CERT-In

Indian Computer Emergency Response Team

Handling Computer Security Incidents

Web Server Security Guidelines

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Issue Date: August 17, 2004

Table of Contents

1. Introduction

A Web Server is a computer host configured and connected to Internet, for serving web pages on request. Information on Public web servers can be accessed by people anywhere on the Internet. Since web servers are open to public access they can be subjected to attempts by hackers to compromise the server.
Hackers can deface websites and steal valuable data from systems. This can translate into a significant loss of revenue if it is a financial institution or an e-commerce site. In the case of corporate and government systems, loss of important data may actually mean the launch of information espionage or information warfare on their sites. Apart from data loss or data theft a web defacement incident can cause significant damage to the image of an organization. Common security threats to a public web server can be classified as the following-

- Unauthorized access
    - Defacement
    - Content theft
    - Data manipulation
- Improper usage
    - Launch pad for external attacks
    - Hosting improper/malicious contents (e.g phising)
- Denial of Service
- Physical Threats

Hackers take advantage of different security flaws in a web hosting infrastructure and exploit the vulnerability to compromise the system. Common security flaws that can lead to a compromise can be categorized as

- Insufficient network boundary security controls
- Flaws or bugs in web hosting software (OS, application etc)
- Insecure design and coding of hosted application
- Weak password
- Social engineering
- Lack of operational control

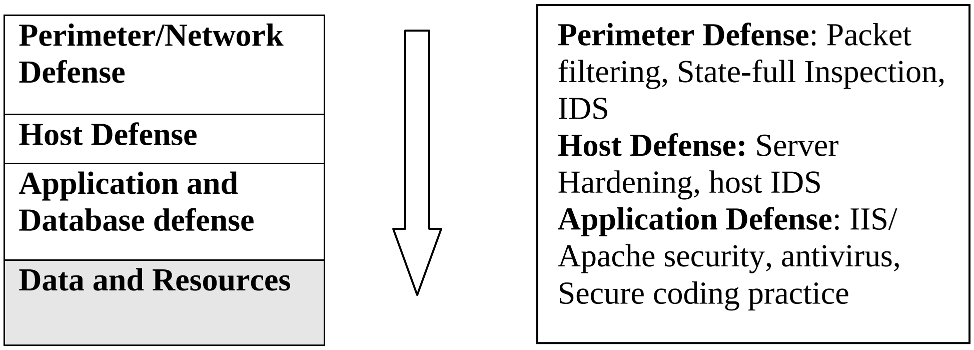
An attacker can adopt various hacking techniques or tools to exploit or take advantage of the above mentioned security flaws. A discussion on common hacking/attack methods can be referenced from the following document.

CERT-In: Hacking - How they do it?
http://www.cert-in.org.in/advisory/CIAD200303.pdf

1.1 Defense in depth

Securing a web server comprises of implementing defense in depth using various security controls at network architecture, operating system and application levels.

Defense in depth is defined as the practice of layering defenses to provide added protection. The defense in depth architecture places multiple barriers between an attacker and business-critical information resources. These multiple layers prevent direct attacks against important systems and avert easy reconnaissance of networks.



Perimeter Defense: Packet filtering, State-full Inspection, IDS
Host Defense: Server Hardening, host IDS
Application Defense: IIS/ Apache security, antivirus, Secure coding practice

Fig 1

2. Network Security

2.1 Design Screened subnet

The network architecture should be designed to create different security zones/segments for external users, internal users and the servers. The Web server should be placed in the secure Server Security segment (also referred to as DMZ[**] or screened subnet) isolated from the public network and organization's internal network. The network architecture can be designed as a single layer or multi layer, as per the requirement of the organization.

A Web Hosting Network should have at least three segments. viz.

Internet Segment
Public server segment (Web, Mail, DNS servers)
Internal Segment

A firewall should be used to restrict traffic between the public network and the Web server, and in between the Web server and internal networks.
Servers providing supporting services to the Web Server (like Database Server, LDAP Server) should be placed on another subnet isolated from public and internal networks. In a multi-layer architecture, the traffic to this subnet is filtered using another firewall.

Some typical Network designs have been shown in the Figures 2 and 3.

