



NISCC Technical Note 06/03

Issued 1 August

Guidance on Securing Web Sites

Key Points

- This is an updated re-issue of advice first published as NISCC Technical Note 03/2002.

**National Infrastructure
Security Co-Ordination Centre**
PO Box 832
London, SW1P 1BG

Tel: 020 7821 1330 Ext 4511
Fax: 020 7821 1686
Email: enquiries@nisc.gov.uk
Web: www.nisc.gov.uk

NISCC Technical Note 06/03:

Guidance on Securing Web Sites

Introduction

1. The following Technical Note is intended for those within the NISCC constituency for securing web sites against an untrusted user community. In the case where a web site is managed by an Internet Service Provider (ISP), they should ensure as far as possible that the ISP has procedures in place to comply with the organisation's web site security policy and to meet the following specific recommendations for securing the organisation's web site. It is also strongly recommended that the application and maintenance of those procedures is checked on a regular and frequent basis by qualified security consultants such as those accredited under the CHECK service.
2. Following the advice in this note should increase the security of your web site, but it cannot provide complete security. There are aspects of web site security, such as authentication, that are not addressed in this note because they may rely on third-party or proprietary technologies and are large topics in their own right.

Background

3. It needs to be stressed that most successful attacks on web sites are made possible by misconfiguration of the web server and failure to install security patches. The guidance in the sections below aims to provide advice on correct configuration and patch application.
4. The Note assumes that the organisation has a web site security policy in place and procedures for enforcing that policy. The guidance in this Note is designed to inform such security policies and procedures from a technical perspective. Physical and personnel measures will also be required to ensure that the web server environment is secure, but these are beyond the scope of this Note.
5. The following is a list of guidance from vendors and reputable third parties that may be relevant but which is not endorsed by NISCC:
 - <http://www.microsoft.com/technet/security/tools/tools.asp>
 - http://httpd.apache.org/docs/misc/security_tips.html
 - <http://nsa1.www.conxion.com/support/download.htm>
 - <http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf>
6. The security of a web site is determined by the security of the following:
 - The security of the web server
 - Remote web server administration (not addressed here)
 - The security of the operating system of the web server computer
 - The security of the local area network of the web server computer
 - The security of "backend" (eg database) applications supporting the web server
 - The security of the authoritative domain name server for the web server network

7. In this note each area of security will be considered in turn with recommendations for each. All of the recommendations should be followed if good web site security is to be achieved.

8. This note presupposes that the web server is connected to an untrusted user community such as the Internet and does not address the possibility of trusted users accessing or maintaining the web site remotely. Most web servers provide remote file and directory authentication for such purposes, and often use proprietary authentication mechanisms, although the types and use of such authentication are beyond the scope of this Note.

9. There are other aspects of web server practice that are not covered in this note. The following is a list of **all** aspects that are beyond the scope of this note:

- Physical security of the web server
- Remote web server administration
- Authentication to the web server
- Confidentiality of web traffic in transit (eg Secure Sockets Layer/Transport Layer Security)
- Virtual hosting
- Availability measures (eg load balancing)

The security of the web server

10. A web site is hosted by a web server. For the purpose of defining terms, a web server is an application that accepts requests from client web browsers in the hypertext transfer protocol HTTP and HTTP over Secure Sockets Layer (HTTPS) and responds by sending web pages and other content to the client web browsers.

11. These web pages can be manually generated by a web page designer or they can be automatically generated. Automatically generated pages may use executables or interpreted scripting languages such as perl or python to produce the web pages according to the common gateway interface (cgi) specification, or they may use server side programming extensions such as Active Server Pages (ASP), Java Server Pages (JSP) or Personal Home Pages (PHP). Web server security therefore splits into two further areas:

- The security of the web server itself
- The security of any server extension technologies (eg ISAPI extensions in Microsoft Internet Information Services)

12. Tools are available from some vendors to automate configuration of the web server to enhance security (for example the IISLockdown tool for Microsoft Internet Information Services web server). Such tools can be useful in enforcing the measures indicated in this Note. Web server vulnerability scanning tools can also be useful in determining misconfigurations and vulnerabilities, but they are not a substitute for testing by qualified security consultants.

