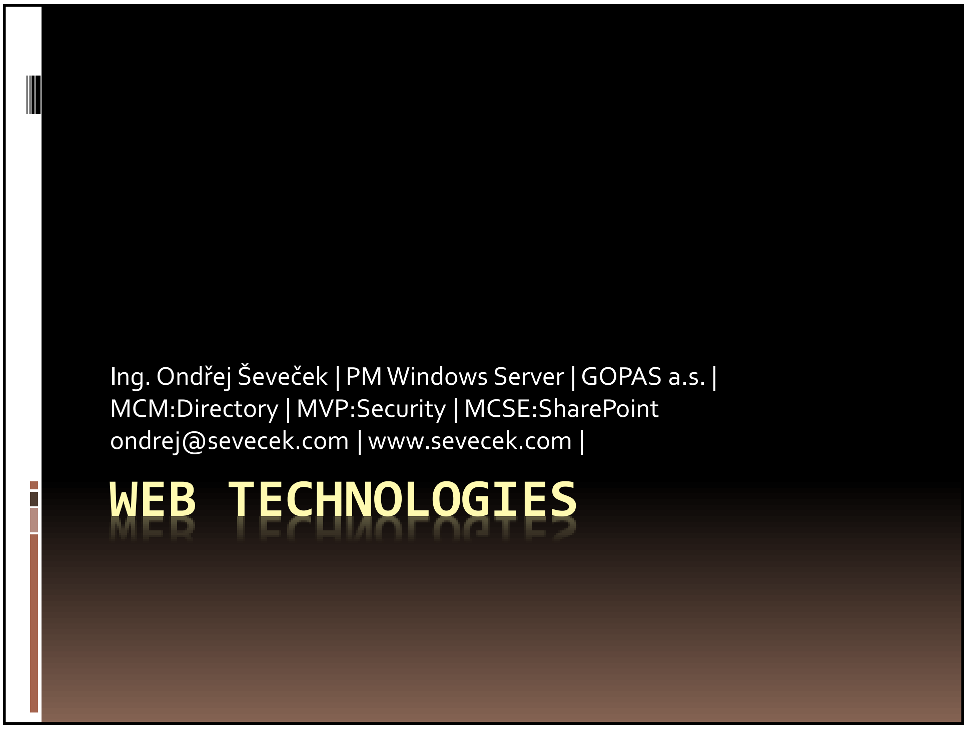
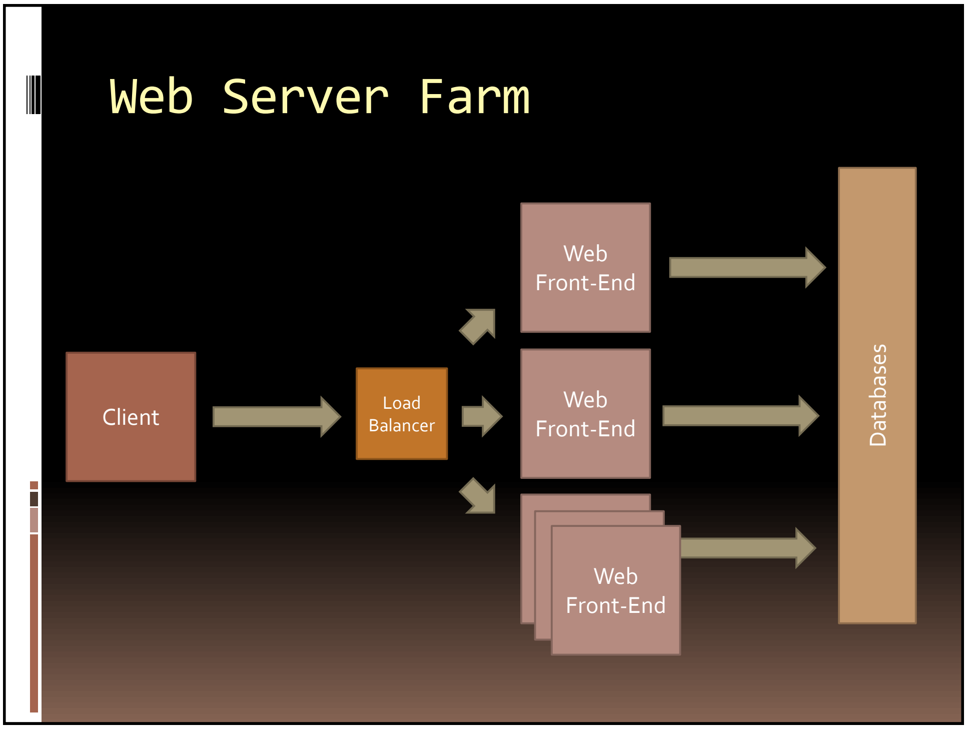


