



**Information Sharing Forum (ISF) - Advisory on Web Defacement**  
**15 March 2005**

**1.0 Executive Summary**

Since Monday, 7th March 2005, several Malaysian websites has been hacked or defaced by attackers unknown. The total number of compromised sites currently lies between 50 - 80 sites, while the real figure has yet to be determined. Several of the defaced sites belong to the Government as well as the private sectors.

Through a brief analysis of the affected websites, the ISF has determined that they were most likely compromised through one or more of the following methods:

1. SQL injection vulnerabilities
2. Vulnerabilities in Awstats (5.7-6.2), a popular web server log analysis tool
2. Vulnerabilities in phpBB, a bulletin board system (< 2.0.13)
3. Vulnerabilities in old versions of PHP (< 4.3.10 or 5.0.3)

**2.0 The purpose of this advisory**

The purpose of this advisory is to notify both the public and private sectors as to the immediate steps that they can take in order to protect themselves from possible defacement. While this advisory does not cover all areas of information and network security, it is published to address the three most common areas in which the web sites targeted were compromised. These are namely SQL injection vulnerabilities, multiple vulnerabilities in Awstats and phpBB, a bulletin board system.

**3.0 The scope of this advisory**

This advisory will help you in:

- Upgrading Apache and PHP
- How to protect sensitive URLs (e.g /admin, /stats)
- How to determine if your web applications are vulnerable to SQL injection and how to protect yourself.

**Note:**

This advisory only addresses the issues based on our brief analysis of the defaced websites.

This advisory IS NOT a silver bullet to a totally secure network! Security is a PROCESS not a PRODUCT!

#### **4.0 Who to contact regarding this advisory**

##### **Malaysian Communications and Multimedia Commission**

63000 Cyberjaya

Selangor

Telephone: +603 8688 8000

Facsimile: +603 8688 1000

Website : [www.mcmc.gov.my](http://www.mcmc.gov.my)

Freephone number: 1-800-888-030

#### **5.0 Defacement methods**

Based on our initial analysis of the defaced sites, the ISF has found that they were vulnerable to SQL injection. In addition, some of the sites ran vulnerable version of phpBB and Awstats. Furthermore, some of the platforms and applications are old and contain multiple vulnerabilities.

These vulnerabilities can lead to:

- Remote Command Execution
- Privilege Escalation

#### **6.0 How to determine if you are at risk**

## 6.1 phpBB

phpBB 2.0.12 and below are vulnerable to various CRITICAL remote exploits including Administrator Authentication Bypass. If you are using a version prior to 2.0.12 it is vital that you upgrade IMMEDIATELY. For users upgrading from 2.0.12 please see 7.1 The latest version of phpBB is 2.0.13.

## 6.2 AWSTATS

Versions of AWSTATS 5.7-6.2 are vulnerable to remote command execution. There is a working exploit in circulation for this issue. Users are strongly encouraged to upgrade to AWstats 6.3

## 6.3 SQL Injection

The quickest way to determine if you are vulnerable to SQL injection is as follows:

Assuming your web application URL is like the following:

```
http://myurl/product.asp?id=1098
```

Test it by placing a single quote after the value 1098, as follows:

```
http://myurl/product.asp?id=1098'
```

If you are vulnerable, and depending on how the application is coded, you may get an error similar to the following:

**Microsoft OLE DB Provider for ODBC Drivers error '80040e14'**

```
[Microsoft][ODBC SQL Server Driver][SQL Server]
Unclosed quotation mark before the character string ".
/product.asp, line 73
```

This means that you are vulnerable to SQL injection attacks. For more information on SQL injection please see section 8.3.

## **6.4 PHP**

There are several critical vulnerabilities in the PHP Hypertext Preprocessor both in versions prior to 4.3.10 and 5.0.3. Versions prior to the above are vulnerable to over 30 non-critical bugs including several very serious security issues.

These include the following:

- CAN-2004-1018 - shmop\_write() out of bounds memory write access.
- CAN-2004-1018 - integer overflow/underflow in pack() and unpack() functions.
- CAN-2004-1019 - possible information disclosure, double free and negative reference index array underflow in deserialization code.
- CAN-2004-1020 - addslashes() not escaping \0 correctly.
- CAN-2004-1063 - safe\_mode execution directory bypass.
- CAN-2004-1064 - arbitrary file access through path truncation.
- CAN-2004-1065 - exif\_read\_data() overflow on long sectionname. magic\_quotes\_gpc could lead to one level directory traversal with file uploads.

