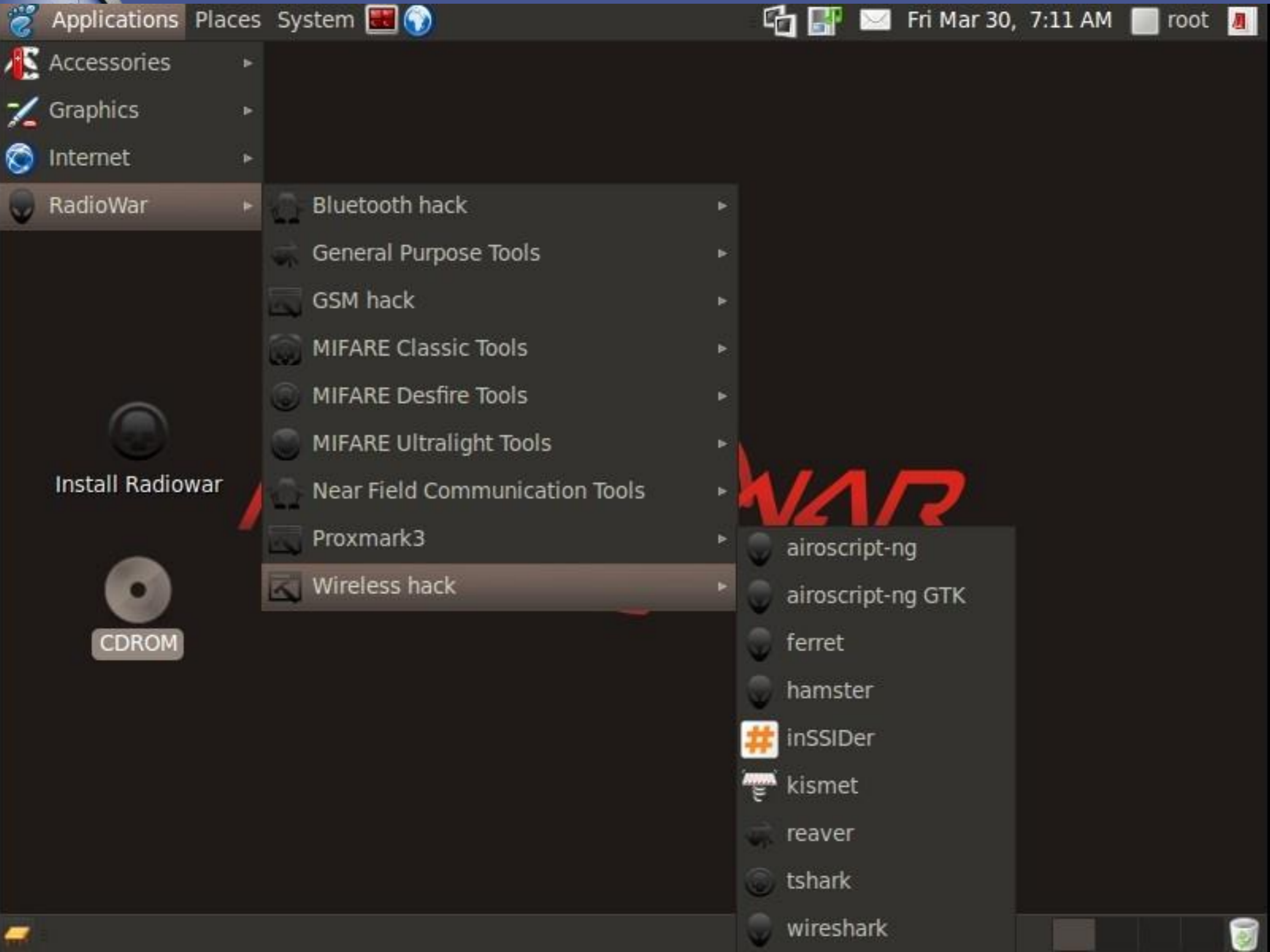
■ **OWASP Foundation Board Member**

■ **VP, Services for Praetorian**



# Live CD & DVD、USB

- 方便！即插即用、即开即用
- Can do it yourself，几十MB~几GB
- OWASP、backtrack、Radiowar...



