AUTOMATED SECURITY SCANNING GUIDE
# Table of Contents

**GETTING STARTED** ................................................................. 3  
**INTRODUCTION** ................................................................. 3  
**REGISTRATION** ................................................................. 3  
  - FREE USER PROCESS .................................................. 3  
  - MEMBERSHIP OPTION .................................................. 3  
**OVERVIEW OF SCAN OPTIONS** ........................................ 4  
**RECON TO VULNERABILITY DISCOVERY** ............................ 4  
  - Intelligence Collection .............................................. 4  
  - Server / IP Address Analysis ....................................... 4  
  - Web Site Fingerprinting and Testing ........................... 4  
  - Content Management Systems (CMS) ......................... 4  
**AUTOMATED SCANS DETAILED** .......................................... 5  
**DOMAIN PROFILER** .......................................................... 5  
**HOSTING SERVER INFO** ..................................................... 6  
**NMAP PORT SCAN** ............................................................ 7  
**OPENVAS VULNERABILITY SCAN** ....................................... 8  
**SSL SECURITY CHECK** ..................................................... 9  
**NIKTO WEB SERVER SCAN** ............................................... 10  
**SQL INJECTION TEST** ..................................................... 11  
**WHATWEB WEBSITE FINGERPRINT** ................................ 12  
**BLINDELEPHANT VERSION TEST** ...................................... 13  
**WORDPRESS SECURITY SCAN** ......................................... 14  
**JOOMLA SECURITY SCAN** ............................................... 15  
**DRUPAL SECURITY SCAN** ............................................... 16  
**MANUAL SECURITY ASSESSMENT** .................................... 17
GETTING STARTED

INTRODUCTION

There are 12 automated scanning tools available from HackerTarget.com; each of these tools perform a variety of security tests and information gathering functions. This guide will outline the process and detail the purpose of the tools.

On-line Security Scans are an easy and convenient way to test public facing Internet hosts.

REGISTRATION

All scans are available for Free and there is also a membership based option that includes the ability to perform a higher number of scans each day along with some other advanced capabilities.

FREE USER PROCESS

1. First time scan users are sent an email confirmation link
2. Once confirmed all scans are available for Free
3. Up to 4 scans can be performed each day

MEMBERSHIP OPTION

1. Select membership option
2. Make payment with Paypal or Credit Card
3. Email is registered and all scans are available up to daily limit

Membership Options
OVERVIEW OF SCAN OPTIONS

RECON TO VULNERABILITY DISCOVERY

Intelligence Collection
Collect information about organizations from open source resources, the domain name system and Internet search engines. These scans send only a limited amount of data to the target and can be hard to detect.

- Domain Profiler Scan
- Hosting Server Info

Server / IP Address Analysis
Discover network details, firewall issues and security vulnerabilities with these types of scans.

- Nmap Port Scan
- OpenVas Security Vulnerability Scan
- SSL Security Check

Web Site Fingerprinting and Testing
Attackers commonly target the web site as it is often the most public and vulnerable part of an organizations infrastructure.

- Nikto Web Server Scan
- SQL Injection Scan
- WhatWeb Site Analysis
- BlindElephant application version testing

Content Management Systems (CMS)
The three most popular CMS systems are the open source WordPress, Joomla and Drupal. These external tests, give a quick overview of the security status of the installation.

- WordPress Security Scan
- Joomla Security Scan
- Drupal Security Scan
AUTOMATED SCANS DETAILED

DOMAIN PROFILER

With only a domain name (myexampledomain.com) this scan type will attempt to discover other related systems and IP addresses, that you can target with other security testing tools.

A PDF report is created and delivered to the user. The report contains details of sub-domains, IP addresses, virtual web hosts on IP addresses, data from the Shodan security search engine and IP address reputation / black list checks.
HOSTING SERVER INFO

This report checks an IP address for virtual web hosts that are sharing the IP address. It then performs a reputation lookup on the websites sharing that IP. Great for finding out the quality of your web host by discovering shared sites hosting Malware and Spam.

A PDF report is created and delivered to the user. The report contains details of the IP address, including hosting, netblock owner and geolocation. Additionally any web sites found to be sharing the IP are also listed with reputation analysis.

This scan is non-intrusive, no packets are sent to the target host.
NMAP PORT SCAN

Nmap is the most popular and well known port scanning tool. It provides a technical report that details open ports, closed ports and filtered ports. Taking the time to look through results can reveal firewall problems, identify internet services and determine operating system of the host.