13. The following steps are recommended:

a. As with any application, ensure that you monitor UNIRAS Notes and commercial sites such as Bugtraq (<http://www.securityfocus.com>) on a regular and frequent basis and install any security patches relevant to the version of the web server that you are using. The web site vendor's web site should also be able to provide instructions on installing the patches and their coverage of vulnerabilities.

- b. Remove any functionality from the web server for which there is no business need. This includes the ability to generate web pages dynamically on the web server, and additional services such as file transfer and network news.
 - c. When configuring the web server (where the web directories are managed or exist in the context of the web server), ensure that any access controls that can be set within the web server application are set on all directories under and including the root directory of the web server as follows:
 - i. Ensure that, unless they are used to store user data, web directories or files within the web directory structure are only modifiable or writable by the web server.
 - ii. Access to web pages should be read only for web users, although the web user will need permission to execute scripts or programs used to generate web pages dynamically if the executables are CGI scripts. By default ASP, JSP and PHP pages do not need execute permission.
 - iii. Web users should not be able to list the contents of directories.
 - iv. No access should be granted to other directories or programs in the web directory structure unless there is an explicit need.
 - v. No access should be granted to the web server executable or to the web server configuration files.
 - d. Do not assign access control override privileges to the web user as these can be abused by attackers to turn off access control.
 - e. Enable logging on the web server so that all web server activity is logged. This should be analysed on a regular and frequent basis by the staff responsible for web security or their nominated representatives in their ISP for events indicative of an attack, for instance attempts to run non-existent scripts. The web server log should also contain all attempted and established connections including complete URLs, HTTP request parameters, error messages, remote authentication attempts, all scripts run and any access control violations for files and directories under access control of the web server.
14. For the security of cgi scripts and server extensions, the following steps are recommended:
- a. Remove all sample scripts installed with the server.
 - b. Remove all unnecessary server extensions. Examples include server extensions such as those for network printing, database connectivity, web site indexing, distributed authoring and remote administration.
 - c. Disable any server directives or extensions that enable scripts to run operating system level commands on the web server computer (eg for a UNIX environment, Server Side Includes).
 - d. Ensure that a competent person, preferably a qualified security professional (eg a CHECK consultant or a CLAS consultant), checks all scripts and server side extensions that are used on the web server to ensure that they validate input to allow only expected data types and lengths of input data and produce error

messages otherwise. Care should be taken that characters that can be treated by an application as executable ("special characters") and empty values are filtered by the web server before passing on the data to applications. Escapes to an operating command shell and injection of user scripts should never be permitted.

e. For CGI scripts, if possible, store all scripts in the same directory and forbid execution of scripts outside this directory. In addition, CGI scripts should check their execution context or execution environment, for example, the session state, validity of any security tokens and whether the CGI scripts are being called by the web page that they are expecting or whether they are being called directly. CGI scripts should be written only to execute in a defined context.

The security of the operating system of the web server computer

15. The security of the web server is only as good as the security of its environment. If the operating system is configured securely, the damage that a malicious web user could do will be restricted to what can be obtained with the web user privileges.

16. For the security of the operating system of the web server computer the following steps are recommended:

a. When selecting an operating system, a high level of security will be obtained by:

i. selecting an operating system that has been evaluated against a security standard for discretionary access control, recognised by the UK Government which includes an independent check of the security enforcing source code (eg ITSEC E3 F-C2 or Common Criteria EAL4 with the Controlled Access Protection Profile);

ii. configuring the operating system to run in its evaluated configuration where the configuration permits a web server to run in a networked environment; and

iii. in the case where no evaluation exists for the operating system, following security configuration guidance from the vendor or from a reputable organisation providing specialist advice (for example, guidance on Microsoft Windows NT, 2000 and XP secure configuration is available from Microsoft, see <http://www.microsoft.com/technet/security/tools/tools.asp>, and from NSA, see <http://nsa2.www.conxion.com/>).

