

# ClubHACKMag

Issue 7 | Aug 2010  
www.chmag.in

1st Indian "HACKING" Magazine



© Bharat Narayanan

**TechGyan** Advance XSS attacks | **LegalGyan** Open Source Licenses |  
**ToolGyan** MBSA | **Mom's Guide** Knowing your system in depth |

Welcome to another issue of ClubHACK Magazine. This time around we bring you articles covering topics such as Dom based Advanced XSS Attacks, Microsoft Baseline Security Analyzer, Open Source Licenses, etc.

Also we're getting ready for a big event – ClubHACK Conference in December. And for those who don't know, the keynote guest is Bruce Schneier. Yes it is Bruce!

We would like to encourage everyone who would like to share his/her knowledge with others. Don't be shy, do not doubt your own gifts and talents – do not hesitate and write to us when the idea of article come to your mind!

We are always open to suggestions and feedbacks. Keep them coming at [info@chmag.in](mailto:info@chmag.in)



Abhijeet Patil

# ClubHACKMag

Issue 7, August 2010.

## Team CHmag

Rohit Srivastwa  
*rohit@clubhack.com*

Aarja Bhattacharyya  
*aarja@chmag.in*

Abhijeet R Patil  
*abhijeet@chmag.in*

Abhishek Nagar  
*abhishek@chmag.in*

Deepranjan S More  
*deepranjan@chmag.in*

Pankit Thakkar  
*pankit@chmag.in*

Varun V Hirve  
*varun@chmag.in*

[www.chmag.in](http://www.chmag.in)  
[info@chmag.in](mailto:info@chmag.in)

# CONTENTS

Pg **TechGyan**  
03 DOM Based Advance  
XSS Attacks

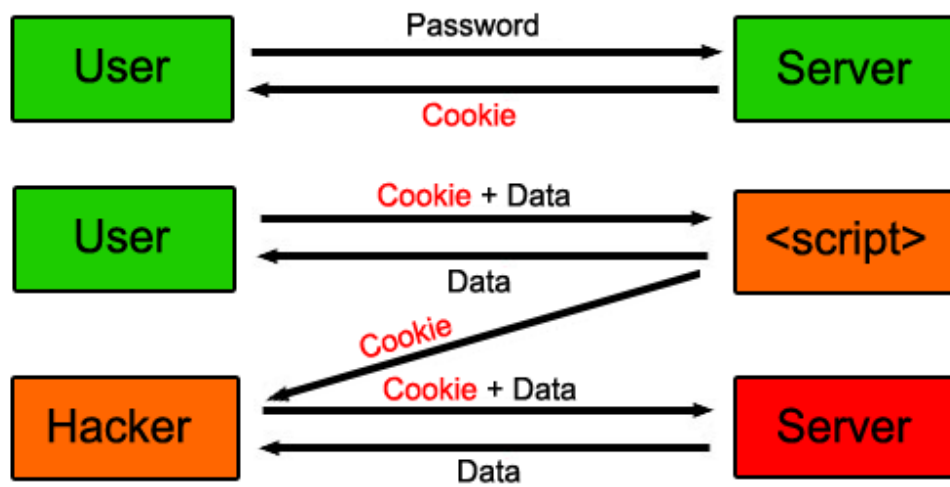
Pg **ToolGyan**  
09 Microsoft Baseline Security  
Analyzer

Pg **Mom'sGuide**  
23 Belarc Advisor

Pg **LegalGyan**  
25 Open Source Licenses

Pg **Command LineGyan**  
31 Playing with  
network config

# TechGYAN



the backend database for the information specified by the *product\_id* value which is shown to the user. (Figure 1.2)

## Advance XSS Attacks, DOM Based

Robert ‘rsnake’ Hensen is considered as Guru of XSS. Let’s learn advance DOM based attack from his own book “XSS attacks: cross-site scripting exploits and defense”

Preview of his book is available at [books.google.com/books?id=Imt5Crr0jJcC](http://books.google.com/books?id=Imt5Crr0jJcC)

### Introduction

DOM-based is unique form of XSS, used very similarly to non-persistent, but where the JavaScript malware payload doesn’t need to be sent or echoed by the Web site to exploit auser. Consider our eCommerce Web site example (Figure 1.1.), where a feature on the Website is used to display sales promotions. The following URL queries

FIG 1.1

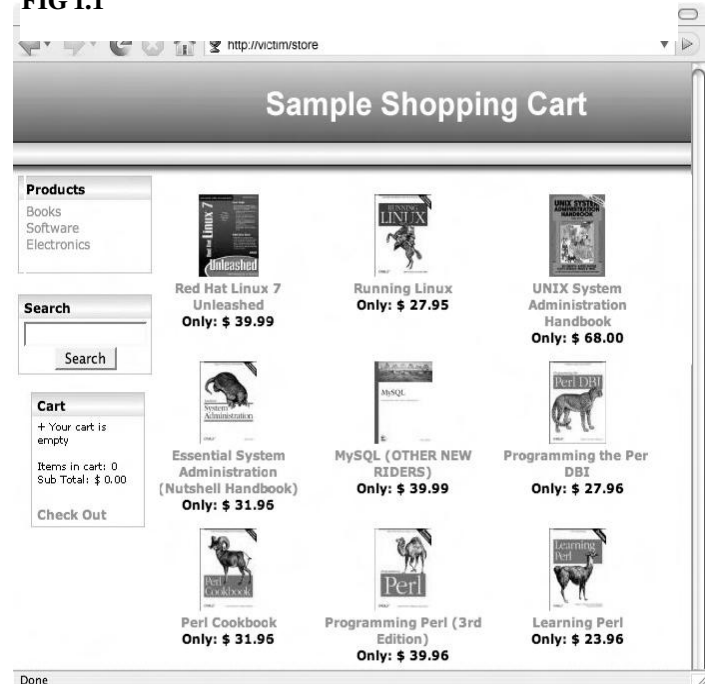


FIG 1.2



To make the user experience a bit more dynamicity, the title value of the URL's can be updated on the fly to include different impulse-buy text

### **Example 1**

```
http://victim/promo?product_id=100&title=Last+Chance!
```

```
http://victim/promo?product_id=100&title=Only+10+Left!
```

Etc.

The value of the title is automatically written to the page using some resident JavaScript.

### **Example 2**

```
<script>
```

```
var url = window.location.href;
```

```
var pos = url.indexOf("title=") + 6;
```

```
var len = url.length;
```

```
var title_string = url.substring(pos,len);
```

```
document.write(unescape(title_string));
```

```
</script>
```

This is where the problem is. In this scenario, the client-side JavaScript blindly trusts the

data contained in the URL and renders it to the screen. This trust can be leveraged to craft

the following URL that contains some JavaScript malware on the end.

### **Example 3**

```
http://victim/promo?product_id=100&title=Foo#<SCRIPT>alert('XSS%20Testing')
```

```
</SCRIPT>
```

As before, this URL can be manipulated to SRC in additional JavaScript malware from

any location on the Web. What makes this style of XSS different, is that the JavaScript malware

payload does not get sent to the Web server. As defined by Request For Comment

(RFC), the "fragment" portion of the URL, after the pound sign, indicates to the Web

browser which point of the current document to jump to. Fragment data does not get sent

to the Web server and stays within the DOM. Hence the name, DOM-based XSS.

## Persistent

Persistent (or HTML Injection) XSS attacks most often occur in either community content-driven Web sites or Web mail sites, and do not require specially crafted links for execution. A hacker merely submits XSS exploit code to an area of a Web site that is likely to be visited by other users. These areas could be blog comments, user reviews, message board posts, chat rooms, HTML e-mail, wikis, and numerous other locations. Once a user visits the infected Web page, the execution is automatic. This makes persistent XSS much more dangerous than non-persistent or DOM-based, because the user has no means of defending himself. Once a hacker has his exploit code in place, he'll again advertise the URL to the infected Web page, hoping to snare unsuspecting users. Even users who are wise to non-persistent XSS URLs can be easily compromised

## DOM-based XSS In Detail

DOM is a World Wide Web Consortium (W3C) specification, which defines the object model for representing XML and HTML structures. In the eXtensible Markup Language (XML) world, there are mainly two types of parsers, DOM and SAX. SAX is a parsing mechanism, which is significantly faster and less memory-intensive but also not very intuitive, because it is not easy to go back to the document nodes (i.e. the parsing mechanism is one way). On the other hand, DOM-based parsers load the entire document as an object structure, which contains methods and variables to easily move around the document and modify nodes, values, and attributes on the fly.

