TUGAS KEAMANAN JARINGAN KOMPUTER

"SCANNING LAZADA.COM"

NAMA : DESY MARITA

NIM : 09011281320017

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

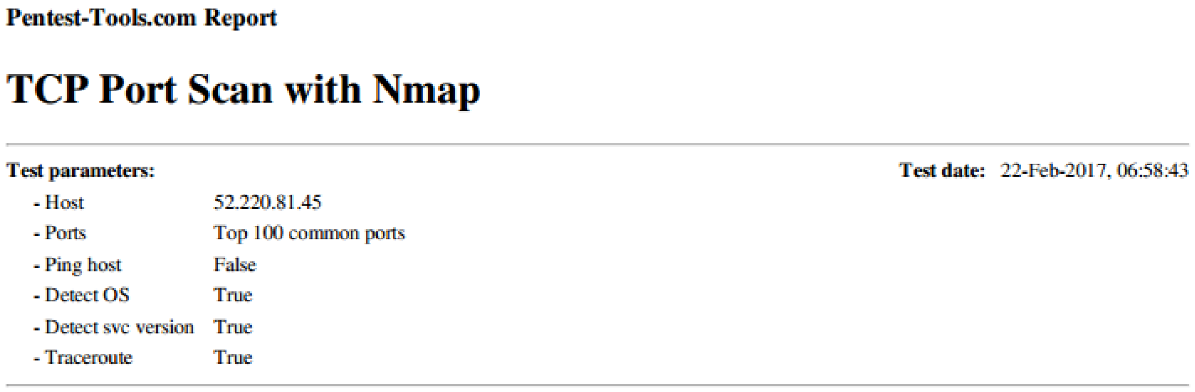
UNIVERSITAS SRIWIJAYA

2017

Scanning bertujuan untuk mencari port target yang terbuka, aplikasi yang rentan terhadap kegiatan hacking dan celah lainnya. Port scanning adalah proses koneksi ke port-port TCP pada host yang menjadi target untuk menentukan service apa yang sedang berjalan (Listening). Dengan mengidentifikasi port-port yang listening ini dapat menentukan jenis aplikasi dan sistem operasi apa yang dipergunakan pada host tersebut. Service yang dalam status listening ini memungkinkan orang yang tidak berhak menerobos ke dalam host tersebut. Target yang saya scan yaitu Lazada.com. Untuk mendapatkan hasil scanning langkah yang dilakukan yaitu :

1. Pertama buka tools yang digunakan, disini saya menggunakan tools port TCP with Nmap dengan mengetikkan alamat website https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap kemudian isikan ip address target yang akan di scan. Lalu akan muncul seperti gambar dibawah ini :

