AUTOMATED SECURITY SCANNING GUIDE

HackerTarget.com LLC
Everyone is a Target

peter <at> hackertarget.com
http://hackertarget.com

Table of Contents

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.

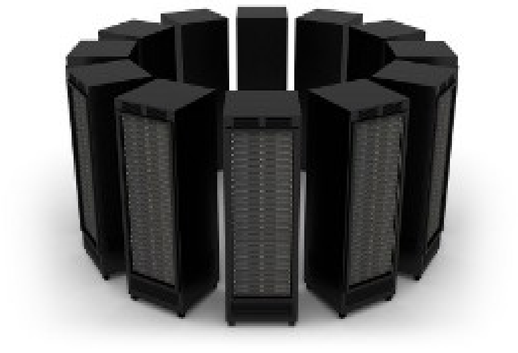
FREE USER PROCESS

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

See the detailed scan page for more information on each scan type

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.

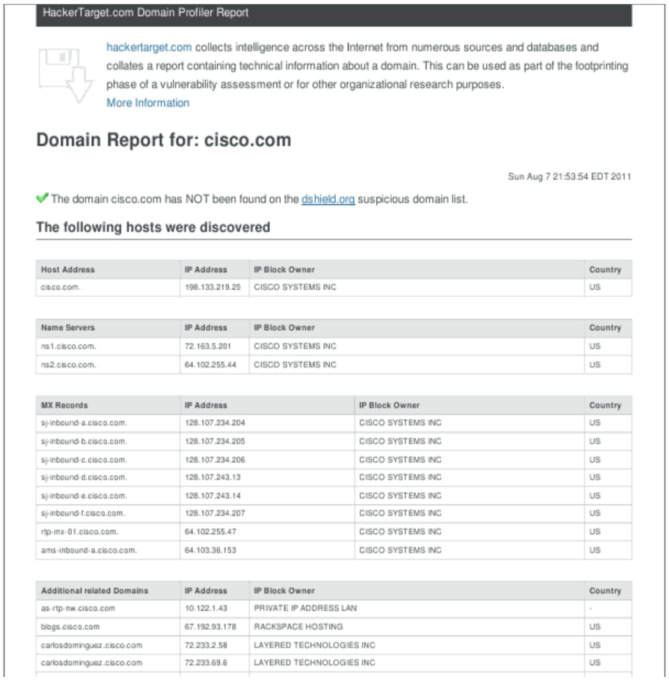
WordPress Security Scan
Joomla Security Scan
Drupal Security Scan

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.

Domain Profiler scans are used to discover targets for other scan types



HackerTarget.com Domain Profiler Report

hackertarget.com collects intelligence across the Internet from numerous sources and databases and collates a report containing technical information about a domain. This can be used as part of the footprinting phase of a vulnerability assessment or for other organizational research purposes.
More Information

Domain Report for: cisco.com

Sun Aug 7 21:53:54 EDT 2011

✓ The domain cisco.com has NOT been found on the dshield.org suspicious domain list.

The following hosts were discovered

Host Address	IP Address	IP Block Owner	Country
cisco.com.	198.133.219.25	CISCO SYSTEMS INC	US

Name Servers	IP Address	IP Block Owner	Country
ns1.cisco.com.	72.163.5.201	CISCO SYSTEMS INC	US
ns2.cisco.com.	64.102.255.44	CISCO SYSTEMS INC	US

MX Records	IP Address	IP Block Owner	Country
sj-inbound-a.cisco.com.	128.107.234.204	CISCO SYSTEMS INC	US
sj-inbound-b.cisco.com.	128.107.234.205	CISCO SYSTEMS INC	US
sj-inbound-c.cisco.com.	128.107.234.206	CISCO SYSTEMS INC	US
sj-inbound-d.cisco.com.	128.107.243.13	CISCO SYSTEMS INC	US
sj-inbound-e.cisco.com.	128.107.243.14	CISCO SYSTEMS INC	US
sj-inbound-f.cisco.com.	128.107.234.207	CISCO SYSTEMS INC	US
rtp-mx-01.cisco.com.	64.102.255.47	CISCO SYSTEMS INC	US
ams-inbound-a.cisco.com.	64.103.36.153	CISCO SYSTEMS INC	US