Applications

Places

System



Fri Mar 30, 7:11 AM



root



Accessories



Graphics



Internet



RadioWar



Bluetooth hack



General Purpose Tools



GSM hack



MIFARE Classic Tools



MIFARE Desfire Tools



MIFARE Ultralight Tools



Near Field Communication Tools



Proxmark3



Wireless hack



airoscrip-ng



airoscrip-ng GTK



ferret



hamster



inSSIDer



kismet



reaver



tshark



wireshark

Install Radiowar



CDROM



Install BackTrack

- BackTrack中文
- Wine 红酒瓶
- 办公
- 多媒体
- 工具
- 互联网
- 设置
- 图像
- 系统
- 未知类别
- 收藏夹
- 运行命令...
- 离开

- 信息搜集工具
- 漏洞扫描工具
- 漏洞利用工具
- 权限提升工具
- 维持访问工具
- 逆向工程工具
- RFID安全工具
- 压力测试工具
- 数字取证工具
- 报告编写工具
- 启动常用服务
- 杂项工具

- 网络安全分析
- WEB应用安全审计
- 数据库安全分析
- 无线安全分析

- DNS安全分析
- SMB信息搜集
- SMTP信息搜集
- SNMP信息搜集
- SSL信息搜集
- VOIP信息搜集
- VPN信息搜集
- 电话信息搜集
- 开放情报搜集
- 路由信息搜集
- 识别IDS和IPS
- 识别操作系统类型
- 识别活动主机
- 识别应用服务
- 网络流量分析
- 网络扫描工具