Ing. Ondřej Ševeček | PM Windows Server | GOPAS a.s. |
MCM:Directory | MVP:Security | MCSE:SharePoint
ondrej@sevecek.com | www.sevecek.com |

WEB TECHNOLOGIES

SharePoint Designer for Business Analysts

WEB TECHNOLOGIES



Web Server Farm

Client

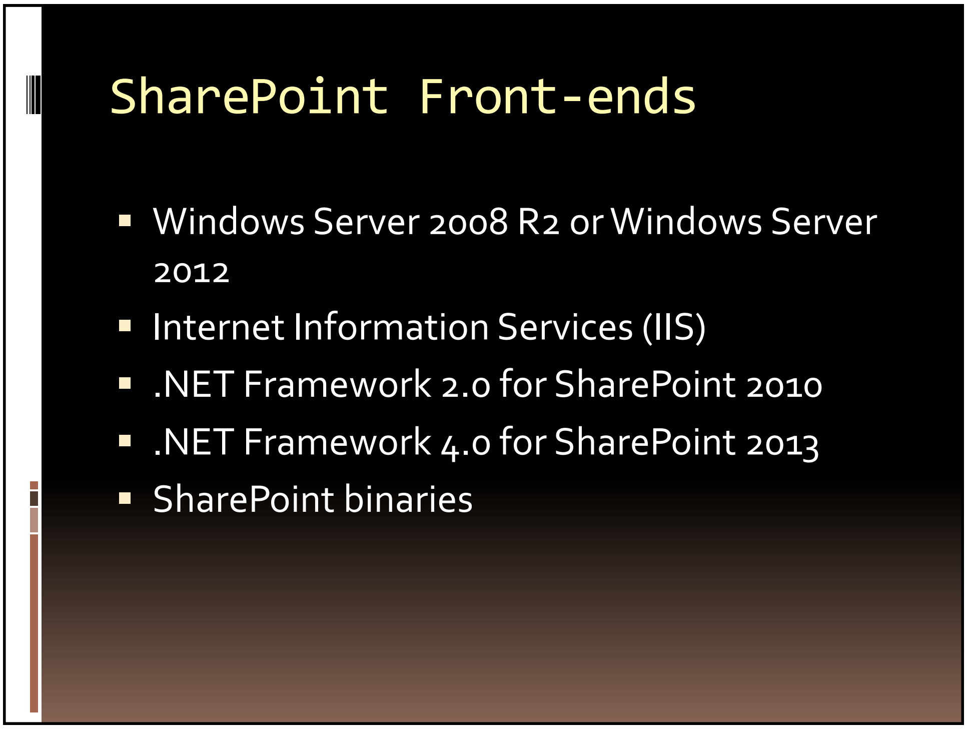
Load Balancer

Web Front-End

Web Front-End