Additional related Domains	IP Address	IP Block Owner	Country
as-rtp-nw.cisco.com	10.122.1.43	PRIVATE IP ADDRESS LAN	-
blogs.cisco.com	67.192.93.178	RACKSPACE HOSTING	US
carlosdominguez.cisco.com	72.233.2.58	LAYERED TECHNOLOGIES INC	US
carlosdominguez.cisco.com	72.233.69.6	LAYERED TECHNOLOGIES INC	US

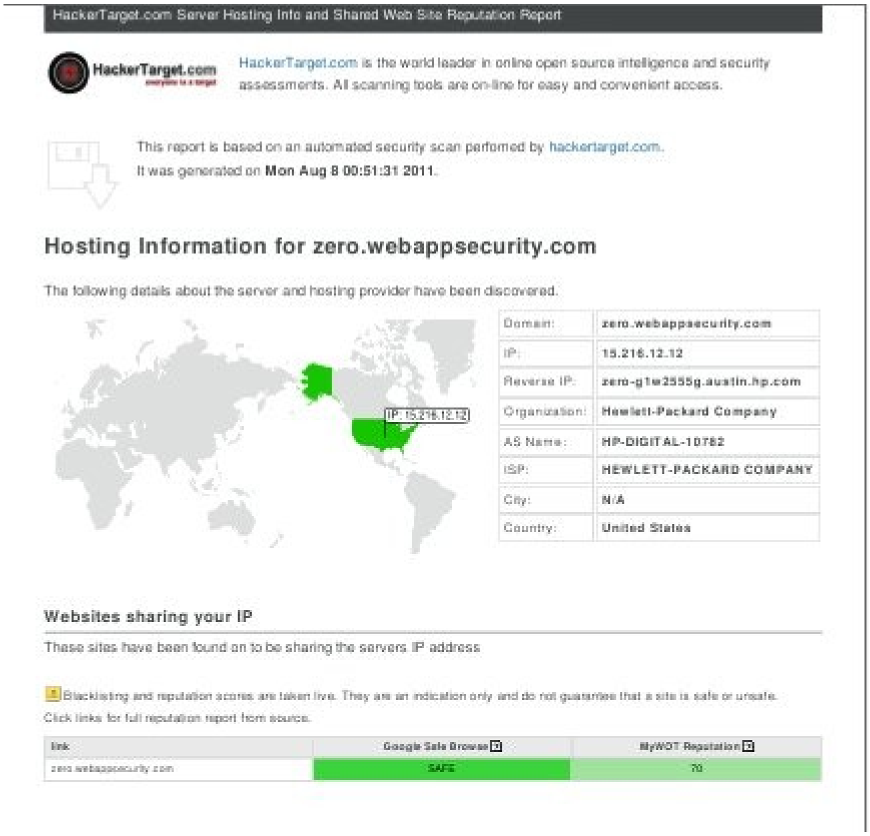
A PDF report is created and delivered to the user. The report contains details of sub-domains, IP addresses, virtual web hosts on IP addresses, data from the Shodan security search engine and IP address reputation / black list checks.

SCAN SAMPLE

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 hosting Malware and Spam.

This scan type can also be used when researching malware spreading web hosts.



HackerTarget.com Server Hosting Info and Shared Web Site Reputation Report

HackerTarget.com is the world leader in online open source intelligence and security assessments. All scanning tools are on-line for easy and convenient access.

This report is based on an automated security scan perfomed by hackertarget.com.
It was generated on **Mon Aug 8 00:51:31 2011**.

Hosting Information for zero.webappsecurity.com

The following details about the server and hosting provider have been discovered.

Domain:	zero.webappsecurity.com
IP:	15.216.12.12
Reverse IP:	zero-g1w2555g.austin.hp.com
Organization:	Hewlett-Packard Company
AS Name:	HP-DIGITAL-10782
ISP:	HEWLETT-PACKARD COMPANY
City:	N/A
Country:	United States

Websites sharing your IP

These sites have been found on to be sharing the servers IP address

Blacklisting and reputation scores are taken live. They are an indication only and do not guarantee that a site is safe or unsafe.
Click links for full reputation report from source.

link	Google Safe Browse	MyWOT Reputation
zero.webappsecurity.com	SAFE	70

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.