- samrdump
- smbclient

R1-CN

CURITY TEAM - AKAST@NGS



# OWASP **WTE**: A 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


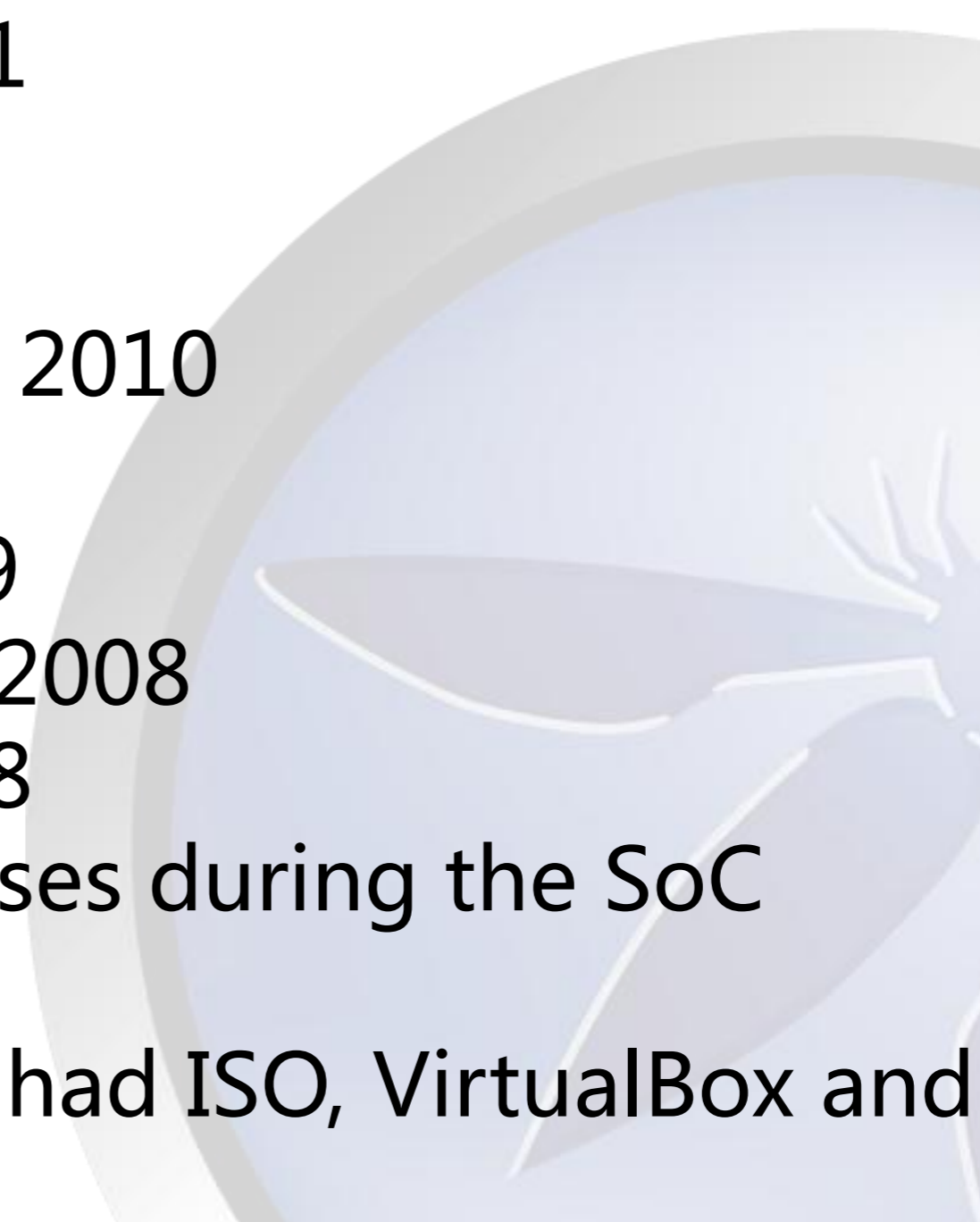
## ■ MAIN LINKS

- [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
<a href="#">OWASP Testing Guide v3</a>	Matteo Meucci
<a href="#">OWASP Ruby on Rails Security Guide v2</a>	Heiko Webers
<a href="#">OWASP Live CD 2008 Project</a>	Matt Tesauro
<a href="#">OWASP Code review guide, V1.1</a>	Eoin Keary
<a href="#">OWASP AntiSamy .NET</a>	Arshan Dabirsiaghi
<a href="#">OWASP .NET Project Leader</a>	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


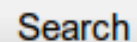
- ▶ ~5,094 GB of bandwidth since launch (Jul 2008)
- ▶ Most downloads in 1 month = 81,607 (Mar 2009)

 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](#)owasp li|ve cd  

owasp live cd

owasp lisbon

owasp library

owasp linux

owasp li

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](http://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](http://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](http://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 ...

[appseclive.org/](http://appseclive.org/) - Cached

File Edit View History Bookmarks Tools Help



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

Google



owasp wte - Google Search



Web Images Videos Maps News Shopping Gmail more

Sign In



Everything

Images

Videos

News

Shopping

More

Austin, TX

Change location

All results

Wonder wheel

More search tools

owasp wte



Search

Instant is on

owasp wte

owasp webgoat

owasp wiki

owasp webscarab

owasp w

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 were 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