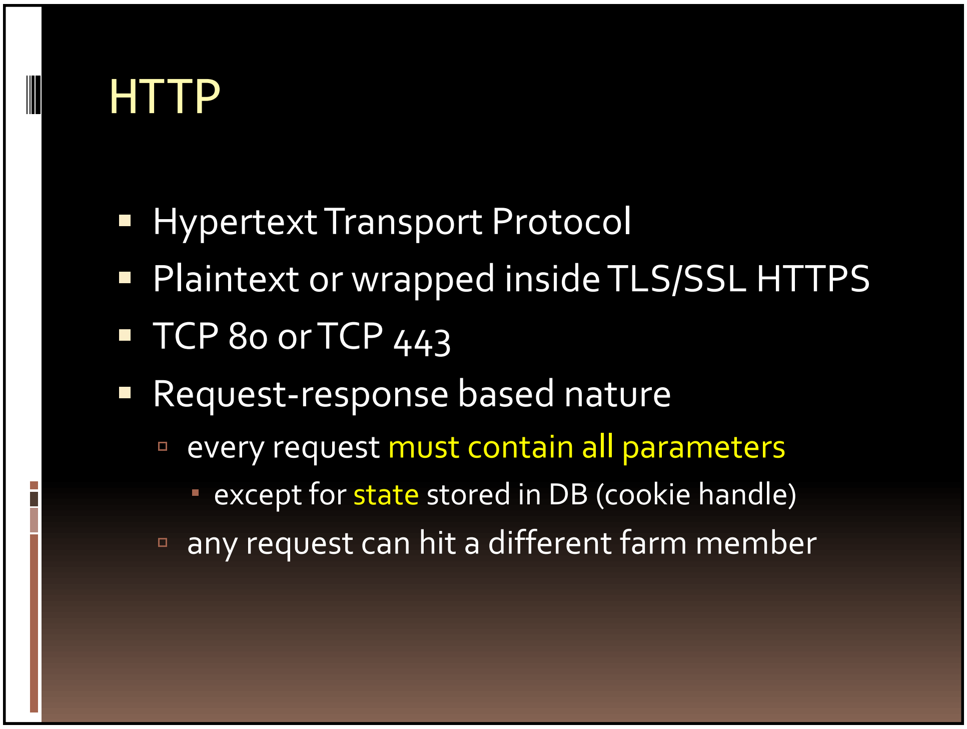
Web Front-End

Databases



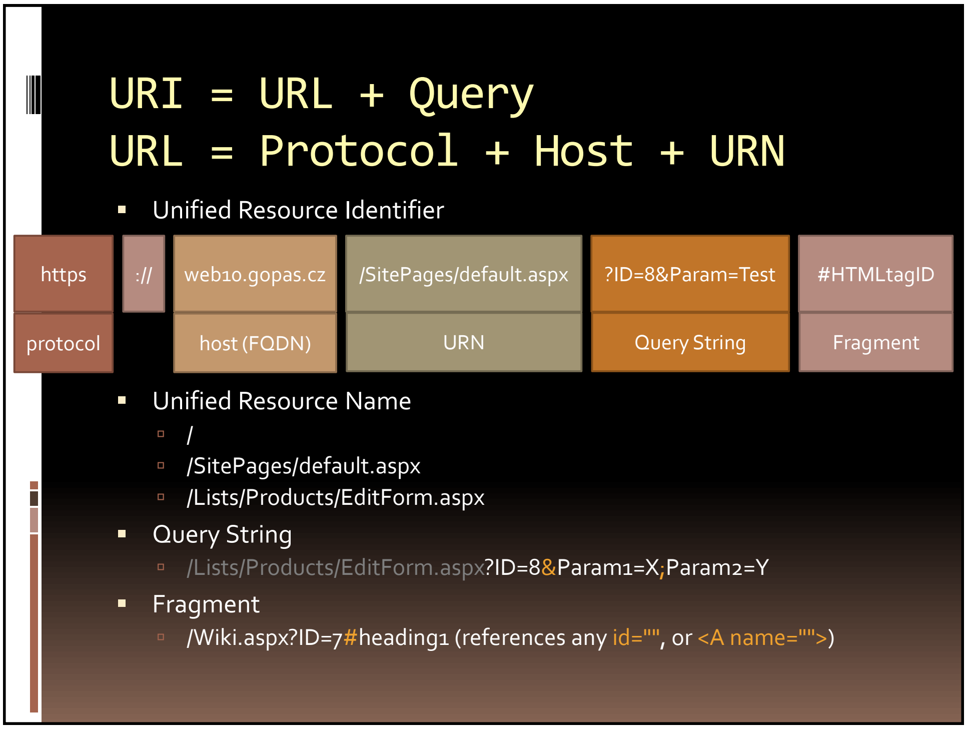
SharePoint Front-ends

- Windows Server 2008 R2 or Windows Server 2012
- Internet Information Services (IIS)
- .NET Framework 2.0 for SharePoint 2010
- .NET Framework 4.0 for SharePoint 2013
- SharePoint binaries