[**] DMZ : De-Militarised Zone is a no-man's land between the Internet and the internal network. This zone is not on the internal network, and is not directly open on the Internet. A firewall or a router usually protects this zone. This is the zone where the servers for public-access are placed.

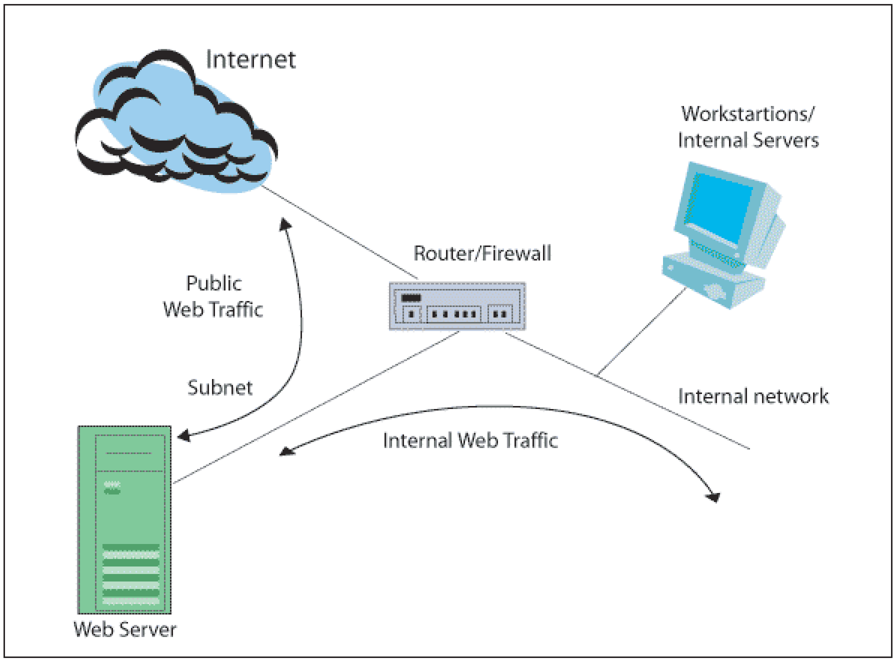

Internet
Workstartions/
Internal Servers
Router/Firewall
Public
Web Traffic
Subnet
Internal network
Internal Web Traffic
Web Server