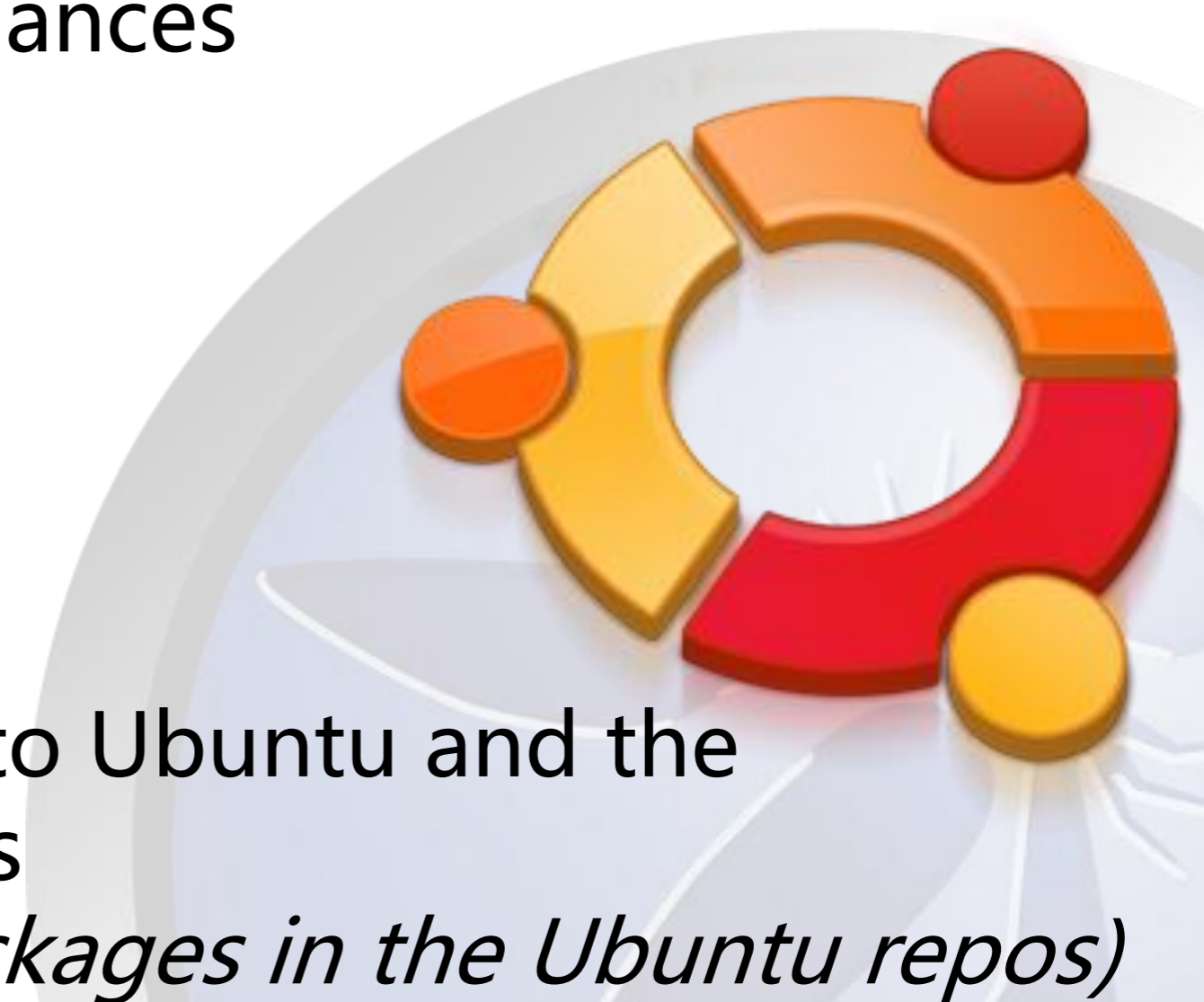


There's a new kid in town

**OWASP WTE**

**Web  
Testing  
Environment**

**Web测试环境**

- 
- 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

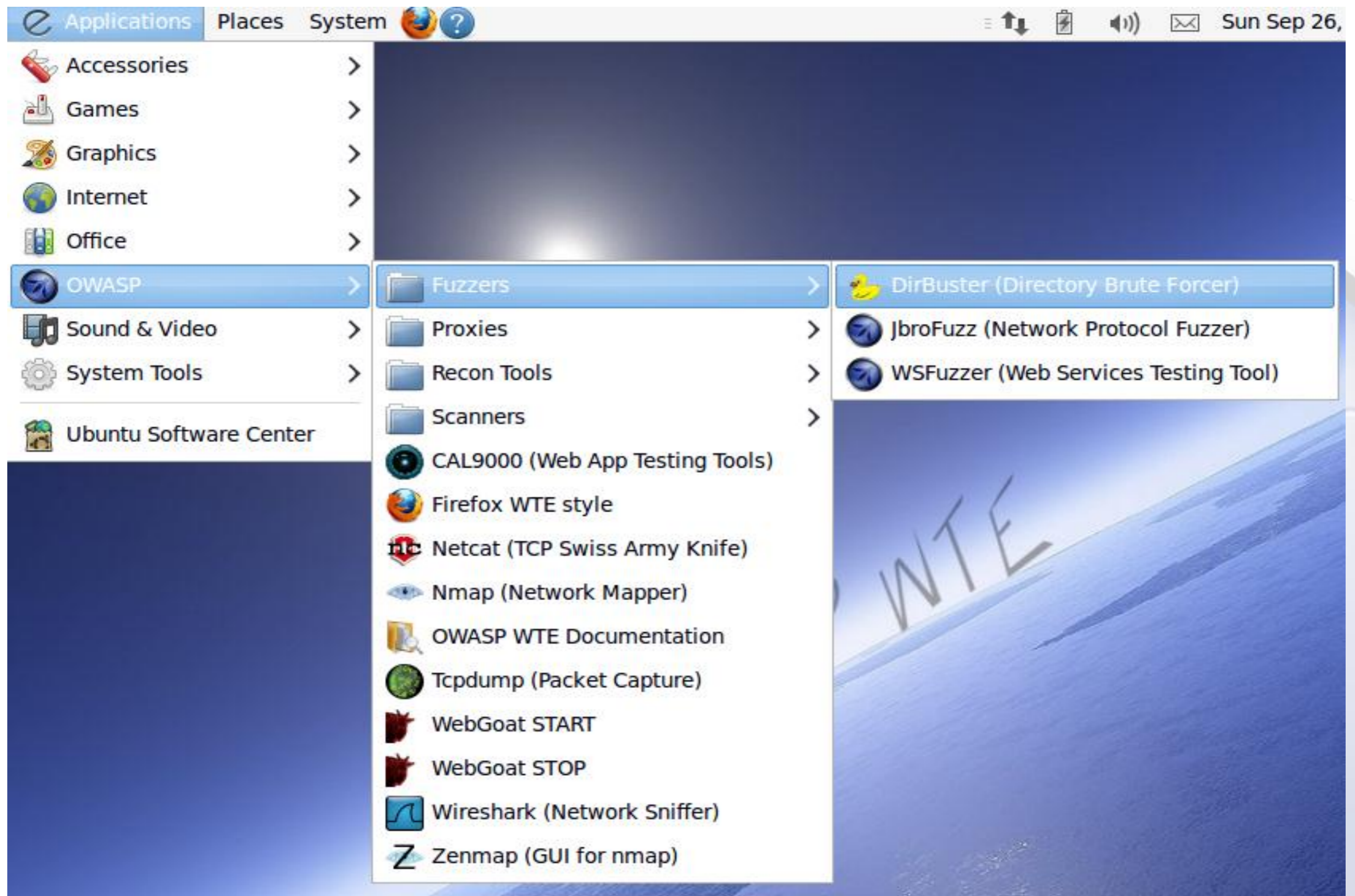
## ■ Design goals

- ▶ Easy for users to **keep updated** (目前国内并不行)
- ▶ 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





## 26 "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

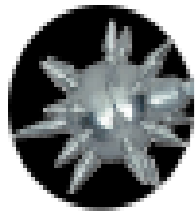
## Other Proxies:



**Burp Suite**



**Paros**



**Spike Proxy**



**Rat Proxy**

## Scanners:



**w3af**



**Grendel  
Scan**



**Nikto**



**nmap**



**Zenmap**



**Fierce Domain  
Scanner**

## SQL-i:



**sqlmap**



**SQL Brute**

**Duh:**



**Firefox**

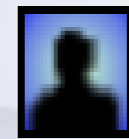
## Others:



**Metasploit**



**Httpprint**



**Maltego CE**



**netcat**



**Wireshark**



**tcpdump**

# Firefox 插件



## Add N Edit Cookies 0.2.1.3

Cookie Editor that allows you add and edit session a



## CookiePie 1.0.2

Use multiple Web accounts and profiles in different t



## DOM Inspector 2.0.3

Inspects the structure and properties of a window ar



## Firebug 1.3.3

Web Development Evolved.



## FormFox 1.6.3

Pops up form action when submit button is about to



## FoxyProxy 2.9

FoxyProxy - Premier proxy management for Firefox



## Greasemonkey 0.8.20090123.1

A User Script Manager for Firefox



## HackBar 1.3.2

A toolbar that helps you find and test SQL injections



## Header Spy 1.3.3.1

Shows HTTP headers on statusbar



## InspectThis 0.9.1

Inspect the current element with the DOM Inspector.