Browsers work with DOM. When a page is loaded, the browser parses the resulting

page into an object structure. The *getElementsByTagName* is a standard DOM function that is used to locate XML/HTML nodes based on their tag name. DOM-based XSS is the exploitation of an input validation vulnerability that is caused by the client, not the server. In other words, DOM-based XSS is not a result of a vulnerability within a server side script, but an improper handling of user supplied data in the client side JavaScript. Like the other types of XSS vulnerabilities, DOM-based XSS can be used to steal confidential information or hijack the user account. However, it is essential to understand that this type of vulnerability solely relies upon JavaScript and insecure use of dynamically obtained data from the DOM structure.

Here is a simple example of a DOM-based XSS provided by Amit Klein in his paper "Dom Based Cross Site Scripting or XSS of the Third Kind":

```
<HTML>
<TITLE>Welcome!</TITLE>
Hi
<SCRIPT>
var
pos=document.URL.indexOf("name=")+5;
document.write(document.URL.substring(p
os,document.URL.length));
</SCRIPT>
<BR>
Welcome to our system
...
</HTML>
```

If we analyze the code of the example, you will see that the developer has forgotten to sanitize the value of the “name” get parameter, which is subsequently written inside the document as soon as it is retrieved. In the following section, we study a few more DOM based XSS examples based on a fictitious application that we created.

## Identifying DOM-based XSS Vulnerabilities

Let’s walk through the process of identifying DOM-based XSS vulnerabilities using a fictitious Asynchronous Javascript and XML (AJAX) application.

First, we have to create a page on the local system that contains the following code:

```
<!DOCTYPE html PUBLIC "-//W3C//DTD
XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xht
ml1-transitional.dtd">
<html
xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type"
content="text/html; charset=UTF-8"/>
<link rel="stylesheet"
href="http://www.gnucitizen.org/styles/scr
een.css" type="text/css"/>
<link rel="stylesheet"
href="http://www.gnucitizen.org/styles/co
ntent.css" type="text/css"/>
<script src="http://jquery.com/src/jquery-
latest.pack.js"
```

```
type="text/javascript"></script>
<title>Awesome</title>
</head>
<body>
<div id="header">
<h1>Awesome</h1>
<p>awesome ajax application</p>
</div>
<div id="content">
<div>
<p>Please, enter your nick and press
<strong>chat</strong>!</p>
<input name="name" type="text"
size="50"/><br/><input
name="chat" value="Chat" type="button"/>
</div>
</div>
<script>
$('[@name="chat"]').click(function () {
var name = $('[@name="name"]').val();
$('#content > div').fadeOut(null, function ()
{
$(this).html('<p>Welcome ' + name + '! You
can
type your message into the form
below.</p><textarea class="pane">' +
name + '&gt;');
</textarea>');
$(this).fadeIn();
```

```

});
});
</script>
<div id="footer">
<p>Awesome AJAX Application</p>
</div>
</body>
</html>

```

Next, open the file in your browser (requires JavaScript to be enabled).The application looks like that shown in Figure 1.3

FIG 1.3



Once the page is loaded, enter your name and press the **Chat** button. This example is limited in that you cannot communicate with other users. We deliberately simplified the application so that we can concentrate on the actual vulnerability rather than the application design. Figure 1.4 shows the AJAX application in action.

FIG 1.4



Notice that this AJAX application does not need a server to perform the desired functions. Remember, you are running it straight from your desktop. Everything is handled by your browser via JavaScript and jQuery.

**\*\* jQuery is a useful AJAX library created by John Resig. jQuery significantly simplifies AJAX development, and makes it easy for developers to code in a cross-browser manner.\*\***

If you carefully examine the structure and logic of the JavaScript code, you will see that the “Awesome AJAX application” is vulnerable to XSS. The part responsible for this input sanitization failure is as follows:

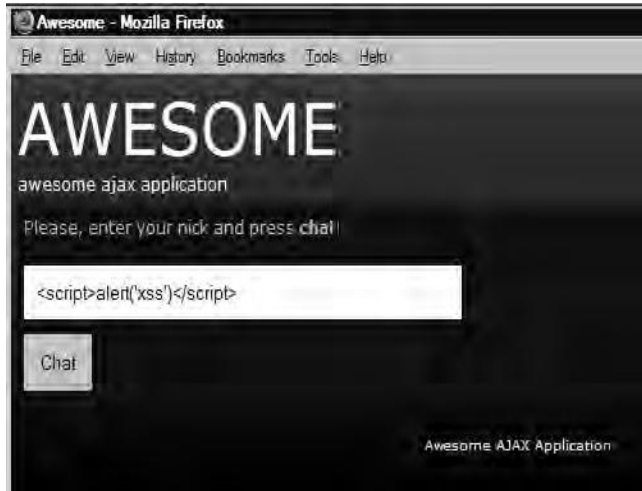
```
$(this).html('<p>Welcome ' + name + '! You can type your message into the form
```

below.</p><textarea class="pane"> + name + ' &gt; </textarea>');

As seen, the application composes a HTML string via JQuery's HTML function. The html function modifies the content of the selected element. This string includes the data from the nickname input field. In our case, the input's value is "Bob." However, because the application fails to sanitize the name, we can virtually input any other type of HTML, even script elements, as shown on Figure 1.5



FIG 1.5



If you press the **Chat** button, you will inject the malicious payload into the DOM. This payload composes a string that looks like the following:

```
<p>Welcome <script>alert('xss')</script>!
You can type your message into the form
below.</p><textarea
class="pane"><script>alert('xss')</script>
&gt; </textarea>
```

This is known as non-persistent DOM-based XSS. Figure 1.6 shows the output of the exploit.

FIG 1.6



**Himanshu Upadhyaya**

[himanshu.upadhyay@hotmail.com](mailto:himanshu.upadhyay@hotmail.com)

Himanshu is working with HCL Technologies as a Technical Support Officer and with Maximum Hit India Pvt. Ltd as a part time Security Consultant, completed CEH from EC-Council, Initiated SARG- Security Analysis & Research Group.

## Tool GYAN



# Microsoft Baseline Security Analyzer

## Connection Manager

To begin scanning, click the “Scan a computer...” button at the bottom to specify the computer you want to scan. You can enter either the computer name or its IP address:

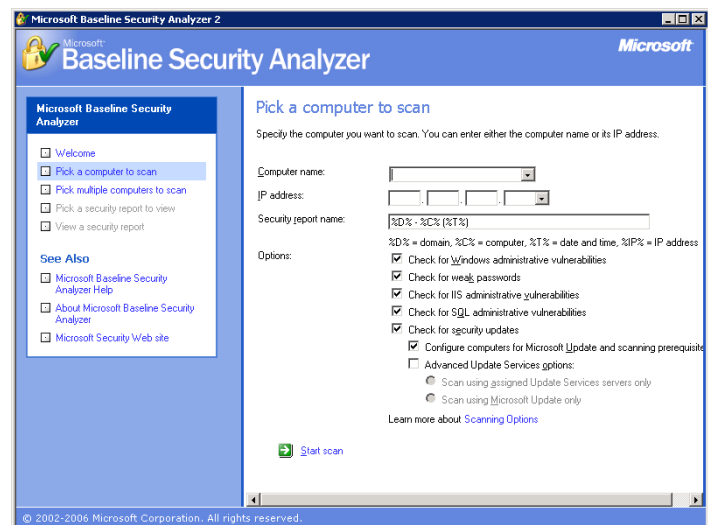
## Launching the MBSA GUI

Download Microsoft Baseline Security Analyzer from

<http://www.microsoft.com/downloads/details.aspx?FamilyID=b1e76bbe-71df-41e8-8b52-c871d012ba78&displaylang=en>

To launch the MBSA GUI, perform the following:

- **Windows** - click on the “Microsoft Baseline Security Analyzer” icon on the desktop. Alternatively, it can be found via Start -> Programs -> Microsoft Baseline Security Analyzer 2.0.1



### Security report name:

The report name can be generated using characters or hard coded names. For e.g.:

A suggested name could be *MailServer-%D% - %C% (%T%)*

where “%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address”

### The default “options” to scan are as follows:

1. Check for Windows administrative vulnerabilities
2. Check for weak passwords
3. Check for IIS administrative vulnerabilities
4. Check for SQL administrative vulnerabilities
5. Check for security updates
  - a. Configure computers for Microsoft Uppdate and scanning prerequisites
  - b. Advanced Update Services options:
    - i. Scan using assigned Update Services servers only
    - ii. Scan using Microsoft Update only

### System Requirements

This section describes the system requirements for computers running or being scanned by MBSA.