HTTP

- Hypertext Transport Protocol
- Plaintext or wrapped inside TLS/SSL HTTPS
- TCP 80 or TCP 443
- Request-response based nature
  - every request must contain all parameters
    - except for state stored in DB (cookie handle)
  - any request can hit a different farm member

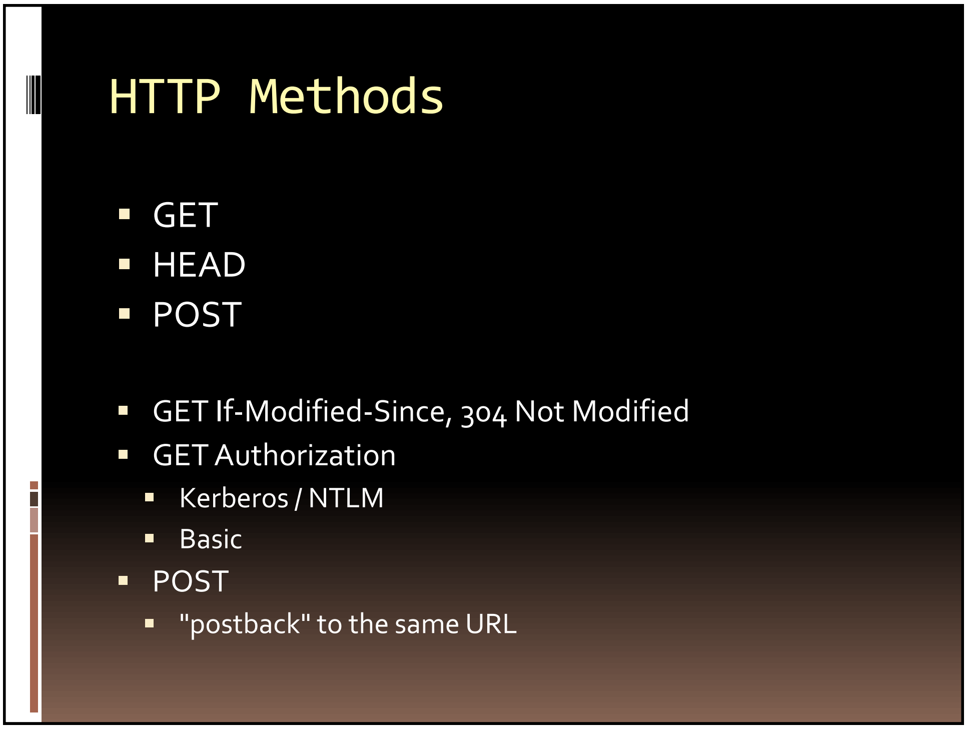


URI = URL + Query
URL = Protocol + Host + URN

- Unified Resource Identifier

https	://	web10.gopas.cz	/SitePages/default.aspx	?ID=8&Param=Test	#HTMLtagID
protocol		host (FQDN)	URN	Query String	Fragment

