Chapter 2:

HTTP is the core communications protocol used by web applications. HTTP is a message-based model, client sends request message and the server returns a response message. Essentially connectionless but uses stateful TCP as its transport mechanism. Each exchange of request and response is an autonomous transaction and may use a different TCP connection. HTTP version 1.0 and 1.1 are the most used, the only difference between them is that 1.1 the `Host` request header is mandatory.

Attacking web applications mostly use `GET` and `POST`. The `GET` method retrieves resources, it can be used to send parameters to the requested resource in the URL query string. URLs are displayed on screen and are logged in multiple places. Because of this the query string should be used to transmit any sensitive data.

The `POST` method is used to perform actions. Request parameters can be sent in both the URL query string and in the body of the message. Browsers do not automatically reissue `POST` requests made by users, because it might cause an action to be performed more than once.

Other methods supported by HTTP include:

- `HEAD` same as `GET` except the server should not return a message body in its response. Can be used to check whether a resource is available before making a `GET` request.
- `TRACE` is designed for diagnostic purposes. Server returns the contents of the request message in the body of the response. Can be used to detect the effect of any proxy servers between the client and the server that manipulate the request.
- `OPTIONS` asks the server to report the HTTP methods that are available for a particular resource.
- `PUT` attempts to upload the specified resource to the server, using the content contained in the body of the request. If this method is enabled, you may e able to use this to attack the application by uploading arbitrary script and executing it on the server.

Uniform resource locator (URL) is a unique identifier for a web resource through which that resource can be retrieved. Format of most URLs is as follows:
`protocol://hostname[:port]/[path/]file[?param=value]`
Port number is usually included only if it differs from the default used by the relevant protocol.

Representational state transfer (REST) is a style of architecture for distributed systems where requests and responses contain representations of the current state of the system's resources. URLs containing parameters within the query string do conform to REST constraints, however the term "REST-style URL" is often used to signify a URL that contains its parameterswithin the URL file path.
URL query string:
`http://wahh-app.com/search?make=ford&model=pinto`
REST-style parameters:
`http://wahh-app.com/search/ford/pinto`
These different parameter styles can be used to map an application's content and functionality and identify its key attack surface.