This is a test run against the nmap test server (scanme.nmap.org)

** Thank you for using the HackerTarget.com Nmap Scanning Service **

HackerTarget.com Membership Status: Non-member

Starting Nmap 5.51 (http://nmap.org) at 2011-08-07 19:22 EDT
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.076s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 996 closed ports
PORT   STATE SERVICE  VERSION
22/tcp      open    ssh        OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
80/tcp      open    http        Apache httpd 2.2.14 ((Ubuntu))
9929/tcp  open    nping-echo Nping echo
31337/tcp open   tcpwrapped
Service Info: OS: Linux

Service detection performed. Please report any incorrect results at http://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 7.99 seconds
The Open Vulnerability Assessment System (OpenVAS) is an application consisting of several services and tools that offers a comprehensive vulnerability scanning solution.

By providing this tool online HackerTarget.com makes this tool available to those who may not have the knowledge, skills or time required to configure the system.

There are two scan options, a default html report that is the raw output from the OpenVas system and an advanced PDF report that has some additional information and tests; along with the relevant vulnerabilities found in the OpenVas scan.

A report is created and delivered to the users designated email address. This scan can take some time to perform as it has a database of over 20000 security checks.
SSL SECURITY CHECK

Using advanced nmap ssl testing scripts and openssl, this scan reveals important information regarding the SSL configuration on a web server. Weak ciphers, SSL versions and certificate information are all revealed.

**Thank you for using the HackerTarget.com SSL Check Service**

HackerTarget.com Membership Status: Valid

Starting Nmap 5.51 (http://nmap.org) at 2011-08-06 01:21 EDT
Nmap scan report for www.sslabs.com (173.203.79.216)
Host up (0.02s latency).
PORT SERVICE STATE SERVICE
443/tcp open https
| ssl-cert: Subject: commonName=www.sslabs.com/organizationName=Parsona Not Validated/countryName=US
| issuer: commonName=StartCom Class 1 Primary Intermediate Server
| C/organizationName=StartCom Ltd./countryName=LI
| PublicKey type: rsa
| PublicKey bits: 2048
| Not valid before: 2011-04-20 05:19:18
| Not valid after: 2012-04-20 05:19:54
| MD5: 001e 0fde 06d0 f2b2 11d8 182a 4c03 7f04
| SHA-1: 2ba7 f19f 53be 4a03 0b2a 1d78 8443 59f1 362d 658
| ssl-enum-ciphers:
| SSLv3
| Ciphers (8)
| TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA
| TLS_RSA_WITH_3DES_EDE_CBC_SHA
| TLS_RSA_WITH_AES_128_CBC_SHA
| TLS_RSA_WITH_AES_256_CBC_SHA
| TLS_RSA_WITH_RC4_128_SHA
| Compression (1)
| uncompressed
| TLSv1.0
| Ciphers (8)
| TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA
| TLS_RSA_WITH_3DES_EDE_CBC_SHA
| TLS_RSA_WITH_AES_128_CBC_SHA
| TLS_RSA_WITH_AES_256_CBC_SHA
| TLS_RSA_WITH_RC4_128_SHA
| Compression (1)
| uncompressed

Nmap done: 1 IP address (1 host up) scanned in 22.35 seconds
NIKTO WEB SERVER SCAN

Nikto is a Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received.

++ Thank you for using the HackerTarget.com Nikto based Web Security Scan ++

HackerTarget.com Membership Status: Valid

Your scan results are listed below. Please note that while Nikto is an excellent tool it can be prone to false positives. Please check your results against your current web software to confirm vulnerabilities.

- Nikto v2.1.4
+ Target IP: 15.216.12.12
+ Target Hostname: zero.webappsecurity.com
+ Target Port: 80
+ Start Time: 2011-06-02 00:58:19

