# SANS
## Pen Test Hackfest 2013
### SUMMIT & TRAINING
E V E N T

**WASHINGTON, DC** | **SUMMIT: NOV 7-8** | **COURSES: NOV 9-14**

SANS is hosting our ultimate annual penetration testing training event in November. Featuring top-notch talks, in-depth training, and evening activities to help participants build awesome skills, the SANS Pen Test Hackfest Summit and Training Event is specially designed for penetration testers across a broad range of skills and disciplines. Here are the top 5 reasons to attend this event:

**NetWars, NetWars, NetWars!** This event will include FOUR full evenings of NetWars challenges, doubling the amount of NetWars time over a traditional SANS conference. NetWars is an action-packed challenge environment where people can build their skills while having fun.

**Coin-a-palooza** For participants who have taken a given SANS course, but have not won the capture-the-flag challenge coin, this event will offer the ability to catch up on the coins by participating in the four nights of NetWars challenges. If you've taken SEC504 in the past (but didn't win the coin), and make it from NetWars Level 1 into 2, you'll earn the 504 coin! If you make it into Level 3, you'll get your choice of a 542, 560, or 575 coin, provided you've taken the associated course sometime in the past. Make it into Level 4, and you'll get your choice of a 617, 642, or 660 coin if you've had those classes! And, if you win NetWars, you'll get the NetWars coin. With Coin-a-palooza, you'll have an opportunity to win up to 4 challenge coins for your collection.

**CyberCity** The SANS CyberCity project helps train cyber warriors that computer and network activities can have major kinetic impact on the real-world. With its power grid, traffic lights, and water reservoir included in a physical model city, participants access and gain control over these assets, preventing attackers from wreaking havoc. This event will include a full evening session of CyberCity missions, the first time SANS has offered direct access to CyberCity at a training event!

**Summit** Two full-days of in-depth presentations chock full of cutting-edge penetration testing topics focused on helping you provide technical excellence and real business value in your vulnerability assessment and penetration testing work.

**Training** Six days of deep SANS training in real-world penetration techniques you can use immediately when you return to your job. The four courses are:

**SEC560**
Network Penetration Testing and Ethical Hacking

**SEC575**
Mobile Device Security and Ethical Hacking

**SEC642**
Advanced Web App Penetration Testing and Ethical Hacking

**SEC660**
Advanced Penetration Testing, Exploits, and Ethical Hacking

*Learn more at www.sans.org/event/pen-test-hack-fest-2013*

# The Ultimate Pen Test

## P O S T E R

### SUMMER 2013 – 25TH EDITION

**On this poster:**
- Must-have tools for penetration testing, ethical hacking, and vulnerability assessment
- Methodology, tips, and tricks for mobile device, web app, network, and wireless pen testing, as well as exploit development
- Specific recommendations for deriving more value out of your penetration testing projects
- A detailed mindmap of sites and distributions you can use to practice your skills
- Resources for keeping your skills current
- A description of the SANS Pen Test Coins for our Capture the Flag winners
- An overview of the awesome courses in the SANS Pen Test Curriculum

# Pen Testing Coins

Each SANS Pen Test Course includes a final full day (Day 6) of hands-on computer security challenges that hammer home the lessons taught throughout the entire course. The top winners in each course of this full-day Capture-the-Flag event receive the much-coveted challenge coin associated with the course. Each coin is unique for its associated course, with a custom logo, a special tag line, and a theme. Coins are available for the 504, 542, 560, 575, 617, 642, and 660 courses, as well as the SANS NetWars challenge. The prize coin congratulates the victors on their great accomplishment and challenges them further to use their amazing skills to make a positive difference in their workplace and career.

And, best of all, each coin includes a special cipher that encodes or encrypts a part of a hidden message (Note: We have purposefully omitted the ciphers from the coin images on this poster). The coins include all kinds of ancient, modern, and custom-created twisted ciphers ready to challenge and delight CtF winners. Coin holders can analyze their prize and determine its unique part of a larger message. People who win all of the challenge coins can decipher the ultimate phrase-that-pays embedded in the coins!