#### Requirements for Running MBSA to Scan the Local Computer

- The computer must be running Microsoft Windows Server™ 2003, Windows 2000 Service Pack 3 or later, or Windows XP.
- Internet Explorer 5.01 or later must be installed.

- An XML parser is required in order for the tool to function correctly. It is recommended that the most recent version of the MSXML parser be installed (. On Windows 2000 systems that do not have MSXML 3.0 or later installed, setup will not continue until the user installs the latest MSXML parser.
- The World Wide Web Service is required if you want to perform local IIS administrative vulnerability checks.
- Windows Update Agent 2.0 is required to scan for updates.
- The following must be enabled:
  - Workstation service
  - Server service

#### Requirements for Running MBSA to Scan Remote Computers

- The computer must be running Microsoft® Windows® Server 2003, Windows 2000 Service Pack 3 or later, or Windows XP.
- Internet Explorer 5.01 or later must be installed.
- An XML parser is required in order for the tool to function correctly. It is recommended that the most recent version of the MSXML parser be installed. On Windows 2000 systems that do not have MSXML 3.0 or later installed, setup will not continue until the user installs the latest MSXML parser.
- The IIS Common Files are required on the computer performing remote scans of IIS computers. The IIS 6.0 Common Files are required on the local computer when remotely scanning an IIS 6.0 server.
- Windows Update Agent 2.0 is required to scan for updates.

- The following must be enabled:
  - Workstation service
  - Client for Microsoft Networks.

### Requirements for a Computer to Be Scanned Remotely

- The computer must be running Windows 2000 Service Pack 3 or later, Windows XP (unless using simple file sharing), or Windows Server 2003. Itanium-based computers must be running Windows Server 2003 or Windows Server 2003 with SP1.
- Internet Explorer 5.01 or later is required for IE zone checks.
- IIS 5.0, 6.0 is required for IIS product and administrative vulnerability checks.
- Microsoft SQL Server version 7.0 or 2000 or Microsoft Data Engine or Microsoft SQL Server 2000 Desktop Engine (MSDE) is required for SQL product and administrative vulnerability checks.
- Windows Update Agent 2.0 is required to scan for updates.
- Microsoft Office System 2003, Office 2000, or Office XP is required for Office product and administrative vulnerability checks.
- Windows Installer 3.0 or later is required for Office product updates checks.
- The following must be enabled:
  - Server service
  - Remote Registry service
  - File and Print Sharing

- Distributed COM (DCOM) is required for remote security update scanning.

To run MBSA, you must be logged in with an account that has local administrative privileges on each computer being scanned either locally or remotely.

Internet access is required on the computer running MBSA in order to download an offline catalog (CAB) file from the Microsoft Web site. If a previous copy of the file was downloaded in a prior scan, the tool will attempt to use the locally cached copy if an Internet connection is not detected. The file will be downloaded and used for a scan based on the available connectivity of the target computer to the Microsoft Update site. If the target computer can utilize a connection to Microsoft Update, a more efficient scan can be used with less network utilization than the .cab file.

### Obtaining an XML Parser

XML parsers have shipped in each version of Internet Explorer since version 5.01. However, it is recommended to have the latest version of Internet Explorer and the latest version of the MSXML parser installed.

The latest version of the MSXML parser is available from the [Microsoft Web site](#).

Additional information on the Microsoft XML parser is available from the [Microsoft XML Developer Center](#).

### Scanning Options

The following checks are optional. Before scanning a computer, you can choose whether or not to run these checks.

- **Check for Windows administrative vulnerabilities**

Selecting this option scans for problems in a way that Windows is configured on the target computer. The factors include the number of members of the local Administrators group, file-system type, and whether Windows Firewall enabled are checked and reported.

- **Check for weak passwords**

Selecting this option tests the passwords of local user accounts to determine whether any are blank or have other problems that might allow them to be guessed easily.

- **Check for IIS administrative vulnerabilities**

Selecting this option checks for Internet Information Services (IIS) administrative vulnerabilities. When scanning servers running IIS, the computer running MBSA must have the Common Files installed for the highest version of IIS to be scanned. For example, to scan servers running IIS 6.0, the IIS 6.0 Common Files must be installed on the computer running MBSA.

- **Check for SQL Server administrative vulnerabilities**

Selecting this option checks for administrative vulnerabilities on each instance of Microsoft SQL Server, Microsoft Data Engine, or Microsoft SQL Server 2000 Desktop Engine (MSDE) running on the target computer.

**Note:**

Scanning SQL Server running in a cluster configuration can produce erroneous errors for Sysadmin role members, guest account, and account password tests.

- **Check for security updates**

Selecting this option checks the target computer for missing Microsoft Windows and Microsoft Office updates. When you select this option, you can also specify the following options:

- **Configure computers for Microsoft Update and scanning prerequisites**

Selecting this option installs the current version of Microsoft Update Agent on the target computer if it is absent or out of date and configures the target computer to meet other requirements for scanning for security updates.

- **Scan using Update Services servers only**

Selecting this option scans only for those security updates that are approved on the computer's Update Services server. The Microsoft Update Web site or an offline catalog is not used.

- **Scan using Microsoft Update only**

Selecting this option uses only the security update catalog downloaded from the Microsoft Update Web site to determine the updates to be checked. Updates that are not approved on the computer's Update Services server are reported as though they were approved.

## Security Checks

This section lists the security settings that Microsoft Baseline Security Analyzer version 2.0.1 checks during a full scan. Note that if a product is not installed on a computer being scanned, the corresponding product checks will not be performed and will not be reflected in the MBSA scan reports.

### ▪ Security update checks

Scanning computers for security updates utilizes Windows Server Update Services. MBSA provides integration for Update Services administrators and is a comprehensive standalone tool for the information technology professional.

### ▪ Windows checks

Check for account password expiration:  
Check for file system type on hard drives  
Check if Auto Logon feature is enabled  
Check if Guest account is enabled  
Check the Restrict Anonymous registry key settings

Check the number of local Administrator accounts

Check for blank or simple local user account passwords

Check if unnecessary services are running  
List the shares present on the computer  
Check if Windows auditing is enabled  
Check the Windows version running on the scanned computer

Check if Internet Connection Firewall is enabled

Check if Automatic Updates is enabled  
Check if incomplete updates require the computer to be restarted

### ▪ IIS checks

Check if the IIS Lockdown tool (version 2.1) was run on the computer  
Check if IIS sample applications are installed

Check if IIS parent paths are enabled  
Check if the IIS Admin virtual folder is installed

Check if the MSADC and Scripts virtual directories are installed

Check if IIS logging is enabled  
Check if IIS is running on a domain controller

### ▪ SQL Server checks

Check if Administrators group belongs in Sysadmin role

Check if CmdExec role is restricted to Sysadmin only

Check if SQL Server is running on a domain controller

Check if sa account password is exposed  
Check SQL Server installation folders access permissions

Check if Guest account has database access  
Check if Everyone group has access to SQL Server registry keys

Check if SQL Server service accounts are members of the local Administrators group

Check if SQL Server accounts have blank or simple passwords

Check the SQL Server authentication mode type

Check the number of Sysadmin role members

### ▪ Desktop application checks

List the Internet Explorer security zone settings for each local user

Check if Internet Explorer Enhanced Security Configuration is enabled for Administrators

Check if Internet Explorer Enhanced Security Configuration is enabled for non-Administrators

List the Office products security zone settings for each local user

### Command-Line Tool

Instead of the MBSA graphical user interface (GUI) tool, you can use the MBSA command-line tool to perform local and remote security scans and to display reports from previous scans. The tool is located in the directory where MBSA 2.0.1 was installed (by default, %programfiles%\Microsoft Baseline Security Analyzer 2).