All users of PHP are strongly encouraged to upgrade to the latest release as soon as possible.

## **6.5 Apache**

Make sure that you are running the latest version of Apache. The latest version is 1.3.33 for the 1.3.x series and 2.0.53 for the 2.0 series. If you are running mod\_ssl, make sure you upgrade to the latest version as well. The latest version of mod\_ssl for Apache is 2.8.33.

## **6.6 IIS**

Make sure your IIS and Operating System has been fully patched. Please see section 7.8 and 8.7 for further details.

## **6.7 Rootkits**

A rootkit is a collection of tools an intruder brings along to a victim computer after gaining initial access. A rootkit generally

contains network sniffers, log-cleaning scripts, and trojaned replacements of core system utilities such as ps, netstat, ifconfig, and killall. Although the intruders still need to break into a victim system before they can install their rootkits, the ease-of-use and the amount of destruction they cause make rootkits a big threat for system administrators. For rootkit detection tools, please see 7.7

## 6.8 Protecting Sensitive URLs

Check that sensitive URLs are protected using .htaccess or equivalent.

If your website has a URL like /admin, /stats etc. make sure that they are protected using .htaccess or a similar method in order to provide a layer of authentication for these critical directories. For details on enabling .htaccess in Apache and the equivalent for IIS please see 7.8

## 7.0 Solution

### 7.1 Upgrade phpBB 2.0.13

To manually upgrade from phpBB 2.0.12 to 2.0.13:

Open includes/sessions.php

#### Find:

```
if( $sessiondata['autologinid'] == $auto_login_key )
```

#### Replace with:

```
if( $sessiondata['autologinid'] === $auto_login_key )
```

A second minor issue relates to a path disclosure bug in viewtopic.php

Open viewtopic.php

#### Find:

```
$message = str_replace('\\"', '\"',  
substr(preg_replace('#(\>(((?>([^\><]+|(?R)))*)\<))#se'
```

```
, "preg_replace('#\b(" . $highlight_match . ")\b#i', '<span style=\"color:#\" . $theme['fontcolor3'] . \"\"><b>\\\\1</b></span>', '\\0')", '>' . $message . '<'), 1, -1));
```

### **Replace with:**

```
$message = str_replace('\\", ""', substr(@preg_replace('#(\>(((?>([\^><]+|(?R)))*)\<))#s e', "@preg_replace('#\b(" . $highlight_match . ")\b#i', '<span style=\"color:#\" . $theme['fontcolor3'] . \"\"><b>\\\\1</b></span>', '\\0')", '>' . $message . '<'), 1, -1));
```

## **7.2 Upgrade awstats to version 6.3**

To upgrade awstats, download the latest version from <http://awstats.sourceforge.net>. The latest version is 6.3

## **7.3 Check application codes for SQL injection vulnerabilities**

While the testing for SQL injection vulnerabilities is beyond the scope of this document, please utilize section 6.3 in order to do a quick assessment on whether you are at risk. You can also use a web vulnerability scanner to identify other possible problem areas.

The most popular web vulnerability scanner is Nikto. It can be downloaded from <http://www.cirt.net>. Nikto requires Perl to run and is installed by default on Linux and Unix systems. For Windows users, PERL can be obtained from:

<http://www.activestate.com/Products/ActivePerl/>

After downloading and installing Nikto, you can run it as follows to scan your website:

```
nikto.pl -host mywebserver -generic
```

## **7.4 Upgrade PHP 4.3.10 or 5.0.3**

To upgrade PHP, download the latest codes from

<http://www.php.net/downloads.php>

Specific instructions to upgrade PHP for different Linux distributions can be found from their respective sites.

## 7.5 Upgrade Apache

The latest stable release of Apache is 1.3.33 or 2.0.53 Apache is available for download from <http://httpd.apache.org/download.cgi> Binary distributions are available from <http://www.apache.org/dist/httpd/binaries/>

## 7.6 Microsoft Windows Update

To check for patches on Microsoft Operating Systems users can use the Windows Update Service (<http://windowsupdate.microsoft.com>) For details on securing IIS please see 8.8

## 7.7 Rootkits

For Linux and UNIX systems, chkrootkit can be used to check for rootkits. Chkrootkit can be downloaded from <http://www.chkrootkit.org/>

For Windows, tools such as flister (<http://invisiblethings.org/tools/flister.zip>) can be used.