SCAN SAMPLE

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)

Discover interesting services; find holes in your firewall

```
** 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
```

SCAN PROJECT

OPENVAS VULNERABILITY SCAN

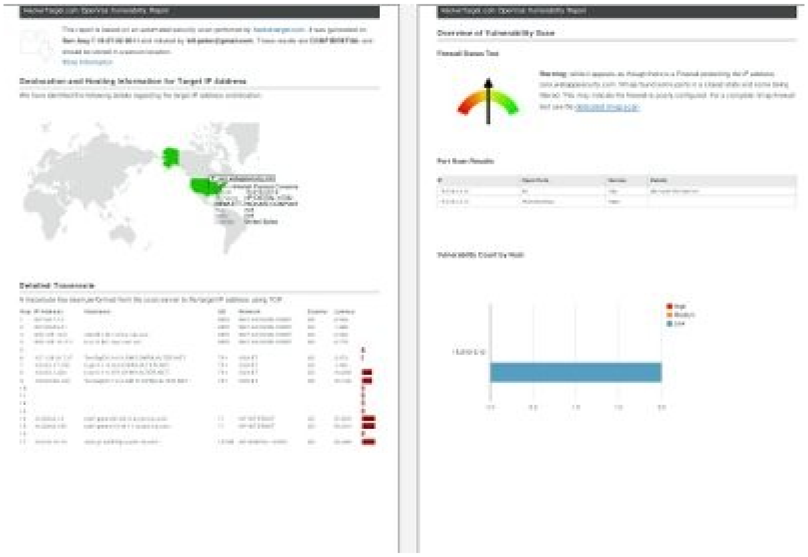
The Open Vulnerability Assessment System (OpenVAS) is an application consisting of several services and tools that offers a comprehensive vulnerability scanning solution.

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.

OpenVAS4

Find security vulnerabilities before the bad guys do with this powerful scan

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.



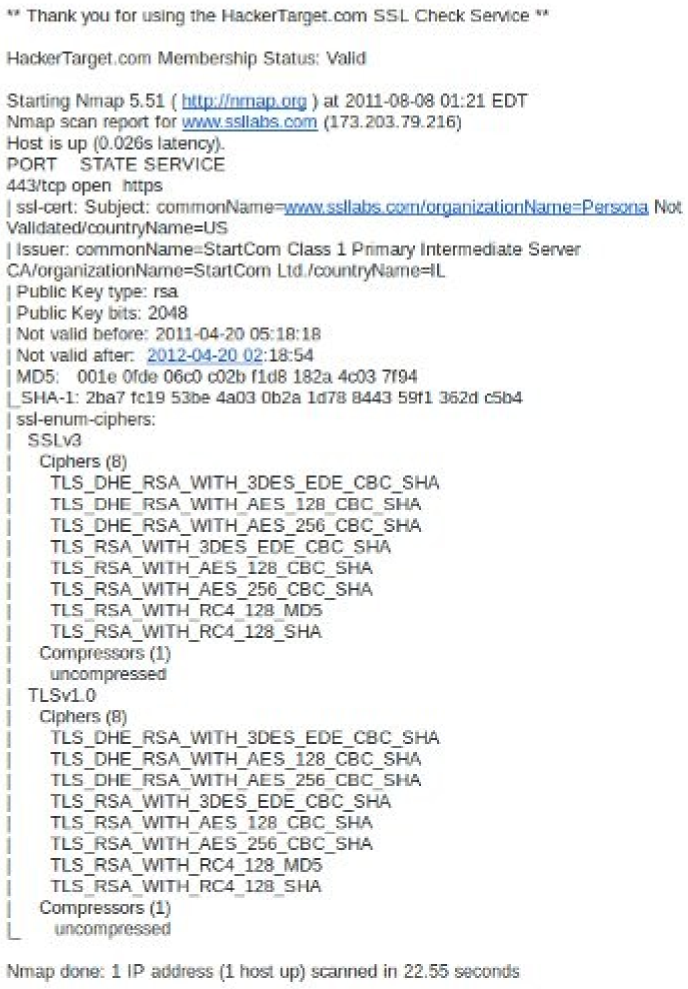
A report is created and delivered to the users designated email address. This scan can take some time to perform as it has a database of over 20000 security checks.