## JSView 2.0.5

View the source code of external stylesheets and jav



## Live HTTP headers 0.14

View HTTP headers of a page and while browsing.



## Modify Headers 0.6.6

Add, modify and filter http request headers



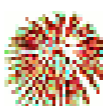
## No-Referer 1.3.1

Lets you open a tab without sending the HTTP referer information.



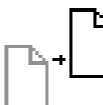
## NoScript 1.9.2.6

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



## UriParams 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.

# Firefox 各种代理

- 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



Apache/2.2.9...



FoxyProxy: Disabled



## ■ OWASP **Documents** 英文版本

- ▶ 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



# deb http://appseclive.org/apt/stable / #OWASP WTE Stable Repository disabled on upgrade to natty  
# deb http://appseclive.org/apt/testing / #OWASP WTE Testing Repository

## Index of /apt/downloads

- [Parent Directory](#)
- [all-wte-files.md5](#)
- [owasp-wte-Feb-2011.iso.rar](#)
- [owasp-wte-Feb-2011.vdi.rar](#)
- [owasp-wte-Feb-2011.vmdk.rar](#)
- [owasp-wte-Sept-2011 vdi.rar](#)
- [owasp-wte-Sept-2011 vmdk.rar](#)
- [sums-owasp-wte-Sept-2011.txt](#)

Apache Server at appseclive.org Port 80

## Index of /apt/testing

- [Parent Directory](#)
- [Packages.gz](#)
- [README](#)
- [owasp-wte-sqlix-1.0-1 all.deb](#)
- [owasp-wte-sqlmap-0.9-1 all.deb](#)
- [owasp-wte-wpscan-198svn-1 all.deb](#)
- [owasp-wte-wpscan-198svn-2 all.deb](#)

Apache Server at appseclive.org Port 80

## Index of /apt/stable

- [Parent Directory](#)
- [Packages.gz](#)
- [README](#)
- [owasp-wte-burpsuite-1.4.01-1 all.deb](#)
- [owasp-wte-cal9000-2.0-1 all.deb](#)
- [owasp-wte-cloud-1.0-1 all.deb](#)
- [owasp-wte-doc-2.0-1 all.deb](#)
- [owasp-wte-ende-1.0rc7-1 all.deb](#)
- [owasp-wte-fierce-1.0.3-1 all.deb](#)
- [owasp-wte-firefox-6.0.2-1 i386.deb](#)
- [owasp-wte-grendel-scan-1.0-2 all.deb](#)
- [owasp-wte-httpprint-301-1 all.deb](#)
- [owasp-wte-jbrofuzz-2.5-1 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-2.1.4-1 all.deb](#)
- [owasp-wte-nmap-5.00-1 all.deb](#)
- [owasp-wte-paros-3.2.13-2 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-4041svn-1 all.deb](#)
- [owasp-wte-wapiti-2.2.1-1 all.deb](#)
- [owasp-wte-webgoat-5.3-RC1-2 all.deb](#)
- [owasp-wte-webscarab-20090122-2 all.deb](#)
- [owasp-wte-webslayer-svn-r4-1 all.deb](#)
- [owasp-wte-wireshark-1.2.7-1 all.deb](#)
- [owasp-wte-wsfuzzer-1.9.5-2 all.deb](#)
- [owasp-wte-zap-1.3.4-1 all.deb](#)

# 源安装


File


Edit


Package


Settings

Help


 Reload

 Mark All Upgrades

 Apply

 Properties

Quick search

 Search

All

owasp-wte

☐

owasp-wte-netcat

0.7.1

Netcat is a featured networking utility

☒

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

# 源安装

The screenshot shows a software management application with a sidebar on the left containing 'Get Software', 'Installed Software', and 'History'. The main area displays search results for 'owasp-wte'. The results list various tools with their descriptions and IDs. Some items have a green checkmark icon next to them, indicating they are installed or available. The search bar at the top right contains the text 'owasp-wte'.