   Ip address target : 52.74.30.111

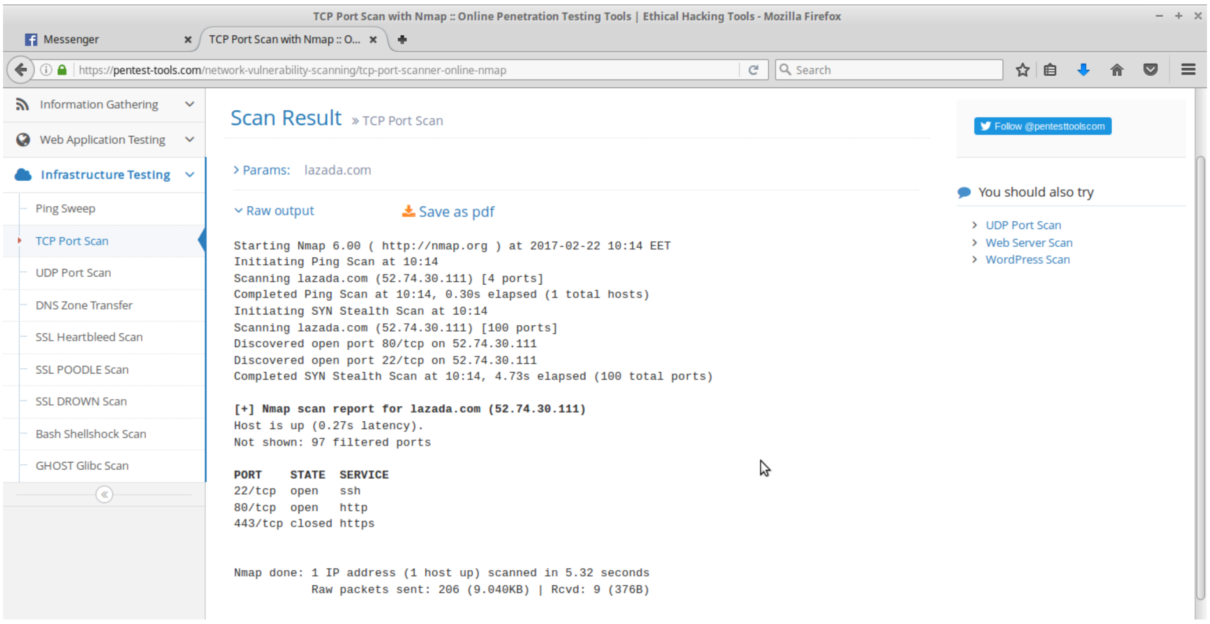


Pentest-Tools.com Report

TCP Port Scan with Nmap

Test parameters: **Test date:** 22-Feb-2017, 06:58:43

- Host	52.220.81.45
- Ports	Top 100 common ports
- Ping host	False
- Detect OS	True
- Detect svc version	True
- Traceroute	True



TCP Port Scan with Nmap :: Online Penetration Testing Tools | Ethical Hacking Tools - Mozilla Firefox

https://pentest-tools.com/network-vulnerability-scanning/tcp-port-scanner-online-nmap