SCAN SAMPLE PROJECT

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.

PCI Compliance has specific requirements regarding SSL configuration.



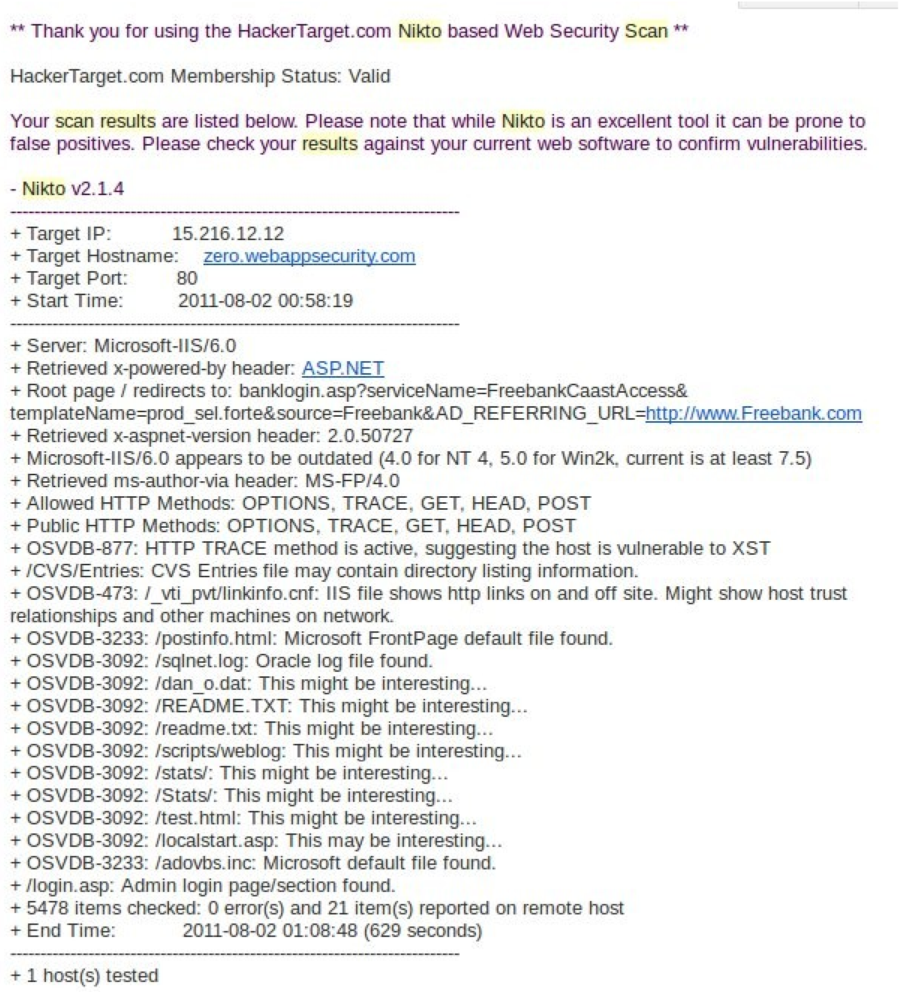
```
** Thank you for using the HackerTarget.com SSL Check Service **

HackerTarget.com Membership Status: Valid

Starting Nmap 5.51 ( http://nmap.org ) at 2011-08-08 01:21 EDT
Nmap scan report for www.ssllabs.com (173.203.79.216)
Host is up (0.026s latency).
PORT    STATE SERVICE
443/tcp open  https
| ssl-cert: Subject: commonName=www.ssllabs.com/organizationName=Persona Not
Validated/countryName=US
| Issuer: commonName=StartCom Class 1 Primary Intermediate Server
CA/organizationName=StartCom Ltd./countryName=IL
| Public Key type: rsa
| Public Key bits: 2048
| Not valid before: 2011-04-20 05:18:18
| Not valid after:  2012-04-20 02:18:54
| MD5:   001e 0fde 06c0 c02b f1d8 182a 4c03 7f94
|_SHA-1: 2ba7 fc19 53be 4a03 0b2a 1d78 8443 59f1 362d c5b4
| 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_MD5
|       TLS_RSA_WITH_RC4_128_SHA
|     Compressors (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_MD5
|       TLS_RSA_WITH_RC4_128_SHA
|     Compressors (1)
|_      uncompressed

Nmap done: 1 IP address (1 host up) scanned in 22.55 seconds
```