Fig. 2

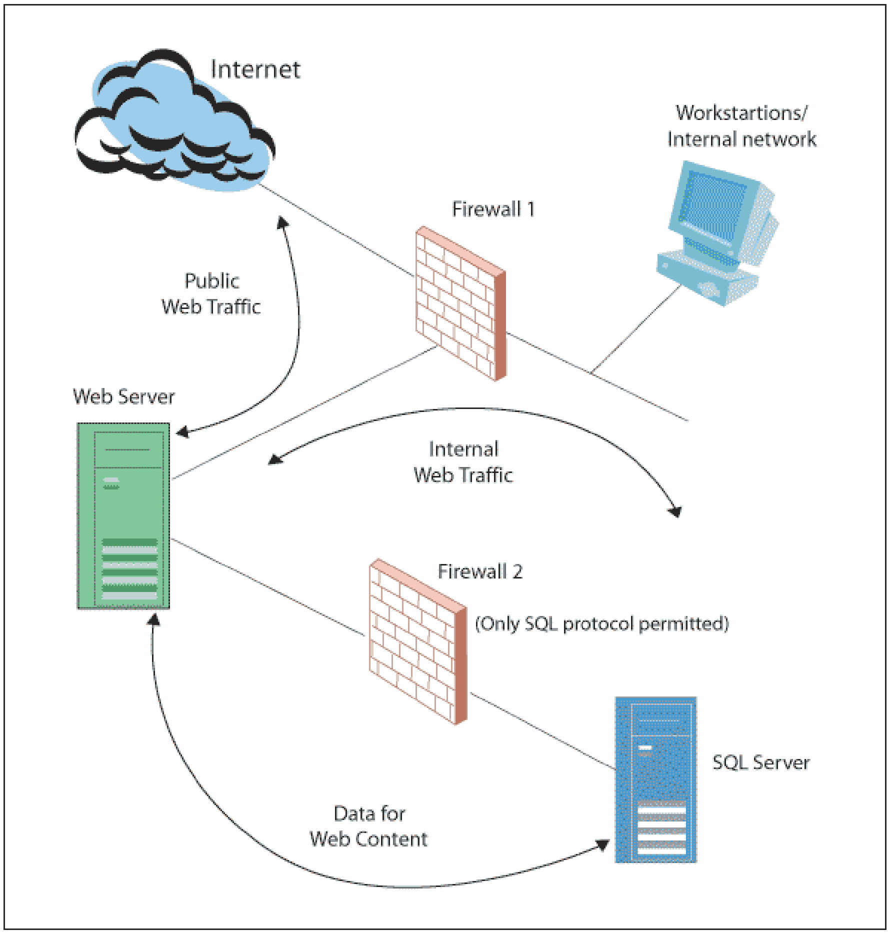

Internet
Workstartions/
Internal network
Firewall 1
Public
Web Traffic
Web Server
Internal
Web Traffic
Firewall 2
(Only SQL protocol permitted)
SQL Server
Data for
Web Content

Fig. 3

The following guidelines may be consulted while designing the network architecture.

CERT-In: Network Perimeter Security
http://www.cert-in.org.in/presentation/perimeterSecurity.pdf

CERT/CC
http://www.cert.org/security-improvement/practices/p075.html

NIST: A guide for selecting Network Security Products
http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf

2.2 Access controls

Access controls to the network resources can be enforced at different levels of the network. The primary access control devices are routers and firewalls.

2.2.1 Router

The router is the first line of defense to the network of an organization and hence the router itself should be secured. Necessary control should be applied on the router to stop unwanted traffic and attacks at the perimeter itself. In the secure configuration of a router, the following should be considered.

- Deploy proper access management and preferably disable remote administration.
- Enable secret password
- Change default SNMP community string
- ACLs (access control lists)should include
    - Apply egress/ingress filter
    - Filter all RFC 1918, 3330 address space and special/reserved addresses
    - Permit the required services for the required IP Addresses only
    - Deny everything else.
- Turn on logging to a central syslog server.

The following documents detail the router configuration steps to secure the network and the router.

CISCO: Improving Security on Cisco Routers
http://www.cisco.com/warp/public/707/21.html

CERT-In: Cisco Router Security Best Practices
http://www.cert-in.org.in/guidelines/CISG-2004-02.pdf

Juniper Networks:
www.juniper.net/solutions/literature/app_note/350013.pdf

2.2.2 Firewall

A firewall is a combination of hardware and software, located at a network gateway, protecting the resources of a network from users of other networks. It enforces a boundary between two or more networks and limits access between networks and network segments in accordance with the local security policy. It filters all network packets to determine whether to forward them toward their destination or discard them.

Firewalls available commonly use different technologies like

Packet filter
Statefull Inspection Firewall
Application Proxy Firewall

Firewall is available both as software and as an appliance. All the above technologies have their own advantages and disadvantages. Users should choose the best possible combination after analyzing the requirement of the network to be protected and the servers that shall be deployed behind it.

A Firewall should be appropriately implemented to segregate the networks into different network segments. The following should be considered during the implementation of a firewall system-

- If a software firewall is used, the host on which the Firewall is installed should be secured.
- For the firewall deployment in an organization, specific security guidelines as specified by the firewall vendor should also be consulted.
- The firewall should be configured for full logging and a mechanism for generating alerts on suspicious activity.
- A firewall is only effective when proper rules (local security policy) are applied. Thus, the rules (local security policy) should be carefully designed, after considering all the threats and security requirements. Rules are then applied to protect the organizational network and servers deployed behind the firewall.

Do’s and Don’ts of firewall rule base

- Clean up rule:
  - Place a ‘DENY ANY-ANY’ rule, at the end of the rule base.
  - Never create a ‘ALLOW ANY ANY’ rule.
  - ALLOW rules should be created only for required services and servers.
  - This will result in all traffic being disallowed, unless specifically allowed.
- Lockdown/Stealth rule:
  - All traffic destined for the firewall itself should be disallowed.
- Anti-spoofing rule:
  - Place anti-spoofing rule as per RFC 1918 and 2827

- Enable DoS/DDoS prevention features on firewall.
    - Several Firewalls contain features to prevent DoS attacks. These should be enabled.
- Enable Application level filtering features of firewall.
    - If the firewall has abilities to perform Application level filtering, they should be enabled.