## Syntax

To perform a full scan of one or more computers:

```
MBSACLI [/target {[domain\]computer |
IP} | /r IP-IP | /d domain] [/n
option[+option...]]
[/o template] [/qp] [/qr] [/qe] [/qt]
[/q] [/listfile file] [/wa | /wi]
[/catalog file] [/nvc] [/nai] [/nm]
[/nd] [/u username /p password]
```

To scan the local computer for updates only, sending the results to standard output (STDOUT) in XML:

```
MBSACLI [/xmlout] [/unicode] [/wa |
/wi] [/nd] [/catalog file]
```

To scan one or more computers for updates only, creating reports that can be displayed by MBSA:

```
MBSACLI [/target {[domain]\computer |
IP} | /r IP-IP | /d domain]
[/n OS+IIS+SQL+Password]
[/o template] [/qp] [/qr] [/qe]
[/qt]
[/q] [/unicode] [/listfile file]
[/wa | /wi] [/catalog file] [/nvc]
[/nai] [/nm] [/nd] [/u username /p
password]
```

To display a report:

```
MBSACLI [/l] [/ls] [/lr report] [/ld
report] [/nvc]
```

To display usage information:

```
MBSACLI [/?]
```

## Parameters

You cannot use any of these parameters more than once each time you run the command.

**/target** [domain\]computer | IP

Scans the specified computer. You can identify the computer by using its IP address or its name and, optionally, the domain to which it belongs.

**/r IP-IP**

Scans all the computers that are identified by a range of IP addresses.

**/d domain**

Scans all the computers in the specified domain.

**/n option[+option...]**

Excludes the specified scan types from the scan. You can specify the following options, separating them with a plus sign (+):

### OS

Excludes Windows administrative vulnerability checks

### SQL

Excludes SQL Server administrative vulnerability checks

### IIS

Excludes IIS administrative vulnerability checks

### Password

Excludes password vulnerability checks

**/o template**

Specifies the template that MBSA uses when naming the XML output file. You can use these symbols to represent computer-specific information:

%d%

Replaced with the name of the computer's domain

%c%

Replaced with the name of the computer

%t%

Replaced with the date and time when the scan was performed

**%IP%**

Replaced with the computer's IP address  
The default file-name template is %d -  
:%c% (%t%).

You can also use the variable names that were supported by previous versions of MBSA: %domain%, %computer name%, and %date%.

**/qp**

Does not display scan progress.

**/qr**

Does not display the report list.

**/qe**

Does not display the error list.

**/qt**

Does not display the text output after scanning a single computer.

**/q**

Does not display scan progress, the report list, the error list, or text output.

**/listfile file**

Scans the computers identified in a file. The *file* argument is the path and name of a text file in ASCII or Unicode format that contains one or more IP addresses or computer names. Each IP address or computer name must appear on a separate line.

**/xmlout**

Checks the local computer for security updates only, displaying the results as XML text. To save the report in a file, use command redirection to redirect standard output (STDOUT) to a file, for example, **mbsacli /xmlout > output.xml**.

For more information about using this parameter, see **Security Updates Scan** Help file from install location.

**/wa**

Scans only for security updates that are approved on the computer's Update Services server. The Microsoft Update web site and the offline catalog are not used. This parameter cannot be used with the **/wi** parameter.

**/wi**

Uses only the Microsoft Update web site or offline catalog for security update information. Updates that are not approved on the computer's Update Services server are displayed as though they were approved. This parameter cannot be used with **/wa** parameter. Use this parameter to scan computers whose assigned Update Services servers are not available.

**/catalog file**

Specifies the offline catalog containing the security update information to be used when scanning. The offline catalog must be a .cab file signed by Microsoft. The default offline catalog is Wsusscan.cab, which is downloaded from the Microsoft Web site. When this parameter is not used, Wsusscan.cab is downloaded from the Microsoft Web site if it is different from the locally cached version. Using this parameter prevents a newer file from being downloaded, and so should be used with care. The *file* argument must specify a file located on the computer performing the scan.

**/nvc**

Prevents MBSA from checking for a newer version of MBSA.

**/nai**

Prevents MBSA from installing or updating the Windows Update Agent on the computer being scanned. When this parameter is used, computers that do not have the required version of Automatic Updates will return an error

in the report, and computers that do not have Windows Installer 3.0 or later may receive incomplete results from Microsoft Office and other products that require Windows Installer 3.0 for scanning.

**/nm**

Scans computers by using an offline catalog instead of the Windows Update site. Depending on the size of the offline catalog and network load, using this parameter may cause MBSA to take more time to or more network bandwidth.

**/nd**

Do not download any files from the Microsoft Web site when scanning. Use this parameter to prevent the download of Wsuscan.cab, Muauth.cab, WindowsUpdateAgent20-x86.exe and WindowsUpdateAgent20-x64.exe during the scanning process. When this parameter is selected, MBSA will use any previously downloaded copies of the files. If you want, you can download the files yourself and place them in C:\Documents and Settings\username\Local Settings\Application Data\Microsoft\MBSA\2.0\Cache. This parameter applies only to downloads from the Microsoft Web site to the scanning computer. Downloads from the scanning computer to the target computer are automatic and cannot be disabled if the corresponding features are used.

**/u username /p password**

Specifies the user name and password to be used when scanning a remote computer. The **/u** and **/p** parameters must be used together and cannot be used when scanning the local computer. The specified user must have

administrative privileges on the computer being scanned. For security purposes, the password is not sent over the network in clear text. Instead, MBSA uses the Windows challenge-response mechanism to secure the authentication process.

**/l**

Lists all available reports.

**/ls**

Lists reports from the most recent scan.

**/lr report**

Displays an overview of the specified report.

**/ld report**

Displays the details of the specified report. When scanning a single computer, this is the default behavior unless the **/qt** parameter is used.

**/unicode**

Produces the report with Unicode characters. Users running Japanese MBSA or scanning computers running Japanese Windows should specify this parameter.

**/?**

Displays usage information for the command-line tool.

**Selecting a computer to scan**

Use the following parameters to specify the computer to be scanned. If you do not specify one of these parameters on the command line, MBSA scans the local computer, that is, the computer on which it is running.

**/target [domain\]computer**

Scans the named computer. The domain or workgroup name is optional.

**/target nnn.nnn.nnn.nnn**

Scans the computer identified by the specified IP address.

**/r nnn.nnn.nnn.nnn-*nnn.nnn.nnn.nnn***

Scans the computers identified by a range of IP addresses.

**/listfile filename**

Scans each computer identified by name or IP address listed in the specified file. Place each computer name or IP address on a separate line in either an ASCII or UNICODE format text file.

**/d domain**

Scans all computers in the specified domain.

**Excluding specific checks**

To exclude a specific check from scan, use the **/n** parameter with the keyword for that check. The following are the keywords you can use with the **/n** parameter.

**/n IIS**

Skips IIS checks

**/n OS**

Skips Windows Operating System (OS) checks. This also skips the Internet Explorer and Outlook zone checks and the Office macro security checks.

**/n Password**

Skips password checks.

**/n SQL**

Skips SQL Server/MSDE checks.

**/n Updates**

Skips security update checks.

**Specifying parameters for security update checks**

The following parameters determine how a security update check is performed and reported.