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

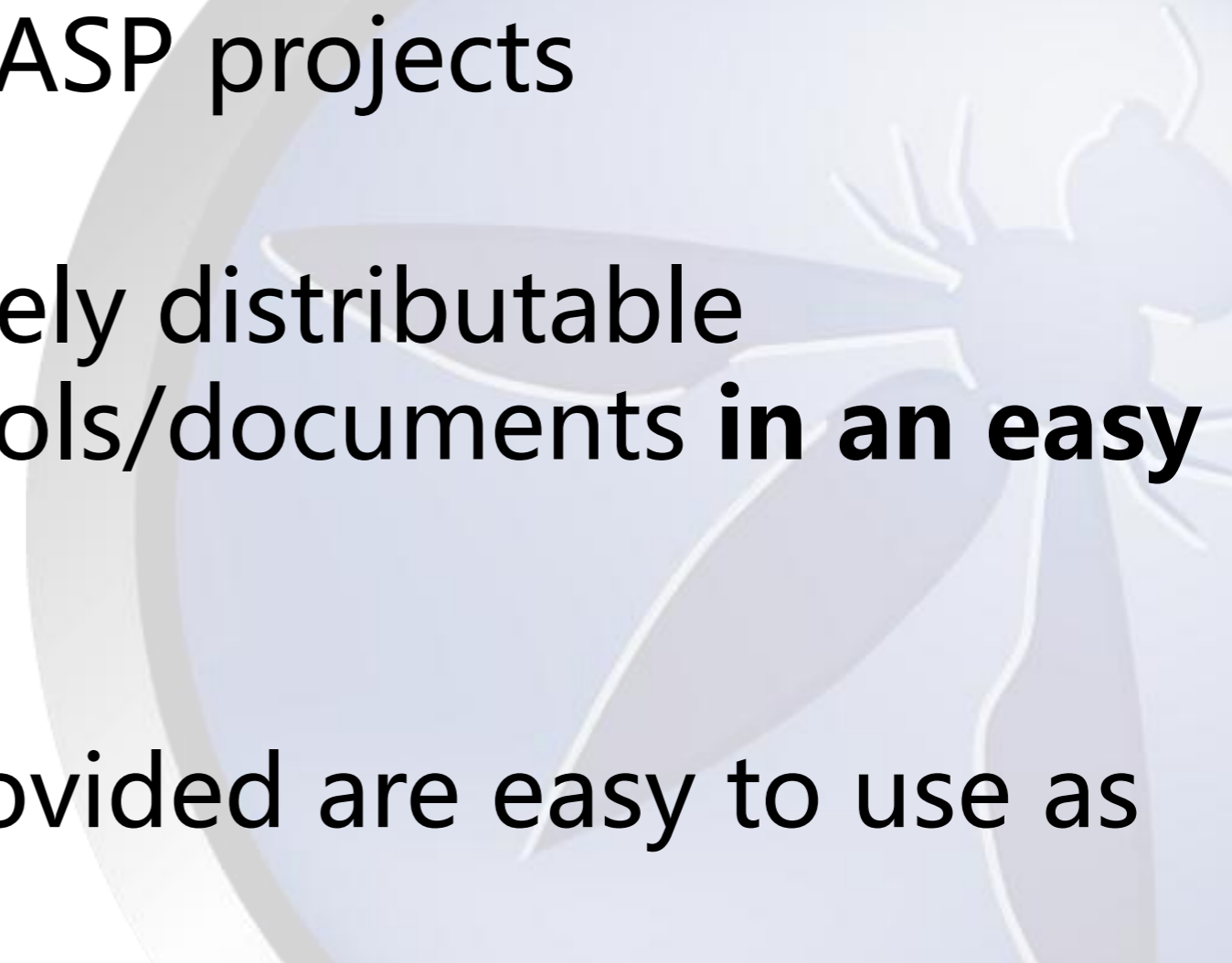


What is next?