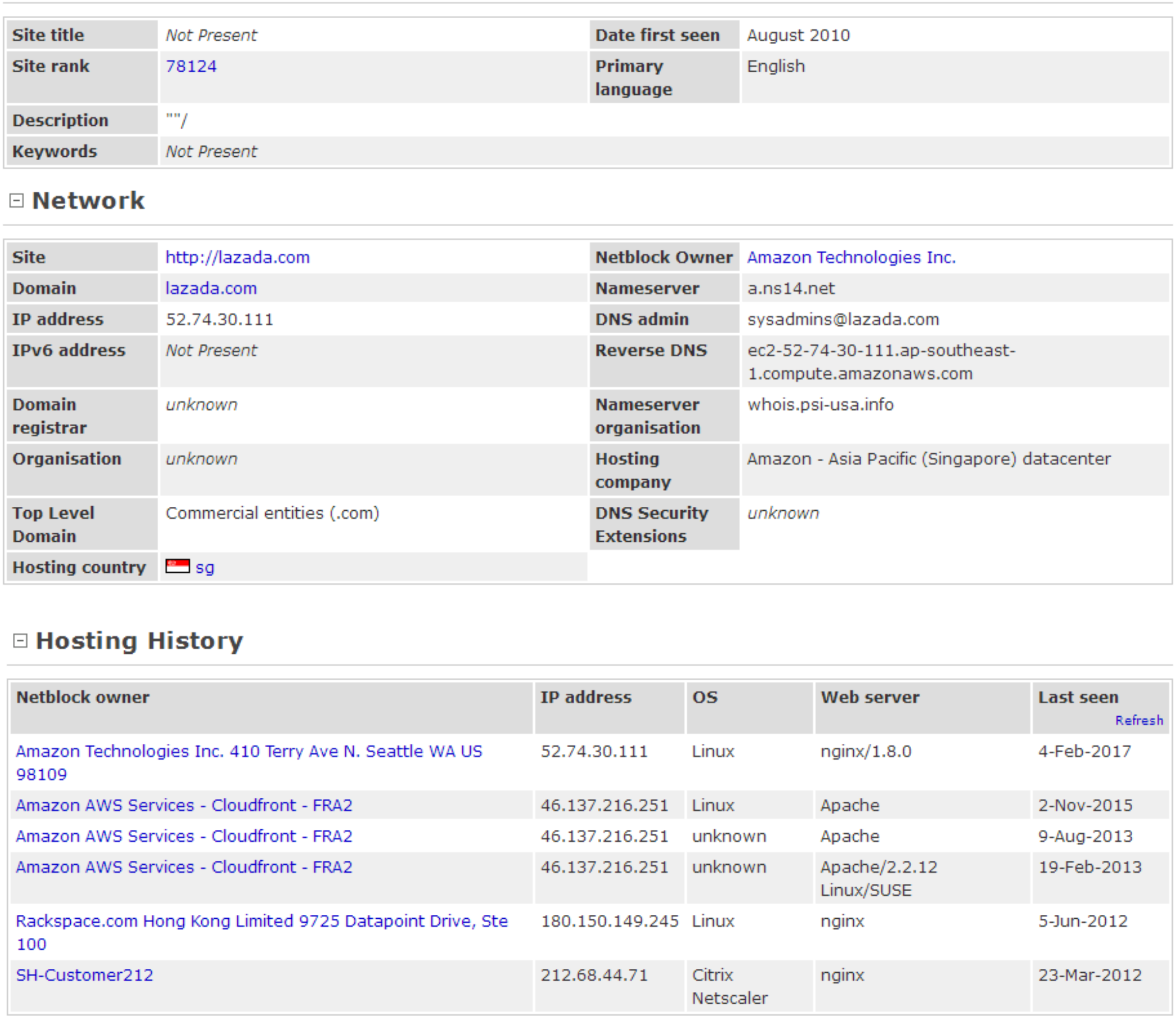
Scan Result » TCP Port Scan

Params: lazada.com

```
Starting Nmap 6.00 ( http://nmap.org ) at 2017-02-22 10:14 EET
Initiating Ping Scan at 10:14
Scanning lazada.com (52.74.30.111) [4 ports]
Completed Ping Scan at 10:14, 0.30s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:14
Scanning lazada.com (52.74.30.111) [100 ports]
Discovered open port 80/tcp on 52.74.30.111
Discovered open port 22/tcp on 52.74.30.111
Completed SYN Stealth Scan at 10:14, 4.73s elapsed (100 total ports)

[+] Nmap scan report for lazada.com (52.74.30.111)
Host is up (0.27s latency).
Not shown: 97 filtered ports

PORT    STATE  SERVICE
22/tcp  open   ssh
80/tcp  open   http
443/tcp closed https


Nmap done: 1 IP address (1 host up) scanned in 5.32 seconds
           Raw packets sent: 206 (9.040KB) | Rcvd: 9 (376B)
```

Gambar di atas menunjukan port-port yang bisa di akses dan yang tidak bisa di akses. Pada scan yang dilakukan pada target mendapatkan hasil port yang bisa di akses ada 2 yaitu ssh (port 22/tcp) dan http (port 88/tcp). Sedangkan yang tidak bisa di akses ada 1 yaitu https (port 443/tcp).

2. Tools kedua yang digunakan yaitu Netcraft dengan mengetikkan alamat website http://toolbar.netcraft.com/site_report?url=lazada.com lalu memasukkan nama Domain target yang akan di scan lalu akan muncul seprti gambar di bawah ini :



Site title	*Not Present*	**Date first seen**	August 2010
Site rank	78124	**Primary language**	English
Description	""/		
Keywords	*Not Present*		

⊟ **Network**

Site	http://lazada.com	**Netblock Owner**	Amazon Technologies Inc.
Domain	lazada.com	**Nameserver**	a.ns14.net
IP address	52.74.30.111	**DNS admin**	sysadmins@lazada.com
IPv6 address	*Not Present*	**Reverse DNS**	ec2-52-74-30-111.ap-southeast-1.compute.amazonaws.com
Domain registrar	*unknown*	**Nameserver organisation**	whois.psi-usa.info
Organisation	*unknown*	**Hosting company**	Amazon - Asia Pacific (Singapore) datacenter
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	sg		

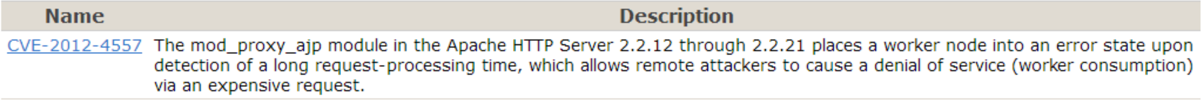
⊟ **Hosting History**

Netblock owner	IP address	OS	Web server	Last seen Refresh
Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	52.74.30.111	Linux	nginx/1.8.0	4-Feb-2017
Amazon AWS Services - Cloudfront - FRA2	46.137.216.251	Linux	Apache	2-Nov-2015
Amazon AWS Services - Cloudfront - FRA2	46.137.216.251	unknown	Apache	9-Aug-2013
Amazon AWS Services - Cloudfront - FRA2	46.137.216.251	unknown	Apache/2.2.12 Linux/SUSE	19-Feb-2013
Rackspace.com Hong Kong Limited 9725 Datapoint Drive, Ste 100	180.150.149.245	Linux	nginx	5-Jun-2012
SH-Customer212	212.68.44.71	Citrix Netscaler	nginx	23-Mar-2012