**/wa**

Scans only using an assigned Update Services server. Unapproved updates are not listed. This parameter checks for security updates using only the computer's assigned Update Services server. MBSA will not utilize the Microsoft Update site or the offline catalog when scanning. This parameter cannot be use with the **/wi** parameter. If

a scanned computer does not have an Update Services server assigned, the scan will return an error. Unapproved updates are displayed as an informational result.

**/wi**

Scans only using Microsoft Update. Updates that are not approved on the target computer's assigned Update Services server are shown as though they were approved. This parameter checks for security updates using only the Microsoft Update site or the offline catalog. It does not use the target computer's assigned Update Services server when scanning. This parameter cannot be used with the **/wa** parameter. Default is to show unapproved updates as an informational result.

**/xmlout**

Checks the local computer for security updates only, displaying the results as XML text.

**/catalog file**

Specifies the offline catalog containing the security update information to be used when scanning. The offline catalog must be a .cab file signed by Microsoft. The default offline catalog is Wsusscan.cab, which is downloaded from the Microsoft Web site. When this parameter is not used, Wsusscan.cab is downloaded from the Microsoft Web site if it is different from the locally cached version. Using this parameter prevents a newer file from being downloaded, and so should be used with care.

**/nai**

Prevents MBSA from installing or updating the Windows Update Agent on the computer being scanned. When this parameter is used, computers that do

not have the required version Automatic Updates will return an error in the report, and computers that do not have Windows Installer 3.0 or later may receive incomplete results from Microsoft Office and other products that require Windows Installer 3.0 for scanning.

#### **/nm**

Scans computers by using an offline catalog instead of the Windows Update site. Depending on the size of the offline catalog and network load, using this parameter may cause MBSA to take more time to or more network bandwidth.

#### **Scanning only for security updates**

Using **/xmlout** specifies that MBSA only checks for security updates and displays scan results as XML text in the command line window. Only the MBSA engine (Mbsacli.exe and Wusscan.dll) files are needed for this type of scanning, and only the parameters listed below can be used with this parameter:

- **/catalog**
- **/wa**
- **/wi**
- **/nvc**
- **/nd**
- **/unicode**

When using the **/xmlout** parameter, you must explicitly redirect the XML output into a file using standard console redirection. Also, the XML results must be processed separately from MBSA because they observe a different format than the full MBSA report files. The benefit of this parameter is to avoid the full installation package of MBSA 2.0.1 while checking for updates on a single computer. If the minimum system requirements are met, only the engine files are needed and can be easily copied from

another computer having a full installation present.

#### **Displaying results and details**

You can use the MBSA command-line interface to list or display reports produced by previous scans. These report parameters cannot be combined with scanning parameters.

#### **/l**

Lists all the reports that are available.

#### **/ls**

Lists the reports from most recent scan.

#### **/lr report**

Displays an overview of the named report.

#### **/ld report**

Displays details of the named report. Unless the **/qt** parameter is used, this is the default behavior whenever MBSA scans a single computer.

## **General Notes**

### **Scan Reports**

Scan reports are stored on the computer on which MBSA is installed, in the SecurityScans folder of the user's profile (%userprofile%\SecurityScans). MBSA creates an individual security report for each computer that it scans, either locally or remotely. Report files are named with the file extension .mbsa, which is a registered file association for MBSA, so that clicking on the file in Windows Explorer will start MBSA to view the report.

### **Security Updates Scan**

When you perform a security update scan, all security-related updates are checked and reported. If a target computer has a registered Update Services server, the report will indicate which updates have not been approved on the Update Services server using an informational score. When you

select the **Scan using Update Services servers only** check box or use the `/wa` parameter on the command line, only security updates marked as approved by the Update Services administrator are checked and reported by MBSA.

In addition, updates that are installed and not yet superseded by another update will be included in the Current Update Compliance section of the report. When an update has been superseded by another update and both are installed, the report will only reflect the more recent update and not both. When available during update publication, related IDs will be included in the report as they have been listed in the Technical Details section of the security bulletin.

Security update checks are not performed for products that are not installed on a scanned computer, and these checks are not listed in the Security Update Scan Results table in the report.

For more information, see [Scanning Options](#); you can also access this topic while running MBSA.

### Partially Installed Updates

For updates installed by using Windows Update, Microsoft Update, or Automatic Updates that required a restart of the computer that was postponed by the user, the report will indicate that the update is not installed because the required reboot has not occurred. In this case, restarting the computer and scanning again will cause the update to report the proper installation status.

For updates that were installed by directly downloading or running the update, but for which a required system restart was postponed, MBSA will provide an indication of the pending restart under the Windows Check named Incomplete Updates. This capability is available only for those updates

that were built using the standard installer (update.exe) with a minimum version of 6.1.22.0.

### Localized Versions

MBSA 2.0.1 has console localization support for Japanese, German, and French, but has the ability to scan localized OS versions of the target computers independently of the console language. This is because all languages supported by Microsoft Update can be scanned equally, but the results are stored in the language of the MBSA console installation.

The following examples illustrate scenarios that may be encountered when using different languages of the operating system and of the MBSA console:

- A Japanese system with the Japanese version of MBSA installed that scans a Japanese system: results of scanning a Japanese target computer are shown in Japanese.
- A French system with the Japanese version of MBSA installed that scans a French system: Results are shown in Japanese due to the Japanese version of MBSA installed.

### Remote (Network) Scans

MBSA can be used to scan a domain or a range of IP addresses from a central computer given the system requirements listed earlier in this topic. When performing remote scans, you must run MBSA while logged on with an account that has local administrative privileges on each computer being scanned. When using the MBSA command-line tool to perform scans, you can either run the tool while logged on with an account with local administrative privileges on each computer, or you can use the `/u` and `/p` parameters to supply the user name and password of such an account. In a multidomain environment where a firewall

or filtering router separates the two networks (two separate Active Directory® domains), TCP ports 139 and 445 and UDP ports 137 and 138 must be open in order for MBSA to connect and authenticate to the remote servers being scanned.

### Error Reporting

Microsoft Baseline Security Analyzer displays an error if any of the following occurs:

- A user attempts to scan the computer but is not a local administrator on the computer being scanned.
- A computer being scanned does not respond to an initial connection attempt from the computer on which the tool is running. This may be the result of an invalid host name or IP address, or it may be a network connectivity issue.
- A remote computer being scanned does not have the proper services enabled.
- IIS Common Files are not installed on the computer running MBSA when performing a remote scan of an IIS server.
- The computer running MBSA does not have Internet access to download the .cab file required to perform the security update check during a scan. If a previous copy of the .cab file was downloaded in a prior scan, the tool will attempt to use this locally cached copy if an Internet connection is not detected.

### Security Implications of Remote Scanning

If you use MBSA to scan remote computers, you should be aware of two aspects that might affect your network's security.

### Updating Windows Update Agent on Target Computers

When scanning a target computer for security updates, MBSA relies on Windows Update Agent (WUA) running on the target computer. If the target computer does not have the current version of WUA installed, MBSA by default installs the required version of WUA. If you are a network administrator and are concerned that a hostile user on the Local Area Network (LAN) might be able to intercept the WUA installation files and corrupt them or substitute malware (such as a Trojan horse program) for the installation files while they are being transmitted to the target computers, you can prevent this default behavior. (An MBSA user who is not a network administrator, such as a user scanning only the local computer, need not be concerned about this risk.) When using the Windows-based MBSA application, clear the **Configure computers for Microsoft Update and scanning prerequisites** check box before performing a security update scan. When using the MBSA command-line tool, specify the `/nm` and `/nai` options on the command line.

If you prevent MBSA from installing or updating WUA on target computers, you can use one of several methods to ensure that the current version of WUA is installed on each target computer:

- Rely on Windows Server Update Services to install WUA on the target computer
- Register the target computer with the Microsoft Update Web site
- Manually install WUA on each target computer
- Deploy WUA within a system image

The following sections describe each of these methods in greater detail. In addition to these methods, you can deploy WUA

using a software distribution product, such as SMS or a third-party solution.