The following guidelines may be consulted while designing and implementing the firewall system

CERT-In: System Security Guidelines
http://www.cert-in.org.in/guidelines/CISG200304.pdf

CERT/CC
http://www.cert.org/security-improvement/practices/p053.html

NIST
http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

CERT-In: Perimeter Design & Implementation Issues
http://www.cert-in.org.in/presentation/27thfeb03/firewallcert.pdf

There are various firewalls available from different vendors. Some of the leading firewalls are:

Commercial	
Checkpoint	www.checkpoint.com
CISCO PIX	www.cisco.com
NetScreen	www.juniper.net
Raptor	www.symantec.com
Cyberguard	www.cyberguard.com
E-trust	www.ca.com
Microsoft ISA Server	www.microsoft.com/isa
Gauntlet	
Opensource	
IPTables/Netfilter	www.netfilter.org

2.3 Intrusion Detection Systems

An intrusion detection system (IDS) protects the network perimeter, extranets, and the internal network in real-time. An IDS system analyzes the network data stream and identifies attempts to hack or break into a computer system. It identifies attacks through various methods including anomaly detection and signature matching and can generate an alarm or react to the attack attempt.

- IDSs are available both as appliance and as software. If software IDS is used the host should be hardened first.

- The IDS should be updated with the latest signatures. Current rules should be applied and tuned so that false alarms are not generated.
- IDS should be deployed with network sensors in all segments of the network. Host IDS should be deployed on all critical servers including the web server.

There has been rapid development in this field with Intrusion Prevention Systems (IPS) now available. Being an inline device IPS has both advantages and disadvantages. Thus, the deployment of an IPS can be considered after careful analysis. The following guides may be consulted during the deployment of an IDS/IPS.

CERT-In: Intrusion Detection System
http://www.cert-in.org.in/guidelines/CISG-2003-06.pdf

NIST
http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

CERT-In: Intrusion Detection System
http://www.cert-in.org.in/presentation/27thfeb03/IDS.pdf

Some of the available Intrusion Detection Systems

Commercial

ISS Real Secure	www.iss.net
CISCO IDS	www.cisco.com
Session wall	www.ca.com
NetScreen	www.juniper.com
Tripwire	www.tripwire.com

Opensource

SNORT	www.snort.org

Some of the available Intrusion Prevention Systems

Commercial

UnityOne-1200	www.tippingpoint.com
ISS Proventia	www.iss.net
NetScreen-IDP	www.juniper.com
McAfee IntruShield	www.nai.com
Top Layer Attack Mitigator IPS 2400	

Opensource

Snort-inline	snort-inline.sf.net

2.4 Antivirus and SPAM prevention

1.1 Antivirus

- An anti-virus package should be installed on the Web Server system, if available on that platform.
- All clients which access the web server for the purpose of administration and content management should use an antivirus package with latest signatures.
- All documents and files hosted on the web server should be uploaded only after being checked for virus and Trojans.
- If the Web Server has provisions for uploading of files from users, appropriate mechanism should be in place at the server side to ensure that the files are virus free.

Some of the available Anti-Virus solutions:

Commercial

TrendMicro	www.trendmicro.com
McAfee	www.nai.com
Symantec	www.symantec.com
Sophos	www.sophos.com
Panda	www.pandasoftware.com
F-Secure	www.f-secure.com
Kaspersky	www.kaspersky.com

Free

AVG Free Edition	www.grisoft.com
AntiVir	www.free-av.com
BitDefender Free Edition v7	www.bitdefender.com

1.2 Open Proxy

Some web servers have modules to act as an http proxy server. It is recommended that such modules should not be installed as the web server can be misused as an open proxy if proper controls are not in place.

1.3 SPAM Prevention

Some websites contain online forms for forwarding links or documents on the website as mail. It is recommended that mail should not be allowed to any external e-mail addresses, as it can be used to SPAM external users.