SCAN PROJECT

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.

Nikto is an old school security testing too that still finds lots of interesting things.



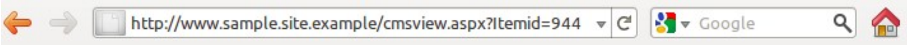
```
** Thank you for using the HackerTarget.com Nikto based Web Security Scan **

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:         2011-08-02 00:58:19
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/6.0
+ Retrieved x-powered-by header: ASP.NET
+ Root page / redirects to: banklogin.asp?serviceName=FreebankCaastAccess&
templateName=prod_sel.forte&source=Freebank&AD_REFERRING_URL=http://www.Freebank.com
+ Retrieved x-aspnet-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-FP/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: /_vti_pvt/linkinfo.cnf: 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: /test.html: This might be interesting...
+ OSVDB-3092: /localstart.asp: This may be interesting...
+ OSVDB-3233: /adovbs.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:           2011-08-02 01:08:48 (629 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

SCAN PROJECT

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:

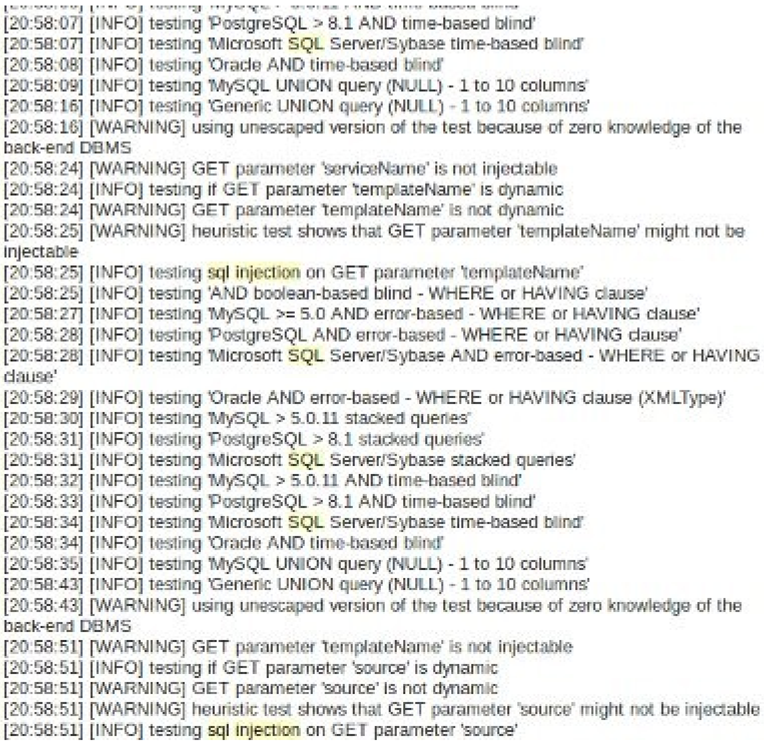


