Web Application Security

Rajendra Kachhwaha
rajendra1983@gmail.com

July 20, 2015

Outline

What is a Web Application & its different types.

1. A web application is a program that runs in a web browser. It is created in a browser-supported programming language (JavaScript,HTML,CSS etc.) and relies on a web browser to render the application.
2. Web applications can be considered as a specific variant of client-server software where the client software is downloaded to the client machine when visiting the relevant web page, using standard procedures such as HTTP.
3. In the early days of the Web each individual web page was delivered to the client as a static document.
4. In 1995, Netscape introduced a client-side scripting language called JavaScript allowing programmers to add some dynamic elements to the user interface that ran on the client side.

What is a Web Application & its different types.

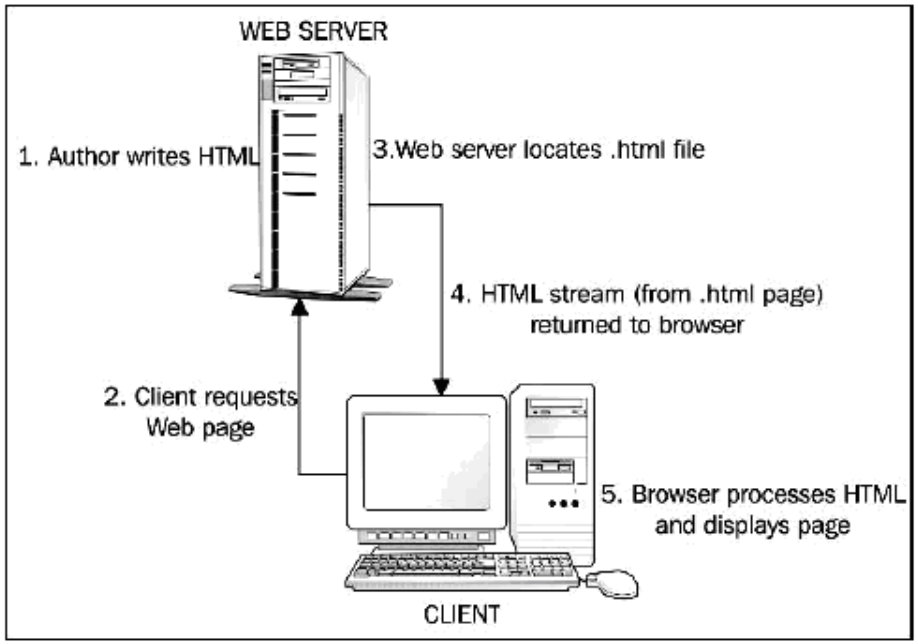
5. In 1996, Macromedia introduced Flash, a vector animation player that could be added to browsers as a plug-in to embed animations on the web pages.
6. In 1999, the "web application" concept was introduced in the Java language in the Servlet.
7. In 2005, the term "Ajax" was coined, and applications like Gmail started to make their client sides more and more interactive. A web page script is able to contact the server for storing/retrieving data without downloading an entire web page.
8. In 2011, HTML5 was finalized, which provides graphic and multimedia capabilities without the need of client side plug-ins.

What is a Web Application & its different types.

A Web application can be categorized in following two types based on the types of web pages.