#### Important

- When MBSA updates WUA on a target computer, it downloads and executes two files in addition to the WUA files: Mbsa2ri.exe and Mbsa2mu.exe. If you choose to allow MBSA to automatically update WUA on target computers, and if you are concerned that these files or the WUA files could be tampered with in transit, you should consider using a secure network protocol such as IPsec to secure the network transmission. See the [Microsoft web site](#) for information about IPsec.

### Using Windows Server Update Services

Windows Server Update Services (Update Services) enables network administrators to deploy the latest Microsoft product updates to Microsoft Windows Server 2000, Windows Server 2003, and Windows XP operating systems. By using Update Services, you can fully manage the distribution of updates that are released through Microsoft Update to computers in your network. Computers that are assigned to an Update Services server automatically receive the current version of WUA, enabling them to be scanned by MBSA. To learn more about Update Services, see the [Microsoft Web site](#).

### Using the Microsoft Update Web Site

You can configure target computers to obtain the current version of WUA directly from Microsoft Update and to configure the target computer to use Microsoft Update when being scanned. To do so, log on each target computer as an administrator,

connect to the [Microsoft Update Web site](#) and follow the instructions provided there.

### Manually Installing WUA

If you want to maintain maximum control over how WUA is installed or updated on target computers, you can manually install WUA on each target computer. Doing so requires that you execute the appropriate WUA installation program on each target computer, either by logging on interactively and then running the installation program, or using a software distribution system such as Microsoft Systems Management Server. You can obtain the necessary WUA installation programs from the Microsoft Web site:

- For x86-based computers: [WindowsUpdateAgent20-x86.exe](#)
- For x64-based computers: [WindowsUpdateAgent20-x64.exe](#)
- For Itanium-based computers: [WindowsUpdateAgent20-ia64.exe](#)

### Deploying WUA Within a System Image

If you are configuring new computers that are being built from a disk image, you can install WUA on the master computer, register the master computer with Microsoft Update, or both, before creating the master image. Be sure you are familiar with how to prepare a Windows system image. For more information, see the [Microsoft Web site](#).

### MBSA and Administrator Accounts

Scanning with MBSA requires you to run MBSA with an account that is an administrator on all scanned computers. Depending upon how your network has been secured, this can introduce significant risk should the user-account be compromised, but it is necessary to be able to scan for certain vulnerabilities. If this risk is acceptable, you should take steps to

mitigate this risk. For example, making this account a member of the Domain Admins group requires less administrative overhead because the account automatically has the required rights on all potential clients, but if the account is compromised, the risk to the enterprise is severe. You should consider creating a special account for this purpose and enabling the account only when it is needed to scan domain computers. Making the account a local administrator on each target computer but not a member of the Domain Admins group requires you to manage this account on every target computer, but the risk of compromise is limited to the target computers themselves, not to the domain as a whole. You can further mitigate the threat by using only Kerberos authentication, which is less vulnerable to attacks than LanMan authentication, but doing so might require an upgrade to Active Directory.



**Prasanna Aiyar**  
[prasanna.aiyar@gmail.com](mailto:prasanna.aiyar@gmail.com)

Prasanna is an Information Security professional since past 5 years. She works as an Identity and Access management professional for Accenture. Prasanna is a Sun Certified Integrator for Identity Manager 7.1. Her experience includes working with Sun Identity Manager, Oracle Identity Manager, Sun Directory Server, risk assessment, auditing, vulnerability scanners and creating reports for vulnerabilities and suggested patches.

The logo for Belarc Advisor features a red curved line above the word "BELARC" in blue, followed by the word "Advisor" in a larger blue font.

# BELARC Advisor

## To know your system details with the Belarc Advisor

---

Belarc Advisor can be very useful for home pc users and getting the computer info in just one click. It is a freeware application for diagnosing PC problems, it analyze your machine elements such as anti-virus, security flaws in Windows have been patched or not then it will give the your computer score showing its overall security level and produces a html report which can be viewed in the web browser.

### Introduction

If you are using a computer system, it is really important to see what's running on your PC. Your personal work on PC makes it important to monitor your system along with safety and security. There are multiple ways to see what's running on your PC. But in this article I am going to tell you how you will check your computer system in details with Belarc Advisor.

Belarc Advisor is a free utility and easy to download.

Download from

<http://www.belarc.com/Programs/advisor.exe>

### System Requirements

**Operating Systems:** Runs on Windows 7, 2008 R2, Vista, 2008, 2003, XP, 2000, NT 4, Me, 98, and 95. Both 32-bit and 64-bit Windows is supported.

**Browsers:** Runs on Internet Explorer, Firefox, Safari, Opera, and many others.

**Hard Disk space:** 2.2 MB.

**License:** Freeware

### What does Belarc Advisor do?

It records essential information such as operating system and processor details, the amount of RAM installed, and drive specifications. It also includes detailed list of the software installed on your system as well as software license numbers and product keys. It even lists Microsoft hot fixes and lets you know if any of these require reinstalling.

After this process Belarc Advisor generates the report, it is displayed in your browser (means it creates html file on your local drive). The report is clearly formatted for easy understanding and is divided into different categories.

That report also shows you the status of your anti-virus software, if you've missed any of the "hot fixes" from Microsoft, and lots of more details.

Let's see how it looks like.

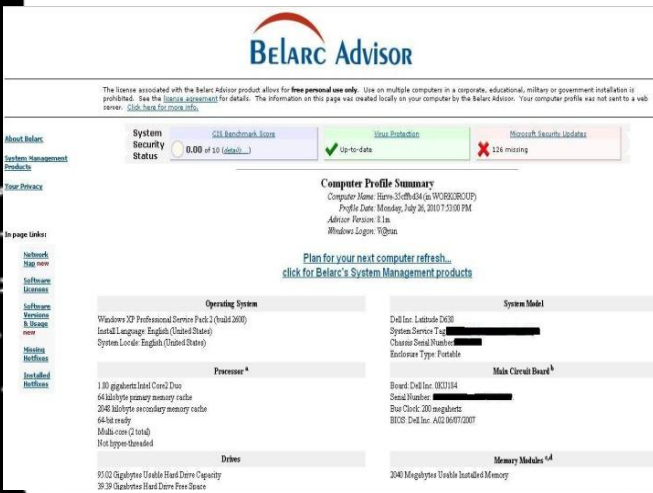


Figure 1

Fig 1. Shows you Security details report of my computer.

In Security details it will show you your Operating system details along with that it will also show your system Processor, Main board, memory modules, Hard drive in detail.

Like this we can also check list of software that is installed on your computer.

[Manage all your software licenses...](#)  
[click for Belarc's System Management products](#)

Software Licenses <a href="#">[Back to Top]</a>	
Ahead - Nero - Burning Rom	████████████████████
Ahead - Nero Fast CD-Burning Plugin	████████████████████
AVG - IDS	████████████████████
Belarc - Advisor	████████████████████
Dell Computer - SysInfo	████████████████████
Microsoft - Internet Explorer	████████████████████
Microsoft - Office Enterprise 2007	████████████████████
Microsoft - WebFides XP	████████████████████
Microsoft - Windows XP Professional	████████████████████