```
http://www.sample.site.example/cmsview.aspx?Itemid=944
```

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.

Enter a URL and have it quickly tested for SQL Injection Vulnerabilities



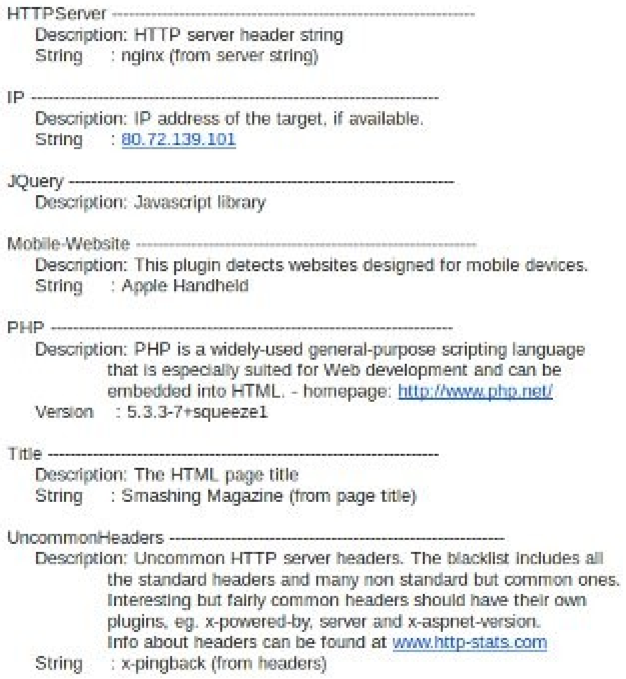
```
[20:58:07] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[20:58:07] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[20:58:08] [INFO] testing 'Oracle AND time-based blind'
[20:58:09] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[20:58:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[20:58:16] [WARNING] using unescaped version of the test because of zero knowledge of the
back-end DBMS
[20:58:24] [WARNING] GET parameter 'serviceName' is not injectable
[20:58:24] [INFO] testing if GET parameter 'templateName' is dynamic
[20:58:24] [WARNING] GET parameter 'templateName' is not dynamic
[20:58:25] [WARNING] heuristic test shows that GET parameter 'templateName' might not be
injectable
[20:58:25] [INFO] testing sql injection on GET parameter 'templateName'
[20:58:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:58:27] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[20:58:28] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[20:58:28] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING
clause'
[20:58:29] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[20:58:30] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[20:58:31] [INFO] testing 'PostgreSQL > 8.1 stacked queries'
[20:58:31] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'
[20:58:32] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[20:58:33] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[20:58:34] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[20:58:34] [INFO] testing 'Oracle AND time-based blind'
[20:58:35] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[20:58:43] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[20:58:43] [WARNING] using unescaped version of the test because of zero knowledge of the
back-end DBMS
[20:58:51] [WARNING] GET parameter 'templateName' is not injectable
[20:58:51] [INFO] testing if GET parameter 'source' is dynamic
[20:58:51] [WARNING] GET parameter 'source' is not dynamic
[20:58:51] [WARNING] heuristic test shows that GET parameter 'source' might not be injectable
[20:58:51] [INFO] testing sql injection on GET parameter 'source'
```

SCAN PROJECT

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.

Find technologies and scripts being used by your favorite sites with this non-intrusive scan.



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

IP -----------------------------------------------------------------------------
    Description: IP address of the target, if available.
    String     : 80.72.139.101

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/
    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
    String     : x-pingback (from headers)
```

SCAN

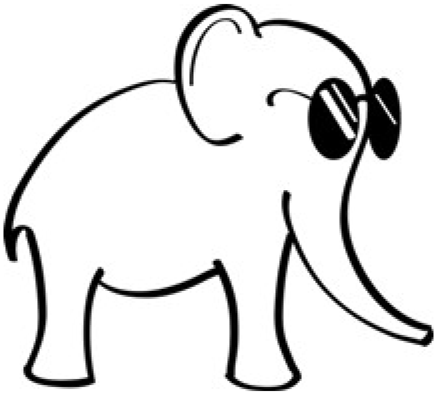
PROJECT

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.