## SANS PEN TESTING CURRICULUM
### Course Overview

**SEC504**
Hacker Techniques, Exploits, and Incident Handling
*GCIH*

**SEC560**
Network Pen Testing and Ethical Hacking
*GPEN*

**SEC542**
Web App Pen Testing and Ethical Hacking
*GWAPT*

**SEC573**
Python for Penetration Testers

**SEC575**
Mobile Device Security and Ethical Hacking

**SEC660**
Advanced Pen Testing, Exploits, and Ethical Hacking
*GXPN*

**SEC642**
Advanced Web App Pen Testing and Ethical Hacking

**SEC617**
Wireless Ethical Hacking, Pen Testing, and Defenses
*GAWN*

**SPECIALIZATIONS**

**SEC580**
Metasploit Kung Fu for Enterprise Pen Testing

**SEC760**
Advanced Exploit Development

**NETWARS**

## PEN TESTING RESOURCES
### http://pen-testing.sans.org/resources

The SANS Penetration Testing Resources website provides a variety of resources. Interact with your fellow professionals and appsec experts on the SANS Pen-Testing Blog or discover solutions to penetration testing issues with a multitude of webcasts. At **http://pen-testing.sans.org/resources** you will find:

- Blog Posts • Links • Tweets • Whitepapers
- Downloads **http://pen-testing.sans.org/resources/downloads**
  The SANS Penetration Testing Community provides a variety of free resources. You can view our many free downloads here.
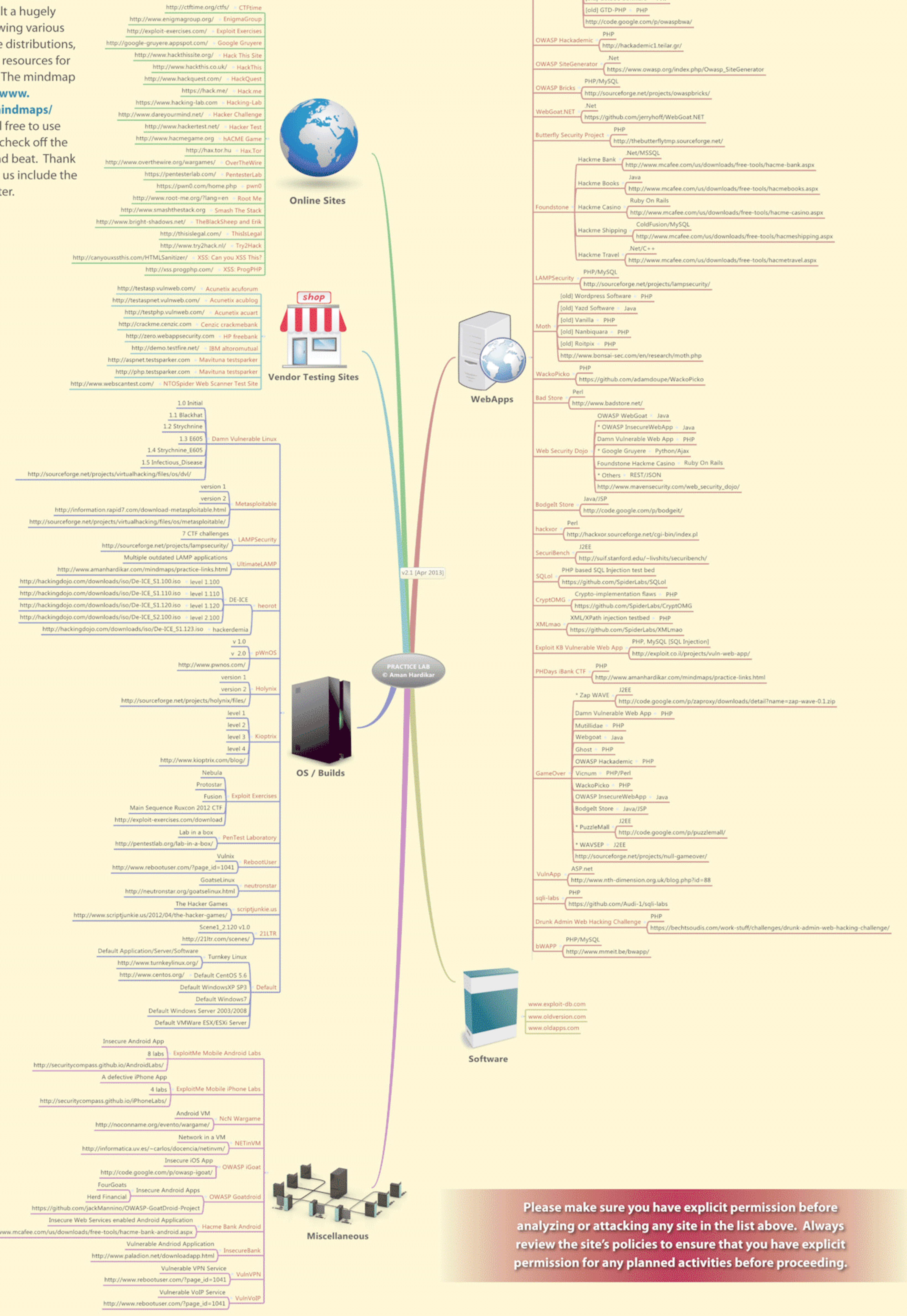- Webcasts
  SANS Webcasts allow you to hear a knowledgeable speaker while viewing presentation slides that you download in advance.