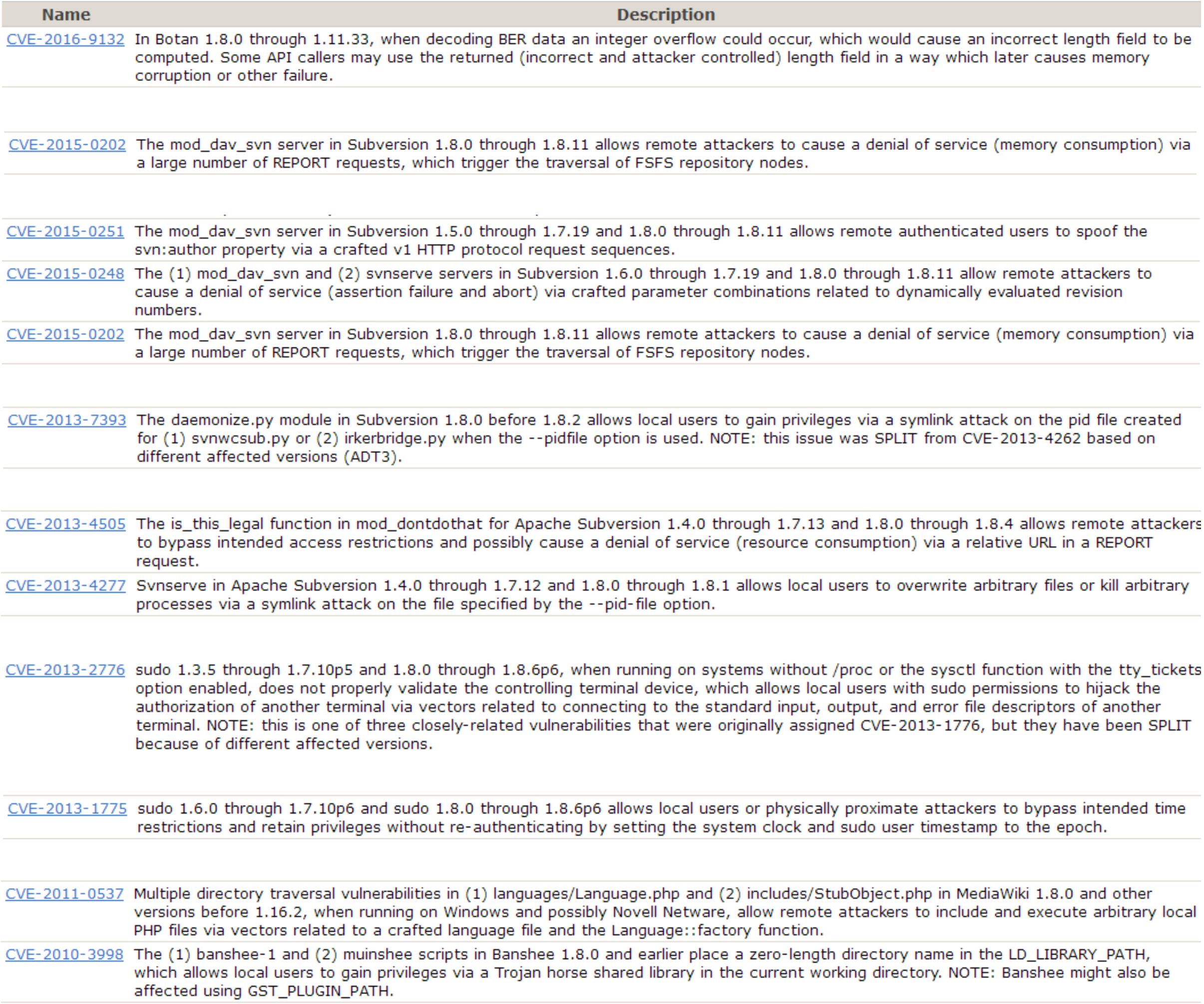
Pada gambar di atas kita dapat mengetahui Ip Address, OS, Web Server, Last seen yang ada pada target.