b. As in the case of the web server, ensure that you monitor UNIRAS Notes and commercial sites such as Bugtraq (<http://www.securityfocus.com>) on a regular and frequent basis and install any security patches relevant to the version of the operating system that you are using. It is recommended that you test the patches prior to installation on an operational system. The operating system vendor's web site should also be able to provide instructions on installing the patches and their coverage of vulnerabilities.

c. Ensure that the web server runs with the least privilege needed. The web server should not run as an administrator (including the web server administrator) or superuser (if applicable). In a UNIX environment if superuser privileges are needed to bind to the HTTP port, the binding should be run as the

superuser using a set user id process and all child processes should be run as an unprivileged web user.

d. Do not assign discretionary access control or mandatory access control override privileges to the web user as these can be abused by attackers who manage to gain web user privilege.

e. To ensure that the web server is an unprivileged user, restrict access for the web server user to files and directories relevant to the web server application (which may be the directory structure under the web server root). Check the permissions on all other files and directories on the web server to ensure that the web server cannot gain access to any executables or data files that are not needed.

f. If the web server directory structure is not virtual (ie the directories exist or are managed within the operating system environment), ensure that access controls are set appropriately on all files and directories relevant to the web server:

i. Ensure that, unless they are used to store user data, web directories or files within the web directory structure are only modifiable or writable by the web server.

ii. Access to web pages should be read only for web users, although the web user will need permission to execute scripts or programs used to generate web pages dynamically if the executables are CGI scripts. By default ASP, JSP and PHP pages do not need execute permission.

iii. Web users should not be able to list the contents of directories.

iv. No access should be granted to other directories or programs relevant to the web server application unless there is an explicit need.

v. No access should be granted to the web server executable or to the web server configuration files.

vi. No access should be granted above the root of web server directory structure.

g. In a UNIX environment, it may be beneficial to security to run the web server with a redefined root directory using the *chroot* command. In this case do not have any symbolic links to files outside the directory structure that include directories under the redefined root directory. The web server root should not be the operating system root.

h. Enable logging on the operating system and for the web server so that security relevant activity is logged. This should be analysed on a regular and frequent basis by the staff responsible for web security or their nominated representatives in their ISP for events indicative of an attack, for instance attempts to access files without the correct permissions. All error messages, application startup and shutdown, attempted remote application logins, and changes in file permissions should also be logged.

i. Ideally the web server should be run as a dedicated web server. To decrease the risk of successful compromise and misconfiguration remove **all**

unnecessary executables (including compilers and utility programs such as Debug, FTP and TFTP) and network services from the web server computer. These steps are part of a host lockdown.

j. Remove all unnecessary user accounts from the server and implement passwords for the remaining accounts that are hard to guess and accord with the department or company security policy for password generation and use. The passwords used on the web server should be different to those used on other systems in the network.

The security of the local area network of the web server computer

17. The web server environment extends from the web server computer to its local area network and to the internet or intranet environment.

18. For the security of the local area network of the web server NISCC Technical Note 01/02 provides general guidance on network security. The following web server specific steps are recommended:

a. Install a firewall between the web server computer local area network and the internet to handle all traffic to and from the internet or intranet. For web traffic the firewall should deny all unnecessary incoming services and should offer HTTP and possibly HTTPS for commercial standard IP encryption of web traffic as uninitiated incoming connections. HTTP should be proxied to provide initial validation of the web page request. In order to help prevent the spread of Internet worms, unless there is a good reason to the contrary the firewall rules should not allow a web server to initiate an HTTP session. DNS should be allowed outbound on an unprivileged port to request DNS lookups and should listen on that port for responses. It is recommended that a certified firewall is used. For details of certified firewalls see the Common Criteria web site, <http://www.commoncriteria.org>.