[Find unused software and reduce licensing costs...](#)  
[click for Belarc's System Management products](#)

new Software Versions & Usage (mouse over i for details, click i for location) <a href="#">[Back to Top]</a>	
i 2007 Microsoft Office system Version 12.0.4518.1014	i Key! - MPUI: a Windows frontend for MPlayer Version 1.1
i Adobe Systems, Inc. - Shockwave Flash Version 10,0,45,2	i Microsoft (g) Windows Script Host Version 5.6.0.8820
i Ahead Software AG - Nero BackItUp Restore Version 1, 2, 0, 61	i Microsoft Clip Organizer Version 12.0.4518.1014
i Ahead Software AG - Nero BackItUp Scheduler Version 1, 2, 0, 61	i Microsoft Corporation - Groove Audit Service Version 4.2.0.2623
i Ahead Software AG - Nero BackItUp Version 1, 2, 0, 61	i Microsoft Corporation - Internet Explorer Version 7.00.5730.13
i Ahead Software AG - Nero Burning ROM Version 6, 6, 0, 19	i Microsoft Corporation - Messenger Version 4.7.3000
i Ahead Software AG - Nero StartSmart Version 2, 0, 0, 29	i Microsoft Corporation - Office Diagnostics Service Version 12.0.4518.1014
i Alexander Roshal - WinRAR archiver Version 3.70.0.0	i Microsoft Corporation - Office Diagnostics Service Version 12.0.4518.1014
i Alps Pointing-Device Driver Version 7.0.101.199	i Microsoft Corporation - Office Source Engine Version 12.0.4518.1014
i Apache HTTP Server Version 2.2.11	i Microsoft Corporation - Windows Installer - Unscd Version 3.0.3790.2180
i arkAdmin - Vista Drive Icon Version 1.04.01.49	i Microsoft Corporation - Windows Movie Maker Version 2.1.4026.0
i AR2 CmH - FakeFolder Version 0.03	i Microsoft Corporation - Windows@ NetMeeting@ Version 3.01
i Avquest Software - Digital Line Detection Version 1, 0, 0, 2	i Microsoft Corporation - Zone.com Version 1.2.626.1
i AVG IDS Version 9.0.0.994	i Microsoft Data Access Components Version 3.525.1117.0
i AVG Internet Security Version 9.0.0.832	i Microsoft Office Groove Version 4.2.0.2623
i Belarc, Inc. - A-Advisor Version 8.1m	i Microsoft Office InfoPath Version 12.0.4518.1014
i BitTorrent, Inc. - µTorrent Version 1.8.2.141.53	i Microsoft Office OneNote Version 12.0.4518.1014
i Bluetooth Stack for Windows by TOSHIBA Version 1.0.0.0	i Microsoft Office Outlook Version 12.0.4518.1014
i Bluetooth Stack for Windows by TOSHIBA Version 4.0.0.0	i Microsoft Office Picture Manager Version 12.0.4518.1014

Figure 2

In Fig 2 you can see list of software installed on your computer.

The results are really detailed and give you important information about your PC and all the software that runs on it.

Once Belarc Advisor installed, then it can generate new reports as required, so you can easily update your profile if your system specifications change.

You can access Belarc's website and receive guidance on hot fixes, which are currently available for the computer under analysis. Belarc Advisor free license is only for personal use, and should not be engaged in corporate usage.

**Varun Hirve**  
varun@chmag.in



**LegalGYAN****open source**

## Open Source Licenses

---

The Open Source Initiative (OSI) is a California (USA) based not for profit organization that spearheads the open source movement around the world.

To qualify as “open source”, particular software must comply with several conditions. In order to understand these conditions, let us take a fictional illustration. Sanya has developed easyPDF - software for converting documents into PDF (portable document format). Sanya wants to release easyPDF as open source software. EasyPDF must comply with the following conditions:

### 1. Free Redistribution

The easyPDF license **cannot restrict** anyone from **selling** or **giving away** the easyPDF software as a component of an aggregate software distribution.

#### Illustration 1

Sameer advises small companies on using technology to streamline their business processes. He also sells software (including easyPDF) to such companies. Sanya cannot stop Sameer from selling easyPDF

#### Illustration 2

Siddharth uses easyPDF along with some code developed by him to create easyWord, word processing software. Sanya cannot stop Sameer from using the easyPDF software as part of easyWord.

The easyPDF license **cannot provide for royalty** or other fee for such sale or distribution.

### Illustration 3

In the previous illustrations, Sanya cannot charge Sameer or Siddharth any royalty or fee for selling or using easyPDF.

## 2. Source Code

The easyPDF software program must

1. include source code, and
2. Allow distribution in source code as well as compiled form.

### Illustration 1

easyPDF is not distributed with the source code. However, when easyPDF is started up by a user, a message is flashed on the user's screen. This message contains details of the website from where the easyPDF source code can be downloaded for free. This is acceptable.

### Illustration 2

easyPDF is not distributed with the source code. However, a CD containing the easyPDF source code can be obtained by sending the cost of postage and the cost of a blank CD to Sanya. This is acceptable

The easyPDF source code must not be deliberately obfuscated. Obfuscated code (also called shrouded code) is source code that is very difficult to read and understand. Programs known as obfuscators can make source code very difficult to read and understand.

Let us take a **simple illustration of obfuscated code**. The following basic code can be put in a webpage:

```
<a href="http://www.sanyanagpal.com">Click here to visit Sanya Nagpal's website</a>
```

The webpage will display a link to sanyanagpal.com and will look something like this:

```
Click here to visit Sanya Nagpal's website
```

The obfuscated code will look like the illustration below:

```
<script language=JavaScript>m='%3Ca%20href%3D%22http%3A//www.sanyanagpal.com%22%3EClick%20here%20to%20visit%20Sanya%20Nagpal%27s%20website%3C/a%3E';d=unescape(m);document.write(d);</script>
```

## 3. Derived works

The easyPDF license must allow modifications and derived works. The license must also allow the modified or derived works to be distributed under the same terms as the easyPDF license.

## 4. Integrity of the author's source code

The easyPDF license can restrict the source-code from being distributed in modified form under some conditions that are illustrated below.

### Illustration 1

The easyPDF license allows others to include “patch files” along with the original easyPDF source code. The “patch files” can modify the easyPDF

program at the time when it is compiled.

#### **Illustration 2**

The easyPDF license can state that the derived works must have a different name.

#### **Illustration 3**

Sanya has release easyPDF version 1. The license can state that the derived software must have a different version number.

### **5. No Discrimination against Persons or Groups**

The license must not discriminate against any person or group of persons.

#### **Illustration**

The easyPDF license cannot state that Pakistani citizens cannot use the program.

### **6. No Discrimination against Fields of Endeavor**

The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

#### **Illustration**

The easyPDF license cannot state that it cannot be used in commercial organizations or banks etc.

### **7. Distribution of License**

The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

#### **Illustration**

Sanya is distributing the easyPDF software from her website. Sameer copies the easyPDF source code and program and distributes it from his website. Pooja downloads easyPDF from Sameer's website. The rights attached to easyPDF now automatically lie with Pooja also.

### **8. License Must Not Be Specific to a Product**

The rights attached to the program must not depend on the program being part of a particular software distribution.

#### **Illustration**

Sanya is distributing the easyPDF software along with a group of other software that she has developed. Collectively this group is called the easySuite and distributed by Sanya as open source.

Sameer extracts the easyPDF program from easySuite. He then distributes easyPDF to Pooja.

Pooja will have the same rights as those granted by easySuite.

### **9. License Must Not Restrict Other Software**

The easyPDF license must not place restrictions on other software that are distributed along with it.

#### **Illustration**

The easyPDF license cannot state that all programs distributed on the same CD must be open source software.

## 10. License Must Be Technology-Neutral

No provision of the license may be predicated on any individual technology or style of interface.

### Illustration:

The easyPDF license cannot be a click-wrap license i.e. it cannot ask users to click on an “I Accept” button.

This is because "click-wrap" agreements are not possible in many cases such as FTP download or where the source code is run in a command line / non-GUI (Graphical User Interface) based environment.

## GNU General Public License

Many popular software programs come with a license similar to the one illustrated below:

This file is part of the easyPDF Software Suite.

easyPDF Software Suite is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License version 3 or any later version as published by the Free Software Foundation.

easyPDF Software Suite is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with easyPDF Software Suite.

If not, see <<http://www.gnu.org/licenses/>>

GNU General Public License (GNU GPL) is one of the most popular licenses in contemporary software.

### Essential features of GNU GPL version 3 are:

1. It is a **copy left** license for software and other kinds of works.

**Copy left** is a general method for making a program or other work free, and requiring all modified and extended versions of the program to be free as well.

Copy left mandates that anyone who redistributes the software, with or without changes, must pass along the freedom to further copy and change it.

Usually, to copy left a program, the programmer first states that the software is copyrighted. Then he adds distribution terms and conditions which are a legal instrument. These terms give everyone the rights to use, modify, and redistribute the program's code or derivatives only if the distribution terms are unchanged.