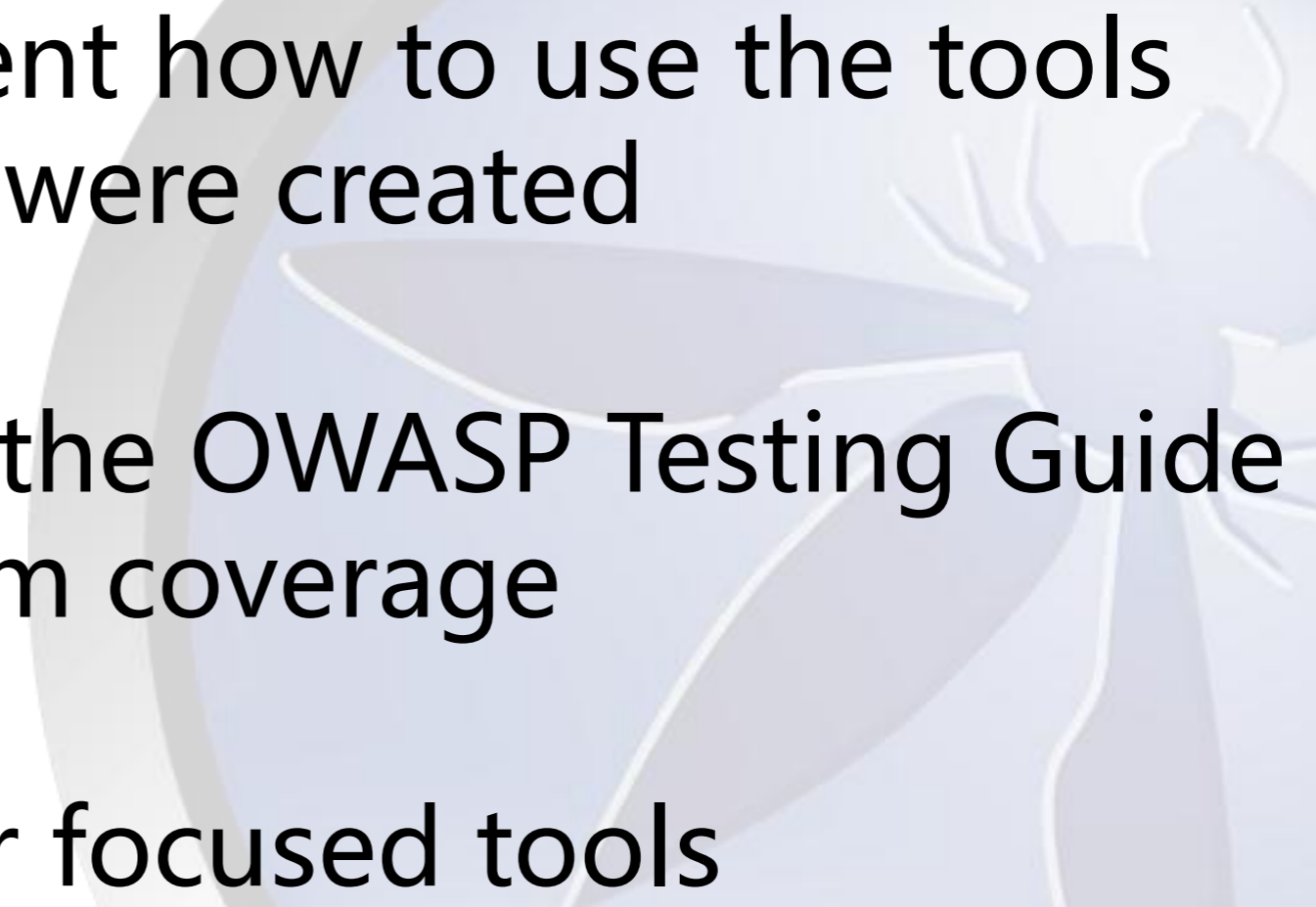


# Goals going forward

- 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
- 

# Goals going forward

- 项目地址：  
[http://www.owasp.org/index.php/Category:OWASP Live CD Project](http://www.owasp.org/index.php/Category:OWASP_Live_CD_Project)
- <http://appseclive.org/> 下载和更新源都被GFW，准备更换到老的项目地址：  
<http://mtesauro.com/>。
- Join the mail list: <https://lists.owasp.org/listinfo/owasp-live-cd-2008-project>

Questions?

公开交流Q群: **74293375**