+ Server: Microsoft-IIS/6.0
+ Retrieved x-powered-by header: ASP.NET
+ Retrieved x-asnpro-version header: 2.0.50727
+ Microsoft-IIS/6.0 appears to be outdated (4.0 for NT 4, 5.0 for Win2k, current is at least 7.5)
+ Retrieved ms-author-via header: MS-FTP/4.0
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /CVS/Entries: CVS Entries file may contain directory listing information.
+ OSVDB-473: /vi.pvt/infixinfo.crit: IIS file shows http links on and off site. Might show host trust relationships and other machines on network.
+ OSVDB-3233: /postinfo.html: Microsoft FrontPage default file found.
+ OSVDB-3092: /sqlnet.log: Oracle log file found.
+ OSVDB-3092: /dan_o.dat: This might be interesting...
+ OSVDB-3092: /README.TXT: This might be interesting...
+ OSVDB-3092: /readme.txt: This might be interesting...
+ OSVDB-3092: /scripts/weblog: This might be interesting...
+ OSVDB-3092: /stats: This might be interesting...
+ OSVDB-3092: /stats: This might be interesting...
+ OSVDB-3092: /index.html: This might be interesting...
+ OSVDB-3092: /localstart.asp: This may be interesting...
+ OSVDB-3233: /faxvbs.inc: Microsoft default file found.
+ /login.asp: Admin login page/section found.
+ 5478 items checked: 0 error(s) and 21 item(s) reported on remote host
+ End Time: 2011-06-02 01:08:48 (629 seconds)

+ 1 host(s) tested

Nikto is an old school security testing tool that still finds lots of interesting things.
SQL INJECTION TEST

SQL Injection is a devastating web application attack that can reveal entire databases of information to an attacker, or even act as a stepping stone to full server compromise.

Enter a URL with HTTP GET parameters such as this:

See the handy introductory guide to sql injection on the HackerTarget.com web page.

If the results from this test identify any SQL Injection vulnerabilities you will need to upgrade your web site application or contact your developer.
### WHATWEB WEBSITE FINGERPRINT

WhatWeb discovers the details about web technologies and scripts in use by a web site. It gathers this information from analyzing the raw html from regular web requests.

**HTTPServer**

- **Description:** HTTP server header string
- **String:** nginx (from server string)

**IP**

- **Description:** IP address of the target, if available.
- **String:** 80.72.135.101

**JQuery**

- **Description:** Javascript library

**Mobile-Website**

- **Description:** This plugin detects websites designed for mobile devices.
- **String:** Apple Handheld

**PHP**

- **Description:** PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. - homepage: [http://www.php.net/](http://www.php.net/)
- **Version:** 5.3.3-7+squeeze1

**Title**

- **Description:** The HTML page title
- **String:** Smashing Magazine (from page title)

**UncommonHeaders**

- **Description:** Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at [www.http-stats.com](http://www.http-stats.com)
- **String:** x-pingback (from headers)
BLINDELEPHANT VERSION TEST

Using a variety of techniques that test for known files in web application this tool attempts to accurately determine the version of the application.

This is important when looking at security as old web applications are a common attack vector and entry point.

To ensure security patches and updates are applied always keep your web applications up to date.
WORDPRESS SECURITY SCAN

Wordpress is the leading open source CMS system. It runs on over 10% of the top 1 Million sites. This makes it a popular target. Following some basic systems management best practice will ensure your site does not get hacked. Run a non-intrusive security scan to check for obvious problems.

A PDF report is created and delivered to the user. The report contains details of common WordPress vulnerabilities and application weaknesses. See the sample report for full details.
JOOMLA SECURITY SCAN

Keeping Joomla installations secure is an ongoing process that involves good systems management and keeping all plugins, extensions and core components up to date.

A PDF report is created and delivered to the user. The report contains details of sub-domains, IP addresses, virtual web hosts on IP addresses, data from the Shodan security search engine and IP address reputation / black list checks.

Joomla is a popular open source CMS. Test Security of your installation now with this non-intrusive scan.
DRUPAL SECURITY SCAN

Drupal installations are wide ranging and highly customized; this external security overview will provide an idea of the security posture of the installation and other information of note.

A PDF report is created and delivered to the user. The report contains details of sub-domains, IP addresses, virtual web hosts on IP addresses, data from the Shodan security search engine and IP address reputation / black list checks.

Drupal runs sites ranging from personal blogs to corporate, political, and government sites including whitehouse.gov and data.gov.uk.
MANUAL SECURITY ASSESSMENT

Automated testing is an easy and convenient way to quickly gage the security of your Internet facing systems and infrastructure. It is not a comprehensive audit and is often prone to false positives and / or false negatives.

Manual Security Assessments involve a hybrid of automated and manual testing techniques that provides a greater level of assurance that your systems are secure.

HackerTarget.com has a comprehensive security assessment offering that is in effect a simulated hacker attack against the target system or organization. This assessment by its nature is much more aggressive than the automated tests and provides a full report detailing any security holes found along with recommendations for increasing the security of the system.