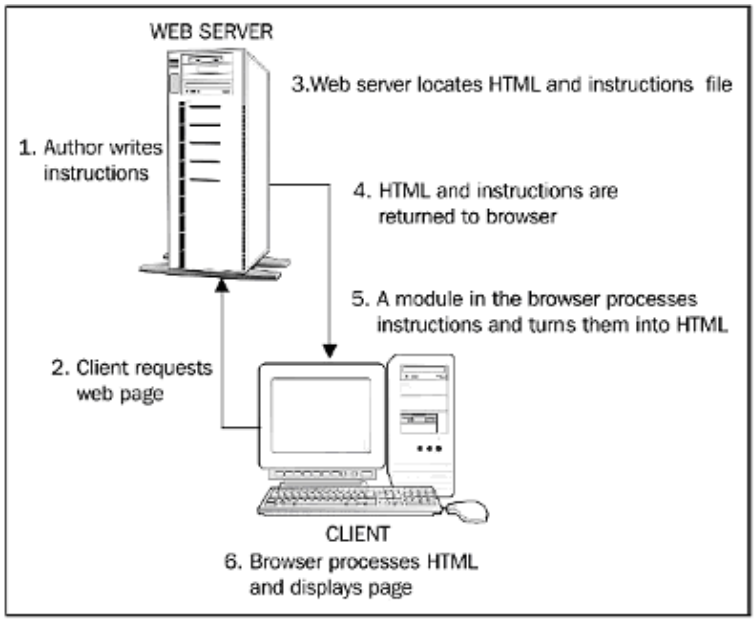
1. Static Web Application.
2. Dynamic Web Application

Static Web Application:

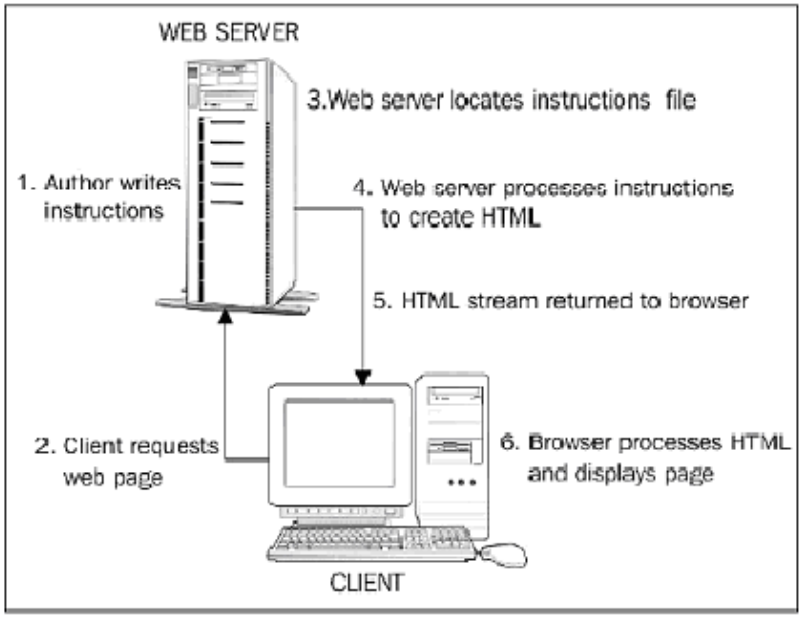


What is a Web Application & its different types.

Dynamic Web Application: A dynamic web page is a kind of web page that has been prepared with fresh information, for each individual viewing. It is not static because it changes with time, the user, the user interaction.



Client Side Dynamic Web Page



Server Side Dynamic Web Page

Web Functionality

In addition to the core communications protocol used to send messages between client and server, web applications employ numerous technologies to deliver their functionality. Any reasonably functional application may employ dozens of distinct technologies within its server and client components.

Server-Side Functionality:

1. Scripting languages such as PHP, VBScript, and Perl
2. Web application platforms such as ASP.NET and Java
3. Web servers such as IIS, Apache, and Netscape Enterprise
4. Databases such as MS-SQL, Oracle, and MySQL
5. Other back-end components such as SOA-based web services

Web Functionality.

Client-Side Functionality:

1. HTML (Hypertext Markup Language)
2. CSS (Cascading Style Sheets)
3. JavaScript
4. VBScript
5. DOM (Document Object Model)
6. AJAX (Asynchronous JavaScript and XML)
7. JSON (JavaScript Object Notation)

Web Functionality.