Copy left is thus the opposite of copyright. Copyright takes away a users freedom while copy left guarantees the freedom.

2. GNU GPL guarantees the **freedom to share and change** all versions of a program. This ensures that the software remains free software for all its users.

GNU GPL covers **free software**. This does not imply that there can be no money

charged for the software. It refers to **freedom to do the following:**

- a. to distribute copies of the software
  - b. to run the software for any purpose
  - c. to sell copies of the software
  - d. to access the source code
  - e. to modify the source code
  - f. to study how the software runs
  - g. to change and adapt the software
  - h. to use parts of the software for new free programs
3. The GNU GPL prohibits the registration of **patents** that can make the software “non-free”.

The following illustrations will clarify some of the conditions of the GNU GPL. The illustrations are based on a fictional situation where Sanya has developed easyPDF - software for converting documents into PDF (portable document format). The easyPDF software and its source code have been released under GNU GPL. Sanya holds the copyright over the source code as well as the software.

#### Illustration 1

Sanya can **sell** the easyPDF software and / or source code for any price that she deems suitable.

#### Illustration 2

Sanya can charge a **fee for downloading** the easyPDF software and / or source code from her website.

#### Illustration 3

Sameer pays a fee and downloads the easyPDF software from Sanya’s website. Sameer can now distribute

the software for free from his website, on CDs etc.

Pooja gets the software free from Sameer’s website. Pooja is not required to inform Sanya about receiving the software. She is also not required to pay Sanya any fees.

#### Illustration 4

Sanya cannot ask Sameer to enter into a non-disclosure agreement in respect of the easyPDF software / source code.

#### Illustration 5

Sameer modifies the easyPDF source code. Sameer cannot ask Pooja to enter into a non-disclosure agreement in respect of the modified easyPDF software / source code.

#### Illustration 6

Noodle Ltd has requested Sanya to make some modifications to the easyPDF source code. Noodle Ltd and Sanya can enter into a non-disclosure agreement whereby Sanya cannot disclose these modifications till Noodle approves them.

Noodle can insist that Sanya cannot release the modified software / source code to anyone else without their permission.

Noodle has the right to distribute the software / source code to others without Sanya’s permission.

#### Illustration 7

Sanya can write a copyright notice in her own name in the license. E.g. the easyPDF source code files can have the following notice: *Copyright © 2008 Sanya Nagpal.*

**Illustration 8**

Sanya can simultaneously release the easyPDF source code / software under the GNU GPL as well as under a commercial license.

**Illustration 9**

Sameer wants to use the easyPDF source code along with the easyBook source code (created by Pooja) and combine them to create a new software program.

If the licenses of easyPDF and easyBook allow the source codes to be combined then the two licenses are said to be **compatible**. If not, the licenses are **incompatible**.

Some licenses may allow linking of the codes but not merging their code into one module.

The licenses of two programs need not be compatible in case the programs are simply required to be installed in the same computer.

**Illustration 10**

Sanya cannot license the easyPDF software / source code to Sameer for exclusive use. The GNU GPL license cannot be revoked.

**Illustration 11**

Sanya cannot force users of easyPDF software / source code to make their PDF documents open source. She has no rights over the documents created by others using easyPDF.

However, if the easyPDF program copies part of itself onto the output, then the output would also come under GNU GPL.



**Rohas Nagpal**  
[rn@asianlaws.org](mailto:rn@asianlaws.org)

# Command LINE

```

netsh>?
The following commands are available:
Commands in this context:
? - Goes up one context level.
? - Displays a list of commands.
abort - Discards changes made while in offline mode.
add - Adds a configuration entry to a list of entries.
alias - Adds an alias.
bridge - Changes to the 'netsh bridge' context.
bye - Exits the program.
commit - Commits changes made while in offline mode.
delete - Deletes a configuration entry from a list of entries.
diag - Changes to the 'netsh diag' context.
dump - Displays a configuration script.
exec - Runs a script file.
exit - Exits the program.
firewall - Changes to the 'netsh firewall' context.
help - Displays a list of commands.
interface - Changes to the 'netsh interface' context.
lan - Changes to the 'netsh lan' context.
nap - Changes to the 'netsh nap' context.
offline - Sets the current mode to offline.
online - Sets the current mode to online.
popd - Pops a context from the stack.
pushd - Pushes current context on stack.
quit - Exits the program.
ras - Changes to the 'netsh ras' context.
routing - Changes to the 'netsh routing' context.
set - Updates configuration settings.
show - Displays information.
unalias - Deletes an alias.
winsock - Changes to the 'netsh winsock' context.

The following sub-contexts are available:
bridge diag firewall interface lan nap ras routing winsock

To view help for a command, type the command, followed by a space, and then
type ?.
netsh>

```

## Playing with network config

Oh! By the way we have discussed a lot on Command Line Gyan about advance stuff but are we comfortable with basic settings which we might use daily?

In this issue of command line gyan, let's play around with IP address configurations

### Windows

On a windows box netsh is most powerful utility I have seen. It's inbuilt in Windows so you don't have to install something for it. command

```
C:\> netsh
```

```
netsh>?
```

If you remember we used netsh in last issue where we touched upon firewalls and while writing that article I thought of writing about netsh in depth sometime. To play more with any option just type the option followed by a '?'

```
netsh> interface
```

```
netsh interface> ?
```

Commands in this context:

```

? - Displays a list of commands.
add - Adds a configuration entry to a table.
delete - Deletes a configuration entry from a table.
dump - Displays a configuration script.
help - Displays a list of commands.
ip - Changes to the 'netsh interface ip' context.
ipv6 - Changes to the 'netsh interface ipv6' context.
portproxy - Changes to the 'netsh interface portproxy' context.
reset - Resets information.
set - Sets configuration information.
show - Displays information.

```

Let's see how we can now use netsh to set an IP address of an interface

```
netsh interface ip> set address ?
Usage: set address [name=] [[source=]dhcp|static] [[address=][/] [[mask=]
] [[gateway=]|none [gwmetric=]] [[type=]unicast|anycast] [[subinterface=]
] [[store=]active|persistent]
```

Let's say you want to set an IP 192.168.1.10 on your interface. The gateway to your network of netmask 24bit is 192.168.1.1. So the command will become

```
set address "Local Area connection" static 192.168.1.10 255.255.255.0
192.168.1.1 1
```

To make my life easy I always rename my network connections to something like LAN1, LAN2 WIFI1 etc.

That enables me to use this command faster on command line directly such as

```
C:\> netsh interface ip set address name="WiFi" static 192.168.1.93
255.255.255.0 192.168.1.1 1
```

or

```
C:\> netsh interface ip set address name="LAN1" source=dhcp
```

Ok, that's IP set, what about DNS, can't go long way without it.

```
C:\> netsh interface ip set dnsserver name="LAN1" static 8.8.8.8 primary
```

Or

```
C:\> netsh interface ip set dnsserver name="WiFi" source=dhcp
```

Remember, you can create batch files with these commands to run directly and make your work faster & efficient

Damn! This NETSH is still due for a deeper coverage.

## Linux

Ok! as we have always seen Linux is much easier on command line, let's see how we can achieve the same outputs on Linux.

The first target is to set an IP address on the interface.

```
# ifconfig eth0 192.168.1.10 netmask 255.255.255.0
```

The best option here in Linux is that you can fake the MAC address also from command line

To change the mac address

```
# ifconfig eth0 down  
# ifconfig eth0 hw ether DE:AD:CA:FE:BA:BE  
# ifconfig eth0 up
```

If you check the commands carefully, we haven't yet configured the gateway and DNS server.

DNS in Linux goes through the universal nameservers configured which can be done by nameserver command. To set the gateway in Linux, we'll have to use route command

```
# route add default gw 192.168.1.1
```

You might have noticed that I generally leave the Linux part short. The reason is I want you people to explore the possibilities in Linux cause that's the way of learning Linux

Happy networking ☺



**Rohit Srivastwa**  
[rohit@clubhack.com](mailto:rohit@clubhack.com)

Teamwork matters in winning  
Against competitors or attackers