3. Host Security

The default configurations in Operating System are typically set by vendors to emphasize features, functions, and ease rather than security. Thus, the first step in securing a Web server is to secure the underlying operating system as several security issues can be avoided if the operating systems is properly secured.

In the securing of a Host, the following should be considered:

- Include specific security requirements when selecting the Operating system of the web server.
    - Security certification level of the chosen platform
    - Level of support provided by the vendor.
    - Compatibility and support issue of the software's to be used on this platform.
    - Support of security features on the platform like authentication, levels of access control, support for remote administration and logging
- Minimize the Operating system with only essential services by removing all operating system and network services not required like Telnet, FTP, NetBIOS, NFS, NIS, etc. and unneeded protocols.
- Keep operating systems and applications software up to date with the latest service pack and patches to protect against common attacks.
- Configure computers for user authentication and remove all unneeded users and groups
- Configure computer operating systems with appropriate object, device, and file access controls
- Harden TCP/IP stacks.
- A strong password policy should be enforced.
- Enable detailed logging including failed logging etc.

The following guidelines are available for help in preparing a host as a Web Server.

Microsoft: Security Centre
http://www.microsoft.com/security/default.mspx

Microsoft: Windows Server 2003 Security Center
http://www.microsoft.com/technet/security/prodtech/win2003/default.mspx

Microsoft: Windows Server 2000 Security Center
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

NIST: windows 2000 security guideline
http://csrc.nist.gov/itsec/guidance_W2Kpro.html

CERT-In: Securing Red Hat Linux 9.0 as a Web Server
http://www.cert-in.org.in/guidelines/CISG-2004-01.pdf

CERT/CC:
http://www.cert.org/tech_tips/usc20_full.html

SUN: Security: Sun Blueprints Program and Sun Blueprints Online Magazine
http://wwws.sun.com/software/security/blueprints

4. Web and Application Server Security

4.1 Web Server Security

Web Server is a program that serves Web pages to Web browsers using the Hyper Text Transfer Protocol (HTTP). Some of the Web Server software contain middle-tier software that act as an application server. This enables users to perform high-level tasks, such as querying a database and delivering the output through the Web Server to the client browser as an HTML file.

In securing a Web Server, administrators should take care of the following

- Based on security needs, check for presence of specific security-related features on the chosen web server. It may include types of authentication, levels of access control, support for remote administration, and logging features.
- Install only the required features of the Application Servers and remove default features not being used.
- Install the latest version of the web server software along with the latest patches.
- Install web server software in a CHROOT cage.
- Remove all sample files, scripts, manuals and executable code from the web server application root directory.
- Remove all files that are not part of the Web site
- Reconfigure the HTTP Service banner so that Web server and Operating System type & version are not reported.
- Create a new custom least-privileged user and group for the Web Server process, unique from all other users and groups.
- Although the server may have to run as root or administrator initially to bind to port 80, the server should not run in this mode.
- The configuration files of the Web Server should be readable by Web Server process but not writable.
- The server should be configured in a manner so that web content files can be read but not written by Web service processes.
- Consider security implications before selecting programs, scripts, and plug-ins for the web server.
- Various Server Side Active Content Technologies are available viz. Java Servlets, ASP, ColdFusion, etc.. Each has its own strengths and weaknesses alongwith an associated risk. Thus the technology to be implemented on the Web server has to be chosen after due consideration.
- Third-party free modules available should not be used without proper checking and verification of their functionality and security.
- Configure the Web server to use authentication and encryption technologies (SSL), where required, along with a mechanism to check the latest CRL (certificate revocation list).

Available web / Application servers

Commercial

Microsoft Internet Information Server (IIS)	
SunOne web server	www.sun.com
IBM Websphere	www.ibm.com/software/info1/websphere/index.jsp
Bea Weblogic	www.bea.com

Open source

Apache	httpd.apache.org
Jakarta Tomcat	jakarta.apache.org

Reference

Microsoft: Internet Information Services (IIS) Security Centre
http://www.microsoft.com/technet/security/prodtech/iis/default.mspx

Apache: Apache Security Guidelines
http://httpd.apache.org/docs/misc/security_tips.html

CERT-In: web server security guideline
http://www.cert-in.org.in/guidelines/CISG200304.pdf

4.2 Secure Coding practices

Server side applications are written in various programming languages. However, flaws in the scripts may allow attackers to penetrate a Web server. Thus, the scripts need to be written with due consideration to security.

