

1. Describe how a web page is requested and displayed. Discuss how browsers, clients and servers are used in this process.
 - a. The web browser forms a connection to a web server, requests a page and receives it. In a more detailed explanation: the browser communicates with a name server to translate the server name into an IP address, which it uses to connect to the server machine. The browser will then form a connection to the server at that IP address on port 80. Following the HTTP protocol, the browser sent a GET request to the server, asking for the file. The server then sent the HTML text for the web page to the browser on the client machine.
2. What is an URL, what are its parts, and how does it relate to web servers? Provide an example and describe each part.
 - a. A URL is the address of a given unique resource on the web. Such resources can be an HTML page, a CSS document, an image, etc. A URL consists of the scheme, domain name, port, path to file, parameters, and an anchor.

Scheme	indicates the protocol that the browser must use to request the resource.
Authority	is separated from the scheme by <code>://</code> . It includes the domain name and the port.
Domain	indicates which web server is being requested. An IP address can also be used.
Port	The port indicates the technical "gate" used to access the resources on the web server.
Path to resource	is the path to the resource on the web server.
Parameters	are a list of key/value pairs seperated with the <code>&</code> symbol. The web server can use those parameters to do extra stuff before returning the resource.
Anchor	Represents a sort of bookmark inside

	the resource, giving the browser the directions to show the content located at that "bookmarked" spot.
--	--

3. Explain what HTTP is.
 - a. HTTP is a protocol for fetching resources such as HTML documents. It is the foundation of any data exchange on the Web and it is a client-server protocol, which means requests are initiated by the recipient, usually the web browser.
4. Describe 2 security issues surrounding web servers
 - a. If the server machine accepts connections on a port from the outside world, and if a firewall is not protecting the port, you can connect to the port from anywhere on the Internet and use the service.
 - b. DOS attacks: A denial of service attack. The attackers overwhelm the web server with web requests in such a way that deters legitimate users from accessing the service by affecting the ability of the server to respond in a timely manner. This is achieved by the attacker transmitting an excessive number of known invalid requests.
 - c. SQL injection vulnerabilities: A website contains input fields and forms in their front end applications to facilitate the interactive processes with the user. These input data fields/forms are used to pass data through SQL queries to access and query the database. In the event that these data input fields are not validated, attackers can use the vulnerability to pass malicious scripts to query the database in an SQL Injection attack.

URLs:

- <http://www.howstuffworks.com/web-server.htm>
- https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_URL
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview>
- <https://study.com/academy/lesson/vulnerabilities-issues-in-web-servers.html>
-