Session: A web application must maintain a set of stateful data generated by the users actions across several requests. This data normally is held within a server-side structure called a session.
State: In some applications, state information is stored on the client component rather than the server. The current set of data is passed to the client in each server response and is sent back to the server in each client request. The ASP.NET platform makes use of a hidden form field called **ViewState** to store state information about the users web interface.

Description of HTTP

Hypertext transfer protocol (HTTP) is the core communications protocol used to access the World Wide Web. Originally developed for retrieving static text-based resources & extended to support the complex distributed applications. HTTP uses a message-based model in which a client sends a request message and the server returns a response message.

HTTP Request:

```
GET /auth/488/YourDetails.ashx?uid=129 HTTP/1.1
Accept: application/x-ms-application, image/jpeg, application/xaml+xml,
image/gif, image/pjpeg, application/x-ms-xbap, application/x-shockwave-
flash, */*
Referer: https://mdsec.net/auth/488/Home.ashx
Accept-Language: en-GB
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; .NET4.0C; InfoPath.3; .NET4.0E; FDM; .NET CLR 1.1.4322)
Accept-Encoding: gzip, deflate
Host: mdsec.net
Connection: Keep-Alive
Cookie: SessionId=5B70C71F3FD4968935CDB6682E545476
```

Description of HTTP

HTTP Response:

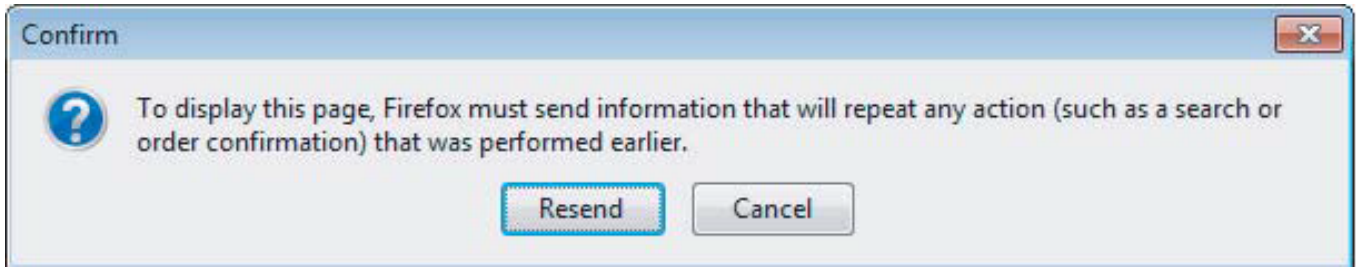
```
HTTP/1.1 200 OK
Date: Tue, 19 Apr 2011 09:23:32 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Set-Cookie: tracking=tI8rk7joMx44S2Uu85nSWc
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1067

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://
www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://
www.w3.org/1999/xhtml" ><head><title>Your details</title>
...
```

Description of HTTP

HTTP Methods:

1. **GET:**Designed to retrieve resources. It can be used to send parameters to the requested resource in the URL query string.
2. **POST:** Designed to perform actions.



3. **PUT:** It attempts to upload the specified resource to the server, using the content contained in the body of the request.

Description of HTTP

URL: A uniform resource locator (URL) is a unique identifier for a web resource through which that resource can be retrieved. The format of most URLs is as follows:

```
protocol://hostname[:port]/[path/]file[?param=value]

https://mdsec.net/auth/488/YourDetails.ashx?uid=129
```

Cookies: The cookie mechanism enables the server to send items of data to the client, which the client stores and resubmits to the server.

Description of HTTP

Status Codes: Each HTTP response message must contain a status code in its first line, indicating the result of the request.

1. 1xx Informational.
2. 2xx The request was successful.
3. 3xx The client is redirected to a different resource.
4. 4xx The request contains an error of some kind.
5. 5xx The server encountered an error fulfilling the request.

200	OK
201	Created
301	Moved Permanently
302	Found
304	Not Modified

400	Bad Request
401	Unauthorized
404	Not Found
500	Internal Server Error
503	Service Unavailable