# Penetration Testing Practice Labs
## Vulnerable Apps/Systems

Created by Aman Hardikar .M
**http://www.amanhardikar.com/mindmaps/Practice.html**

Building your skills through hands-on lab experimentation is vital in the life of a penetration tester. Aman Hardikar .M built a hugely useful mind map showing various free, publicly available distributions, challenges, and other resources for practicing your skills. The mindmap is available on-line at **www.amanhardikar.com/mindmaps/Practice.html**, but feel free to use this poster version to check off the ones you've visited and beat. Thank you, Aman, for letting us include the mind-map in this poster.

### Online Sites

http://ctf time.org/ctf/ – CTF time
http://www.enigmagroup.org/ – EnigmaGroup
http://exploit-exercises.com/ – Exploit Exercises
http://google-gruyere.appspot.com/ – Google Gruyere
http://www.hackthissite.org/ – Hack This Site
http://www.hackthis.co.uk/ – HackThis
http://www.hackquest.com/ – HackQuest
http://hack.me/ – Hack.me
https://www.hacking-lab.com – Hacking-Lab
http://www.darexyourmind.net/ – Hacker Challenge
http://www.hackerstest.com/ – Has.Tor
http://www.hacmegame.org – hACME Game
http://pentesterlab.com/ – PentesterLab
http://pwn0.com/home.php – pwn0
http://www.root-me.org/?lang=en – Root Me
http://www.smashthestack.org – Smash The Stack
http://www.bright-shadows.net/ – TheBlackSheep and Erik
http://thisislegal.com/ – ThisISLegal
http://www.try2hack.nl/ – Try2Hack
http://canyouxssthis.com/HTMLSanitizer/ – XSS: Can you XSS This?
http://xss.progphp.com/ – XSS: ProgPHP

**Vendor Testing Sites**
http://testasp.vulnweb.com/ – Acunetix asp
http://testaspnet.vulnweb.com/ – Acunetix aspx
http://testphp.vulnweb.com/ – Acunetix acupart
http://crackme.cenzic.com – Cenzic crackmebank
http://zero.webappsecurity.com – IBM appscantestsite
http://demo.testfire.net/ – IBM altoromutual
http://aspnet.testsparker.com – Mavituna testsparker
http://php.testsparker.com – Mavituna testsparker
http://www.webscantest.com/ – NTOSpider Web Scanner Test Site