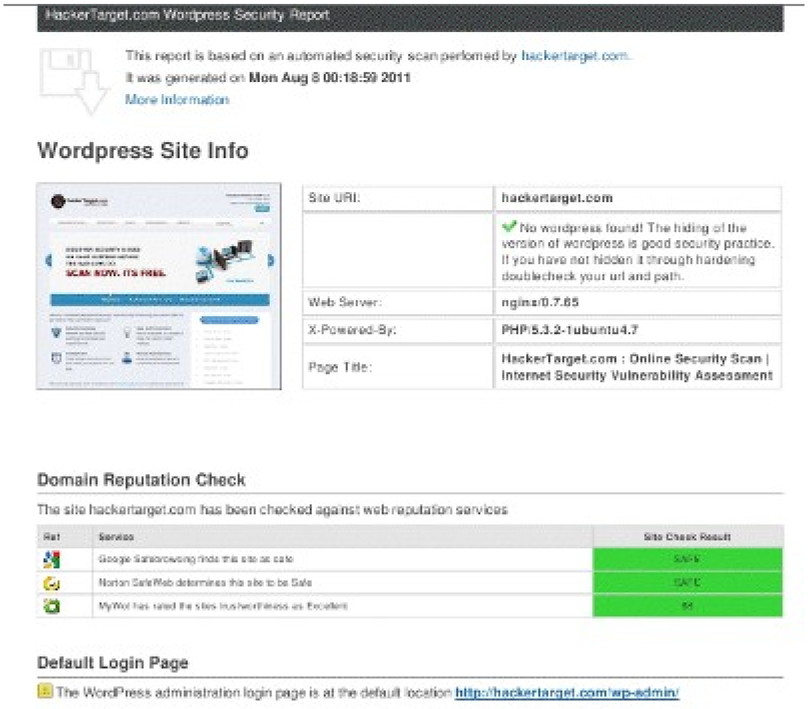


SCAN PROJECT

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.

Wordpress is an easy to use web site content management systems that is a **popular target for hackers**.



HackerTarget.com Wordpress Security Report

This report is based on an automated security scan perfomed by hackertarget.com.
It was generated on **Mon Aug 8 00:18:59 2011**
More Information

Wordpress Site Info

Site URI:	**hackertarget.com**
	✓ No wordpress found! The hiding of the version of wordpress is good security practice. If you have not hidden it through hardening doublecheck your url and path.
Web Server:	**nginx/0.7.65**
X-Powered-By:	**PHP/5.3.2-1ubuntu4.7**
Page Title:	**HackerTarget.com : Online Security Scan | Internet Security Vulnerability Assessment**

Domain Reputation Check

The site hackertarget.com has been checked against web reputation services

Ref	Service	Site Check Result
	Google Safebrowsing finds this site as safe	SAFE
	Norton SafeWeb determines this site to be Safe	SAFE
	MyWot has rated the sites trustworthiness as Excellent	[illegible]

Default Login Page

The WordPress administration login page is at the default location http://hackertarget.com/wp-admin/

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.

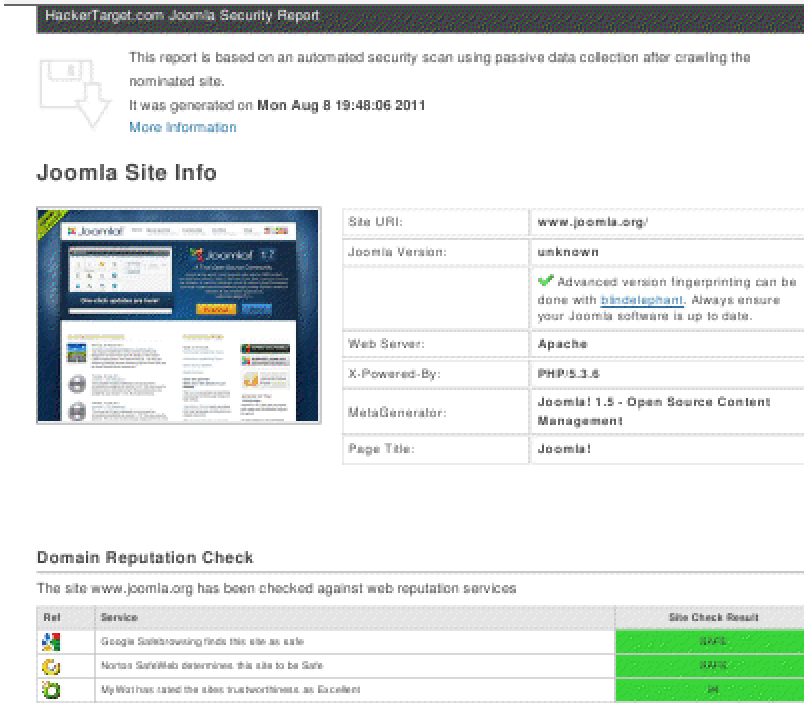
SCAN SAMPLE

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.

