12.1.2 Web Server Hacking Facts

A web server is a system used to store and distribute web pages to clients. In addition, a web server can gather information from a user that is critical for e-commerce or used to access web pages that require access credentials.

This lesson covers the following topics:

- Web server
- Internet Information Services
- Apache web server
- Vulnerabilities

Web Server

A web server is a system used to store and distribute web pages to clients. A client uses a web browser to request access to a web page. The browser sends a request to the web server to open a TCP connection. Once the TCP handshake has been established, the server waits for an HTTP request from the client. This request tells the server the web page that is being requested. The following table describes the request/response sequence.

HTTP Request/Response	Description
GET	Requests specific information from the web server.
HEAD	Requests information from the web server, but transfers only the status line and the header section.
POST	Requests that the web server send data using HTML forms.
TRACE	Performs a loopback test to target the resource.
CONNECT	Establishes a communication tunnel to the web server.

The server searches through its inventory of pages and sends a response back to the client along with the web page, if available. The following table describes HTTP response messages.

HTTP Response Message	Description
1xx: Informational	Request has been received; process continuing.
2xx: Success	Action was received, understood, and accepted.
3xx: Redirection	Additional action needs to be taken to complete the request.
4xx: Client Error	Request included a bad syntax or other error and cannot be completed.
5xx: Server Error	The server did not complete the request.

Internet Information Services

Internet Information Services (IIS) is the web server application designed by Microsoft for the Windows environment. IIS can be used to support most web hosting and supports HTTP, HTTPS, FTP, SMTP, and other protocols. In addition to the core functionalities of email, data transmission, and web page support, IIS provides various modules. These modules include process management, server-side-language, legacy support, protocol listeners, security support, certificate support, authentication support, and database support.

Apache Web Server

Apache web server is open source and is the most widely used web server technology. Although originally designed for use on the Unix platform, support has been expanded to other operating systems. Similar to Microsoft, Apache has add-on modules that provide additional functionality. These modules include authentication, SSL support, proxy support, PHP, HTTP request filtering, intrusion detection, compression support, and enhanced logging.

Vulnerabilities

Security professionals spend a lot of time securing, locking, and restricting access to network resources. Servers and routers are locked behind closed doors. Desktops, laptops, and servers are limited to authorized personnel only. Interestingly enough, similar to a brightly lit, welcoming storefront, web servers are a beacon to users across the globe – an entrance to a network that users are encouraged to enter into, browse, and get comfortable with. This accessible, user-friendly point of connection to the customer is necessary for e-commerce. Given the sensitivity of the content that is being stored on those servers – account numbers, contact information, credit card numbers, and the potential access to a larger network – web servers are notable targets for attackers.

Basic security measures, such as default passwords, remote administrative functions, and removal of unnecessary services, are often overlooked on web servers. Additionally, error reporting, debug logging, and SSL certificates are frequently exploited. This is usually due to configuration errors. Web servers should be a special area of focus to strengthen security.

The following table describes vulnerabilities of web servers.

Vulnerability	Description
Certificates	Self-signed certificates and default certificates are used.
Debugging	Debugging features are enabled and accessible via the web servers.
Software errors	Errors in server software, encryption, and operating system are not fixed. Software is not updated.
Default accounts	Default accounts or passwords are used for hardware or software.
Permissions	File and directory permissions are not properly assigned.
Unused services	Unused services are enabled. These could include remote administration or content management.
Misconfigurations	Misconfigurations in web server, operating systems, networks, SSL certificates, or encryption settings are not tested for and corrected.