The following are some of the common secure coding practices.

- Consider security implications before selecting the scripting technology.
- Various client-side Active Content Technologies are available viz. Java applets, javascripts, vbscript, etc.. Each has its own strengths and weaknesses alongwith an associated risk. The technology to be implemented should be chosen after careful consideration.
- On Linux/Unix hosts, the code should not run with suid.
- The code should use explicit path names when invoking external programs and not rely on the PATH environment value
- Input data received through a web page form should be filtered for malicious input.
- Encryption mechanism should be deployed to encrypt passwords.

Common security issues to be considered

- **SQL Injection**

  Many web pages accept parameters from web user, and generate SQL queries to the database. SQL Injection is a trick to inject SQL script/command as an input through the web front-end.

To avoid SQL Injection, filter out characters like single quote, double quote, slash, back-slash, semi colon, extended characters like NULL, carry return, new line, etc, and reserved SQL keywords like ‘Select’, ‘Delete’, ‘Union’ etc in all strings from:

- Input from users
- Parameters from URL
- Values from cookie

- **Cross site scripting**

  Cross-site Scripting (commonly referred as XSS) is an attack technique that forces a web site to echo attacker-supplied executable code, which loads in a user’s browser.

  When an attacker gets a user’s browser to execute his code, the browser will run the code and the attacker gets the ability to read, modify and transmit any sensitive data accessible by the browser. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site.

- **Information Leakage**

  Information Leakage occurs when a web site reveals sensitive data, such as developer comments or error messages, which may aid an attacker in exploiting the system. Sensitive information may be present within HTML comments, error messages, or source code left on the server.

Details regarding the above mentioned issues, related threats and countermeasures can be found at:

Open Web Application Security Project:
A Guide To Building Secure Web Applications
http://www.owasp.org/documentation/guide

Microsoft: Writing secure code
By Michael Howard and David LeBlanc, Publisher: Microsoft WP publisher

Microsoft: Improving Web Application Security
http://www.cgisecurity.com/lib/Threats_Countermeasures.pdf

Web Application Security Consortium:
Web Application Security Consortium: Threat Classification
http://www.webappsec.org/threat.html

Microsoft:
MSDN : Design Guidelines for Secure Web Applications
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/THCMCh04.asp

4.3 Database Security

A database is installed as a back-end server component to serve a web application through the use of query language, typically SQL. Database security should be in place to ensure data access only to authorized users and protect the data. The following should be considered for securing a database system.

- Stay updated with latest Service Packs and Patches.
- Remove unnecessary services and protocols.
- Depending on importance of data, consider encryption.
- Secure the database server behind a firewall and use IDS to detect any intrusion attempts.
- The database server process should run as a user with minimum privileges and never as administrator.
- Enforce a strict access control policy.
- Enforce secure coding practices for application developers.
- Audit trail logs on the database servers should be enabled.
- Some Database Servers include Web Applications servers by default. It is recommended that they be removed, if not required.
- Database users not required should be removed.
- The database server should not be assigned publicly accessible IP, and access to the database should be allowed only from the Web Server on a particular port only.
- Depending upon importance of data, fine grained record/row level auditing should be considered.

Reference

Microsoft: SQL Server Security Center
http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

Microsoft: SQL Best Practices Analyzer
http://www.microsoft.com/downloads/details.aspx?FamilyID=b352eb1f-d3ca-44ee-893e-9e07339c1f22&displaylang=en

CISecurity: Oracle Security Testing tools and guide
www.cisecurity.com

Others
http://www.petefinnigan.com
http://www.appsecinc.com

5. Content Management

Use of remote authoring tools for editing content directly on public Web site is not recommended.

- It is recommended that administration of the server be done on the console itself. However, if remote administration is required, configure computers for remote administration through a secure channel.
- Configure web content uploading through a secure communication channel e.g. SSH and should be configured for low session time-outs, and account lockouts.
- Management clients used for content management should be placed in a screened network zone with limited access.
- Management clients should be hardened and patched with latest OS updates.
- Contents uploaded on the Web Server should be verified to ensure that it is free of any malicious content.