3. Tools ketiga yang dilakukan untuk melihat CVE yang di pakai dan tipe apa. CVE yang dipakai yaitu Apache. Untuk melihatnya ketikkan tipe CVE apa yang dipakai ke alamat website http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=nginx%2F1.8.0

   Maka akan di dapat hasil seperti gambar di bawah ini :



Name	Description
CVE-2012-4557	The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of service (worker consumption) via an expensive request.



Name	Description
CVE-2016-9132	In Botan 1.8.0 through 1.11.33, when decoding BER data an integer overflow could occur, which would cause an incorrect length field to be computed. Some API callers may use the returned (incorrect and attacker controlled) length field in a way which later causes memory corruption or other failure.
CVE-2015-0202	The mod_dav_svn server in Subversion 1.8.0 through 1.8.11 allows remote attackers to cause a denial of service (memory consumption) via a large number of REPORT requests, which trigger the traversal of FSFS repository nodes.
CVE-2015-0251	The mod_dav_svn server in Subversion 1.5.0 through 1.7.19 and 1.8.0 through 1.8.11 allows remote authenticated users to spoof the svn:author property via a crafted v1 HTTP protocol request sequences.
CVE-2015-0248	The (1) mod_dav_svn and (2) svnserve servers in Subversion 1.6.0 through 1.7.19 and 1.8.0 through 1.8.11 allow remote attackers to cause a denial of service (assertion failure and abort) via crafted parameter combinations related to dynamically evaluated revision numbers.
CVE-2015-0202	The mod_dav_svn server in Subversion 1.8.0 through 1.8.11 allows remote attackers to cause a denial of service (memory consumption) via a large number of REPORT requests, which trigger the traversal of FSFS repository nodes.
CVE-2013-7393	The daemonize.py module in Subversion 1.8.0 before 1.8.2 allows local users to gain privileges via a symlink attack on the pid file created for (1) svnwcsub.py or (2) irkerbridge.py when the --pidfile option is used. NOTE: this issue was SPLIT from CVE-2013-4262 based on different affected versions (ADT3).
CVE-2013-4505	The is_this_legal function in mod_dontdothat for Apache Subversion 1.4.0 through 1.7.13 and 1.8.0 through 1.8.4 allows remote attackers to bypass intended access restrictions and possibly cause a denial of service (resource consumption) via a relative URL in a REPORT request.
CVE-2013-4277	Svnserve in Apache Subversion 1.4.0 through 1.7.12 and 1.8.0 through 1.8.1 allows local users to overwrite arbitrary files or kill arbitrary processes via a symlink attack on the file specified by the --pid-file option.
CVE-2013-2776	sudo 1.3.5 through 1.7.10p5 and 1.8.0 through 1.8.6p6, when running on systems without /proc or the sysctl function with the tty_tickets option enabled, does not properly validate the controlling terminal device, which allows local users with sudo permissions to hijack the authorization of another terminal via vectors related to connecting to the standard input, output, and error file descriptors of another terminal. NOTE: this is one of three closely-related vulnerabilities that were originally assigned CVE-2013-1776, but they have been SPLIT because of different affected versions.
CVE-2013-1775	sudo 1.6.0 through 1.7.10p6 and sudo 1.8.0 through 1.8.6p6 allows local users or physically proximate attackers to bypass intended time restrictions and retain privileges without re-authenticating by setting the system clock and sudo user timestamp to the epoch.
CVE-2011-0537	Multiple directory traversal vulnerabilities in (1) languages/Language.php and (2) includes/StubObject.php in MediaWiki 1.8.0 and other versions before 1.16.2, when running on Windows and possibly Novell Netware, allow remote attackers to include and execute arbitrary local PHP files via vectors related to a crafted language file and the Language::factory function.
CVE-2010-3998	The (1) banshee-1 and (2) muinshee scripts in Banshee 1.8.0 and earlier place a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse shared library in the current working directory. NOTE: Banshee might also be affected using GST_PLUGIN_PATH.