**OS / Builds**

1.0 Initial
1.1 Blackhat
1.2 Strychnine
1.3 E605 – Damn Vulnerable Linux
1.4 Strychnine_E605
1.5 Infectious_Disease
http://sourceforge.net/projects/virtualhacking/files/os/dvl/

version 1
http://information.rapid7.com/download-metasploitable.html – Metasploitable
version 2
http://sourceforge.net/projects/virtualhacking/files/os/metasploitable/
7 CTF challenges – LAMPSecurity
http://sourceforge.net/projects/lampsecurity/
Multiple outdated LAMP applications – UltimateLAMP
http://www.amanhardikar.com/mindmaps/practice-links.html
http://hackingdojo.com/downloads/iso/De-ICE_S1.100.iso – level 1.100
http://hackingdojo.com/downloads/iso/De-ICE_S1.110.iso – level 1.110
http://hackingdojo.com/downloads/iso/De-ICE_S1.120.iso – level 1.120
http://hackingdojo.com/downloads/iso/De-ICE_S2.100.iso – level 2.100
http://hackingdojo.com/downloads/iso/De-ICE_S1.123.iso – hackerdemia

v 1.0 – pWnOS
v 2.0
http://www.pwnos.com/
version 1 – Holynix
version 2
http://sourceforge.net/projects/holynix/files/
level 1 – Kioptrix
level 2
level 3
level 4
http://www.kioptrix.com/blog/
Nebula
Protostar
Fusion – Exploit Exercises
Main Sequence Ruxcon 2012 CTF
http://exploit-exercises.com/download
Lab in a box – PenTest Laboratory
http://pentestlab.org/lab-in-a-box/
Vulnix – RebootUser
http://www.rebootuser.com/?page_id=1041
GoatseLinux
http://neutronstar.org/goatselinux.html – neutronstar
The Hacker Games – scriptjunkie.us
http://www.scriptjunkie.us/2012/04/the-hacker-games/
Scene1_2.120 v1.0
http://21ltr.com/scenes/ – 21LTR
Default Application/Server/Software
http://www.turnkeylinux.org/ – Turnkey Linux
http://www.centos.org/ – Default CentOS 5.6
Default WindowsXP SP3 – Default
Default Windows7
Default Windows Server 2003/2008
Default VMware ESX/ESXi Server

**Miscellaneous**
Insecure Android App
8 labs – ExploitMe Mobile Android Labs
http://securitycompass.github.io/AndroidLabs/
A defective iPhone App
4 labs – ExploitMe Mobile iPhone Labs
http://securitycompass.github.io/iPhoneLabs/
Android VM – NcN Wargame
http://noconname.org/evento/wargame/
Network in a VM – NETinVM
http://informatica.uv.es/~carlos/docencia/netinvm/
Insecure iOS App
http://code.google.com/p/owasp-igoat/ – OWASP iGoat
FourGoats
Herd Financial – OWASP GoatDroid
https://github.com/jackMannino/OWASP-GoatDroid-Project
Insecure Web Services enabled Android App
http://www.mcafee.com/us/downloads/free-tools/hacme-bank-android.aspx – Hacme Bank Android
Vulnerable Android Application
http://www.paladion.net/downloadapp.html – InsecureBank
Vulnerable VPN Service
http://www.rebootuser.com/?page_id=1041 – VulnVPN
Vulnerable VoIP Service
http://www.rebootuser.com/?page_id=1041 – VulnVoIP

### WebApps

Webgoat – Java
Mutillidae – PHP
Ghost – PHP
Vicnum – PHP/Perl
Peruggia – PHP
OWASP CSRFGuard Sample App – Java
Mandiant Struts Forms – Java/Struts
Simple Form in .Net – ASP.Net/C#
Simple Form in .Net – HTML/JS
OWASP AppSensor – Java
[old] Wordpress Software – PHP
[old] Yazd Software – Java
[old] Orange HRM Software – PHP
[old] GetBoo Software – PHP
[old] GTD-PHP – PHP
http://code.google.com/p/owaspbwa/ – BWA (OWASP)