6. Logging and Backup

Logging is a crucial component of security of a Web server. Monitoring and analyzing logs are critical activities as log files are often the best and/or only record of suspicious behavior. In setting up logging and backup mechanisms the following should be considered.

Logging

- Use a centralized Syslog server
- Alert mechanism to alert administrator in case of any malicious activity detected in logs.
- Use the Combined Log Format for storing the transfer Log .
- Establish different log file names for different virtual Web sites that may be implemented as part of a single physical Web server.
- Use the Remote User Identity as specified in RFC 1413.
- Ensure procedures are in place so that log files do not fill up the hard drive.
- Ensure log files are regularly archived, secured and analyzed

Backup

- A proper backup policy should be enforced and ensure regular backup of files.
- Maintain a latest copy of Web site content on a secure host or on media.
- Maintain integrity check of all important files in the system. This can be done by either generating md5 hashes of important files or by using software integrity checkers like tripwire.

Reference:

CERT-In : Implementing Central Logging Server using syslog-ng
http://www.cert-in.org.in/syslog.htm

7. Physical Security

Proper physical and environmental security controls should be in place to protect the hosting system resources. Physical security controls protect against physical damage, unauthorized disclosure of information, theft and loss of control over system integrity.

Natural calamity threats

Care should be taken to mitigate the affects of different threats including natural calamities.

Physical Access Controls

Proper access control mechanism may be deployed to restrict physical access to the servers. Biometric access controls can be deployed for this purpose.

Except for designated administrators, no one else should be allowed to log on to the server locally on the console.

Electromagnetic shielding

Electro-magnetic radiations emanating from the Computer servers may result in data theft. The electromagnetic shielding of the Server room may be done to protect against it.

Disaster recovery centre

Depending on the criticality, a replica of the entire server infrastructure should also be created at a different physical location to recover from any disaster. For critical websites, disaster recovery site should be in a state of readiness to take over web services, when required.

Reference

TEMPEST (Transient Electromagnetic Pulse Emanation Standard) is a U.S. government code word that identifies a classified set of standards for limiting electric or electromagnetic radiation emanations from electronic equipment.

http://www.eskimo.com/~joelm/tempestintro.html#What%20is

8. Security Audit/Penetration Testing

A security audit compares current security practices against a set of defined standards

Vulnerability assessment is a study to locate security vulnerabilities and identify corrective actions.

A penetration test is a real life test of an organization's exposure to security threats and is performed to uncover the security weakness of a system.

Organization should carry out the above tests regularly and also have it verified by empanelled third party Information Security Auditors and Attack & Penetration (A&P) Testing experts.

8.1 Available Tools

Benchmarking / Auditing

Various benchmarking /auditing tools are available to verify the security configuration of servers and applications.

CISecurity: www.cisecurity.com

Windows	benchmarking tool
Solaris	benchmarking tool
Linux	benchmarking tool
HP-UX	benchmarking tool
CISCO router	benchmarking tool
Oracle	benchmarking tool

Microsoft windows best practice analyzer
SQL best practice analyzer

Web applications stress testing

http://wpoison.sourceforge.net/

Vulnerability scanners

Web servers should be scanned periodically for vulnerabilities. There are several automated tools that specifically scan for Operating System and application server for vulnerabilities. The vulnerabilities detected by the scanner should be verified and the vulnerabilities removed by applying patches/upgrades or workarounds.

Commercial
- Retina
- Shadow security Scanner
- GFI scanner

Open source
- Nessus
- Nikto

A list of various security testing tools can referenced from -

CERT-In:
http://www.cert-in.org.in/securitytools.htm
http://www.cert-in.org.in/presentation/27thfeb03/perimetersecurity.pdf

Insecure.org:
http://www.insecure.org/tools.html

9. Security Policy

A security policy defines the rules that regulate how an organization manages and protects computing resources to achieve security objectives.