CVE-2008-0618	Multiple cross-site scripting (XSS) vulnerabilities in the DMSGuestbook 1.8.0 and 1.7.0 plugin for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) gbname, (2) gbemail, (3) gburl, and (4) gbmsg parameters to unspecified programs. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.
CVE-2008-0615	Directory traversal vulnerability in wp-admin/admin.php in the DMSGuestbook 1.8.0 and 1.7.0 plugin for WordPress allows remote authenticated users to read arbitrary files via a .. (dot dot) in the (1) folder and (2) file parameters.
CVE-2007-4828	Cross-site scripting (XSS) vulnerability in the API pretty-printing mode in MediaWiki 1.8.0 through 1.8.4, 1.9.0 through 1.9.3, 1.10.0 through 1.10.1, and the 1.11 development versions before 1.11.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2007-2902	SQL injection vulnerability in main/auth/my_progress.php in Dokeos 1.8.0 and earlier allows remote authenticated users to execute arbitrary SQL commands via the course parameter.
CVE-2007-2901	Multiple cross-site scripting (XSS) vulnerabilities in Dokeos 1.8.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the img parameter to main/inc/lib/fckeditor/editor/plugins/ImageManager/editor.php and other unspecified vectors.
CVE-2006-7126	SQL injection vulnerability in Joomla BSQ Sitestats 1.8.0 and 2.2.1 allows remote attackers to execute arbitrary SQL commands via the query string, possibly PHP_SELF.
CVE-2006-7125	Cross-site scripting (XSS) vulnerability in Joomla BSQ Sitestats 1.8.0 and 2.2.1 allows remote attackers to inject arbitrary web script or HTML via the HTTP Referer header, which is not properly handled when the administrator views site statistics.
CVE-2006-7124	PHP remote file inclusion vulnerability in external/rssfeeds.php in BSQ Sitestats (component for Joomla) 1.8.0, and possibly other versions before 2.2.1, allows remote attackers to execute arbitrary PHP code via the baseDir parameter.
CVE-2006-7123	Multiple SQL injection vulnerabilities in BSQ Sitestats (component for Joomla) 1.8.0, and possibly other versions before 2.2.1, allow remote attackers to execute arbitrary SQL commands via (1) unspecified parameters when importing the (a) ip-to-country.csv file; and the (2) HTTP Referer, (3) HTTP User Agent, and (4) HTTP Accept Language headers to (b) bsqtemplateinc.php.
CVE-2006-7122	Cross-site scripting (XSS) vulnerability in the IP Address Lookup functionality in BSQ Sitestats (component for Joomla) 1.8.0, and possibly other versions before 2.2.1, allows remote attackers to inject arbitrary web script and HTML via the ip parameter.
CVE-2006-6665	Buffer overflow in Astonsoft DeepBurner Pro and Free 1.8.0 and earlier allows user-assisted remote attackers to execute arbitrary code via a long file name tag in a dbr file.
CVE-2006-5256	PHP remote file inclusion vulnerability in claroline/inc/lib/import.lib.php in Claroline 1.8.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the includePath parameter.
CVE-2006-3483	PHPMailList 1.8.0 stores sensitive information under the web document root iwth insufficient access control, which allows remote attackers to obtain email addresses of subscribers, configuration information, and the admin username and password via direct requests to (1) list.dat or (2) ml_config.dat.
CVE-2006-3482	Cross-site scripting (XSS) vulnerability in maillist.php in PHPMailList 1.8.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the email parameter.
CVE-2006-2613	Mozilla Suite 1.7.13, Mozilla Firefox 1.5.0.3 and possibly other versions before before 1.8.0, and Netscape 7.2 and 8.1, and possibly other versions and products, allows remote user-assisted attackers to obtain information such as the installation path by causing exceptions to be thrown and checking the message contents.
CVE-2006-0804	Off-by-one error in TIN 1.8.0 and earlier might allow attackers to execute arbitrary code via unknown vectors that trigger a buffer overflow.
CVE-2004-0409	Stack-based buffer overflow in the Socks-5 proxy code for XChat 1.8.0 to 2.0.8, with socks5 traversal enabled, allows remote attackers to execute arbitrary code.