Joomla is a popular open source CMS.

Test Security of your installation now with this non-intrusive scan.



HackerTarget.com Joomla Security Report

This report is based on an automated security scan using passive data collection after crawling the nominated site.

It was generated on **Mon Aug 8 19:48:06 2011**

More Information

Joomla Site Info

Site URI:	**www.joomla.org/**
Joomla Version:	**unknown**
	✓ Advanced version fingerprinting can be done with blindelephant. Always ensure your Joomla software is up to date.
Web Server:	**Apache**
X-Powered-By:	**PHP/5.3.6**
MetaGenerator:	**Joomla! 1.5 - Open Source Content Management**
Page Title:	**Joomla!**

Domain Reputation Check

The site www.joomla.org has been checked against web reputation services

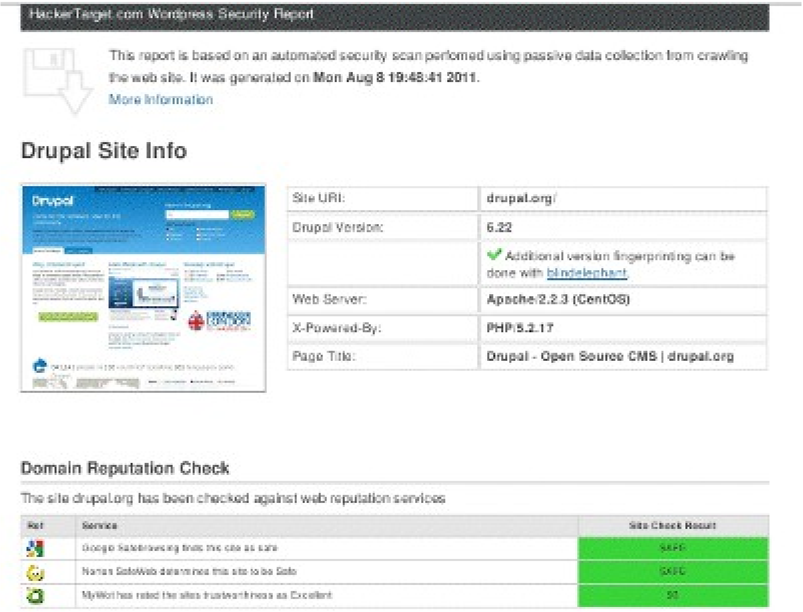
Ref	Service	Site Check Result
	Google Safebrowsing finds this site as safe	SAFE
	Norton SafeWeb determines this site to be Safe	SAFE
	MyWot has rated the sites trustworthiness as Excellent	94

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.

SCAN SAMPLE

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.



HackerTarget.com Wordpress Security Report

This report is based on an automated security scan perfomed using passive data collection from crawling the web site. It was generated on **Mon Aug 8 19:48:41 2011**.
More Information

Drupal Site Info

Site URI:	**drupal.org/**
Drupal Version:	**6.22**
	✓ Additional version fingerprinting can be done with blindelephant
Web Server:	**Apache/2.2.3 (CentOS)**
X-Powered-By:	**PHP/5.2.17**
Page Title:	**Drupal - Open Source CMS | drupal.org**

Domain Reputation Check

The site drupal.org has been checked against web reputation services

Ref	Service	Site Check Result
	Google Safebrowsing finds this site as safe	SAFE
	Norton SafeWeb determines this site to be Safe	SAFE
	MyWot has rated the sites trustworthiness as Excellent	93

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

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.

SCAN

SAMPLE

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.