## 7.8 Protect sensitive URLs

### 7.8.1 .htaccess for Apache

The format of the **.htaccess** file is fairly simple, with four required lines and one required section. The only pieces that need customizing are *AuthUserFile* and *AuthName*. These lines are summarized below:

#### **AuthUserFile**

*Customize* -- This gives the path to the password file that will actually be used for authentication. Give the full path to the file (this can generally be discovered with the 'pwd'

command), and do not put this file in the same directory as your **.htaccess** file.

### **AuthName**

*Customize* -- This gives the name of the group that is allowed to access the data. It is only used in the question asked when the user is required to enter their userid and password. For example: *Username for Authentication at server servername:*

### **AuthType**

Set this to *Basic* for the basic authentication type.  
The **.htaccess** file must be world readable.

.htaccess file contents:

```
AuthType Basic
AuthName "Password Required"
AuthUserFile /www/password.file
AuthGroupFile /www/group.file
Require Group admins
```

The next (and last) step is the creation of the password file mentioned in the **AuthUserFile** line above. This is done through the use of the `htpasswd` command. The syntax of the command is

```
htpasswd -c <passwd file> <user>
```

where the *passwd file* is the information in the **AuthUserFile** line. The command will then prompt you to enter the password and add it to the file. For example:

```
% htpasswd -c .mypasswd administrator
New password:
Re-type new password:
Adding password for user administrator
```

Similar to the **.htaccess** file, this file must be world readable

## **7.8.2 Permissions Wizard for IIS**

The Permissions Wizard is used to create or edit a template and then apply the template to a folder. Apache uses .htaccess files and Directory directives in the main Httpd.conf configuration file. You can easily copy these files and directives around your site to set the same values across multiple folders. There is no equivalent in Internet Information Services (IIS). However, the IIS Permissions Wizard in the Windows 2000 Resource Kit can create templates that you can apply to different folders. You can use this method to emulate the .htaccess functionality for multiple folders.

## 8.0 References

### 8.1 phpBB

<http://www.phpbb.com/phpBB/viewtopic.php?f=14&t=267563>

<http://www.phpbb.com/downloads.php>

### 8.2 Awstats

<http://awstats.sourceforge.net/>

<http://www.k-otik.com/exploits/20050124.awexpl.c.php>

### 8.3 SQL INJECTION REFERENCE

[http://www.nextgenss.com/papers/advanced\\_sql\\_injection.pdf](http://www.nextgenss.com/papers/advanced_sql_injection.pdf)

[http://www.nextgenss.com/papers/more\\_advanced\\_sql\\_injection.pdf](http://www.nextgenss.com/papers/more_advanced_sql_injection.pdf)

<http://www.spidynamics.com/whitepapers/WhitepaperSQLInjection.pdf>

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

### 8.4 PHP

<http://www.php.net>

<http://www.php.net/manual/en/security.php>

<http://www.phpsecurity.org>

### 8.5 Apache

<http://httpd.apache.org>

### 8.6 Rootkits

<http://www.linuxdevcenter.com/pub/a/linux/2001/12/14/rootkit.html>

<http://la-samhna.de/library/rootkits/>

### 8.7 .htaccess for Apache

<http://www.its.queensu.ca/network/policy/htaccess.shtml>

#### Permissions Wizard for IIS

<http://support.microsoft.com/?kbid=324070>

#### Managing a Secure IIS 6.0 Solution

[http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG\\_SEC.mspx](http://www.microsoft.com/resources/documentation/IIS/6/all/techref/en-us/iisRG_SEC.mspx)

## 9.0 Notes

### Advisory Prepared by:

Meling Mudin (mel –at- hackinthebox.org)

Dhillon Andrew Kannabhiran (dhillon –at- hackinthebox.org)

## **Issued via the Information Sharing Forum (ISF) for MCMC**

### **About the Information Sharing Forum (ISF):**

The Malaysian Communications and Multimedia Commission (MCMC) have formed the Information Sharing Forum (ISF) with various Internet service providers (ISP) and other agencies to address information and network security issues in Malaysia.

The ISF seeks to improve communication channel and mutual understanding between ISPs and the information and network security industry in managing information and network security incidents which, if not addressed, would lead to slower information dissemination and ineffective security incident response handling in the country.

The objective of the ISF is to bring together the relevant parties into a single forum to share their experiences and expertise for the benefit of the Malaysian network infrastructure, and to establish effective information sharing mechanism.

The ISF is in a position to complement and support one of the 10 national objectives in the communications and multimedia sector outlined by the Government – to ensure information security and network reliability and integrity.

The ISF is headed by the MCMC. Its members consist of Internet Service Providers (ISPs) and other information and network security agencies and representatives from the industry.