The security policy of an organization should specifically incorporate security requirements of web servers. The web server security policy should incorporate -

- Network and host security policy
- Web Server backup and logging policy.
- Web server administration and Updation policy
- Classification of documents to be published on Web Server
- Password management policy
- Encryption policy
- Physical security

CERT-In Security Guidelines CISG-2003-02
http://www.cert-in.org.in/guidelines/CISG200302.pdf

NIST: SP 800-18: Guide for Developing Security Plans for Information Technology Systems
http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF

10. Incident Handling and Recovery

A computer security incident is any real or suspected adverse event in relation to the security of computer systems or networks. It is an act of violating explicit or implied security policy resulting in, unauthorized access, denial of service/disruption, and unauthorized use of a system for processing or storage of data or changes to system software, hardware, firmware characteristics without the owner's knowledge.

Create a formal policy for Incident handling. A Computer Security Incident Response Team (CSIRT) should be created within the organization to handle incidents through the following six stages of Incident handling

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up

Incident reporting

Follow your site-specific policies related to detecting signs of intrusion and attack. In case of web defacement unplug the system immediately from the network. Report the incident to the organization's designated point of contact and to CERT-In HelpDesk.

India Computer Emergency Response team

The Indian Computer Emergency Response Team (CERT-In) has been established by the Department of Information Technology to be a part of the international CERT community. It has a mandate to respond to computer security incidents reported by the entire computer and networking community in the country along with creating security awareness among the Indian cyber-community.

CERT-In Incident reporting form:
http://www.cert-in.org.in/incidentreport.htm

Further references on Incident Handling

CERT/CC: Handbook for Computer Security Incident Response Teams (CSIRTs)
http://www.cert.org/archive/pdf/csirt-handbook.pdf

NIST: Computer Security Incident Handling Guide
http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61-pdf.zip

CHIHT - Clearing House for Incident Handling Tools
http://chiht.dfn-cert.de/

CERT/CC: Detecting Signs of Intrusion
http://www.cert.org/security-improvement/modules/m09.html

11. Third party hosting

An organization may not have the required infrastructure and expertise and therefore can use a third party organization to host the Web site. The organization can use co-locate their own servers in the service provider's network or directly host on the servers of the service provider itself.

The advantages of third party hosting are

- The service provider may have greater knowledge in securing and protecting Web servers.
- The network can be optimized solely for the support and protection of Web servers.
- DoS attacks aimed at the Web server shall have no effect on the organization's production network.
- Compromise of the Web server does not directly threaten the organization's network.

Disadvantages of third party hosting are

- It requires trusting a third-party with Web server content.
- It is difficult to remotely administer/update Web server.
- There is little control on the security of the Web server.

- The Web server may be affected by attacks aimed at other Web servers hosted by the service provider on the same network.

In selecting a third party hosting organization, a user should keep the following in view.

- Hosting servers should be located in India.
- Hosting organization should have a security policy and should implement the best practices for the websites as per this document
- Hosting organization should have its infrastructure and Web servers audited by auditors empanelled by CERT-In. Hosting organization should also have their web servers tested by A&P testing experts periodically and should take immediate steps to plug the security weakness unearthed.

12. Web server security Thumb rules

- Web administrators should be adequately skilled.
- Use software only from trusted source.
- Keep all software updated.
- IS Security audit and A&P test should be carried out regularly.
- A dedicated machine should be used as a Web server.
- Changes to configuration should be documented (revision control program)
- Central syslog server should be used.
- Encryption should be used.

13. References

CERT-In:	www.cert-in.org.in
CERT/CC:	www.cert.org
US-CERT:	www.us-cert.gov
NIST:	www.nist.gov
SANS:	www.sans.org
OWASP:	www.owasp.org
W3C	www.w3.org/Security/Faq/

Appendix A: Abbreviations

ACL	Access Control List
ASP	Active Server Pages
A&P	Attack & Penetration
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CLF	Common Log Format
CRL	Certificate Revocation List
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial Of Service
DMZ	De-Militarized Zone
DNS	Domain Name System
DoS	Denial of Service
ELF	Extended Log Format
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IP	Internet Protocol
IS	Information Security
IPS	Intrusion Prevention Systems
ISP	Internet Service Provider
LAN	local area network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NFS	Network File Server
NIS	Network Information Service
NTP	Network Time Protocol
RPC	Remote Procedure Call
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WWW	World Wide Web