PHP
http://hackademic1.teilar.gr/ – OWASP Hackademic
.Net
http://www.owasp.org/index.php/Owasp_SiteGenerator – OWASP SiteGenerator
PHP/MySQL – OWASP Bricks
http://sourceforge.net/projects/owaspbricks/
.Net
https://github.com/jerryhoff/WebGoat.NET – WebGoat.NET
PHP – Butterfly Security Project
http://thebutterflytmp.sourceforge.net/
http://www.mcafee.com/us/downloads/free-tools/hacme-bank.aspx – Hackme Bank
http://www.mcafee.com/us/downloads/free-tools/hacmebooks.aspx – Hackme Books
Ruby On Rails – Foundstone
http://www.mcafee.com/us/downloads/free-tools/hacme-casino.aspx – Hackme Casino
ColdFusion/MySQL
http://www.mcafee.com/us/downloads/free-tools/hacmeshipping.aspx – Hackme Shipping
.Net/C++
http://www.mcafee.com/us/downloads/free-tools/hacmetravel.aspx – Hackme Travel

PHP/MySQL – LAMPSecurity
http://sourceforge.net/projects/lampsecurity/
[old] Wordpress Software – PHP – Moth
[old] Vanilla – PHP
[old] Nanbiquara – PHP
http://www.bonsai-sec.com/en/research/moth.php
https://github.com/adamdoupe/WackoPicko – WackoPicko
Perl – Bad Store
www.badstore.net/
OWASP WebGoat – Java
* OWASP InsecureWebApp – Java
Damn Vulnerable Web App – PHP
* Google Gruyere – Python/Apps
Foundstone Hackme Casino – Ruby On Rails – Web Security Dojo
* Others – REST/JSON
http://www.mavensecurity.com/web_security_dojo/

Java/JSP – BodgeIt Store
http://code.google.com/p/bodgeit/
Perl – hackxor
http://hackxor.sourceforge.net/cgi-bin/index.pl
J2EE – SecuriBench
http://suif.stanford.edu/~livshits/securibench/
PHP based SQL Injection test bed – SQLol
https://github.com/SpiderLabs/SQLol
Crypto-implementation fixes – PHP – CryptOMG
https://github.com/SpiderLabs/CryptOMG
XML/XPath injection testbed – PHP – XMLmao
https://github.com/SpiderLabs/XMLmao
PHP, MySQL [SQL Injection] – Exploit KB Vulnerable Web App
http://exploit.co.il/projects/vuln-web-app/
PHP – PHDays iBank CTF
http://www.amanhardikar.com/mindmaps/practice-links.html

J2EE
* Zap WAVE – Java
https://code.google.com/p/zaproxy/downloads/detail?name=zap-wave-0.1.zip
Damn Vulnerable Web App – PHP – Mutillidae
Mutillidae – PHP
Webgoat – Java
Ghost – PHP
DVWA Hackademic – PHP – GameOver
Vicnum – PHP – WackoPicko
WackoPicko – PHP
OWASP InsecureWebApp – Java
BodgeIt Store – Java/JSP
J2EE – * PuzzleMall
http://code.google.com/p/puzzlemall/
* WAVSEP – J2EE
http://sourceforge.net/projects/null-gameover/
ASP.net – VulnApp
http://www.nth-dimension.org.uk/blog.php?id=88
PHP – sqli-labs
https://github.com/Audi-1/sqli-labs
PHP – Drunk Admin Web Hacking Challenge
http://bechsoudis.com/work-stuff/challenges/drunk-admin-web-hacking-challenge/
PHP/MySQL – bWAPP
http://www.mmml.be/bwapp/

**Software**
www.exploit-db.com
www.oldversion.com
www.oldapps.com

---

Please make sure you have explicit permission before analyzing or attacking any site in the list above. Always review the site's policies to ensure that you have explicit permission for any planned activities before proceeding.

# SANS