b. Isolate the web server computer on its own network segment. This may be as a stand alone network or on a DeMilitarised Zone (DMZ) that has restricted access to the internal network and in particular to any database server that are used to store sensitive information. If an organisation does not have a DMZ, the use of a non-routable IP protocols (eg NetBEUI for Microsoft Windows computers) between the web server and the internal network could be considered. (Note that NetBIOS/SMB over TCP/IP should not be made available on Microsoft Windows computers that include the web server, as the use of NETBIOS potentially allows access to shared network resources.)

c. Do not allow any unnecessary trust relationships between the web server computer and other hosts on the network, for example Microsoft Windows domains, UNIX Network Information Service (NIS) or NIS+, as abuse of trust could lead to compromise of all hosts in the trust relationship once one host has been compromised.

d. Enable logging on the firewall so that security relevant activity is logged. This should be analysed on a regular and frequent basis by the staff responsible for web security or their nominated representatives in their ISP for events indicative of an attack, for instance attempts to access services with known vulnerabilities. Successful/denied connections, error messages, multiple access attempts and access to insecure ports should be logged.

The security of "backend" applications supporting the web server

19. Any supporting "backend" applications (eg databases) should be stored on another computer. Care needs to be taken that the web user account can only perform a specified set of actions on the "backend" applications so that the security of those applications is not compromised. For example, if a database application is used as a read-only source to web users, the web user account should have read only access to the database, while if the database is updated by the web user account via web forms, the web user should be restricted to database update queries. This requirement could be met by a database application which provides access control by query type and data object (such as database and table) within the database application.

20. User names and passwords should not be hard coded into web pages as web page source is readable by potential attackers.

21. All backend applications should validate data received to ensure that the data is of the correct data type (eg integer), is not too long, and does not include special characters that may lead to the data being treated as executable.

22. It is recommended that, where possible, the backend application is not directly connected to the end user. The use of a proxy server or data transfer agent may be appropriate in some cases to mediate the connection and to provide data validation and additional authentication mechanisms. It is good practice to ensure that access to backend application takes place in a controlled, well defined way. This may be assisted by a modular, object oriented design of the web server and backend applications as a whole.

The security of the authoritative domain name server for the web server network

23. It is possible to change the IP address associated with a web site address (URL). When this is done maliciously it is known as DNS poisoning. DNS poisoning can be achieved in a number of ways:

- a. by exploiting a buffer overflow in the DNS implementation and altering the DNS databases;
- b. by spoofing the response to a query from a legitimate DNS server by guessing its response identifier;
- c. by exploiting a vulnerability in versions of some older DNS implementations that allows a client to upload incorrect DNS records to a DNS server for a domain for which it is not authoritative (known as "cache poisoning"); or
- d. by spoofing an authoritative DNS server.

24. To prevent these types of DNS poisoning, DNS server administrators should if possible upgrade the DNS version to the latest version and apply all relevant security patches. Some implementations of DNS use cryptographic authentication for DNS updates. Alternatively DNS server administrators should if possible configure their servers to check DNS records obtained from an authoritative DNS server by comparing them with those taken from another authoritative server. Authoritative master primary DNS servers should be protected by a firewall. Zone

transfers should be restricted from master primary DNS servers to designated slave DNS servers, which preferably should be within the perimeter protected by a firewall. It is recommended that the web server administrator confirm with the administrator of the authoritative DNS server that the protective measures identified above have been taken.

25. It is also possible for DNS poisoning to be performed manually. The web address registration authority for the domain that includes your web server may receive bogus requests to alter the IP address associated with the web site URL, by email for example. The staff responsible for web security should satisfy themselves that the registration authority has adequate security measures in place to ensure the authenticity of any changes to the IP addresses in their domain. Examples of reasonably secure authentication schemes are digitally signed emails, challenge-response password authentication over the telephone and a recognised signature on official company notepaper.

26. In order to limit the visibility of hosts on the internal network, some organisations use separate DNS servers for the internal network and for external queries. This approach has much to recommend it provided that the details published on the external DNS server are sufficient for customers to resolve host names of all of the organisation's servers that offer services to them.