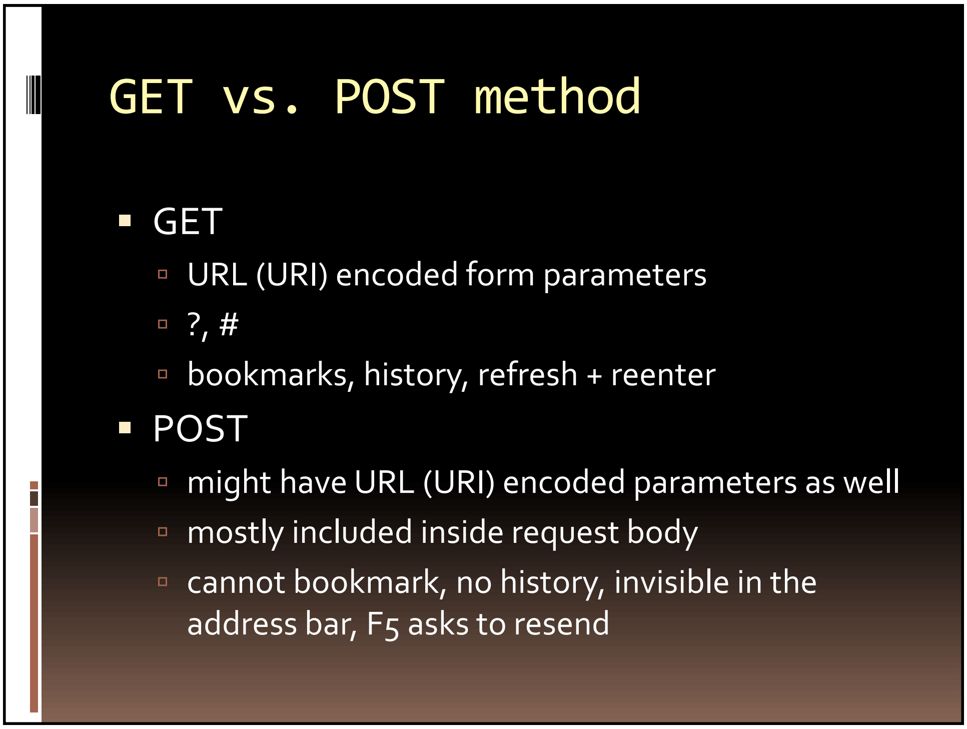
- Unified Resource Name
  - /
  - /SitePages/default.aspx
  - /Lists/Products/EditForm.aspx
- Query String
  - /Lists/Products/EditForm.aspx?ID=8&Param1=X;Param2=Y
- Fragment
  - /Wiki.aspx?ID=7#heading1 (references any id="", or <A name="">)



HTTP Methods

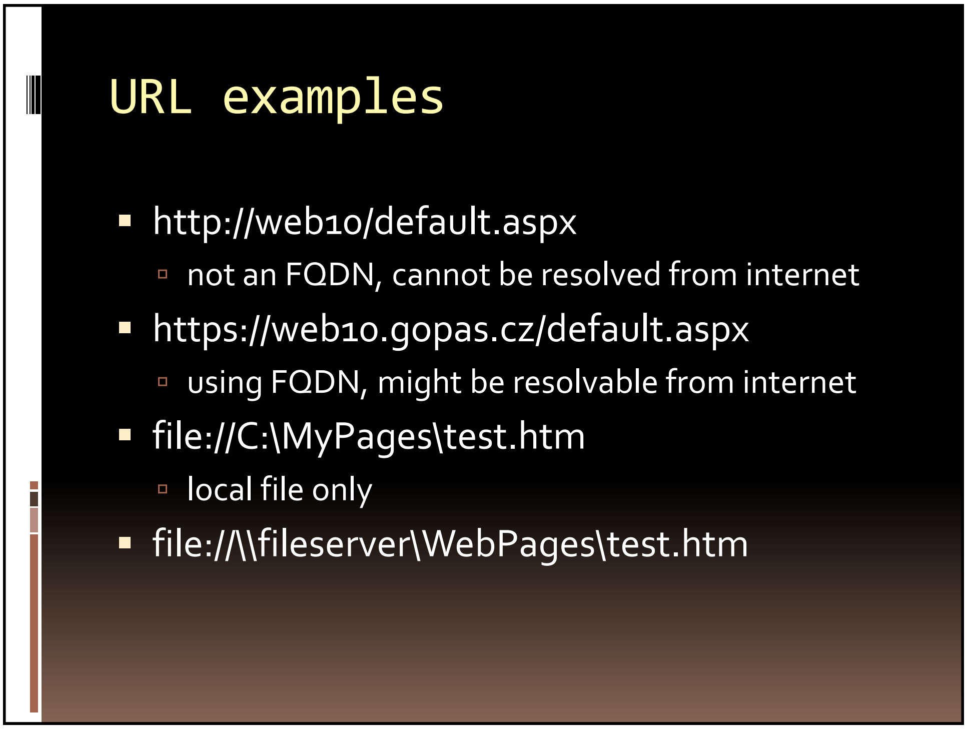
- GET
- HEAD
- POST

- GET If-Modified-Since, 304 Not Modified
- GET Authorization
  - Kerberos / NTLM
  - Basic
- POST
  - "postback" to the same URL



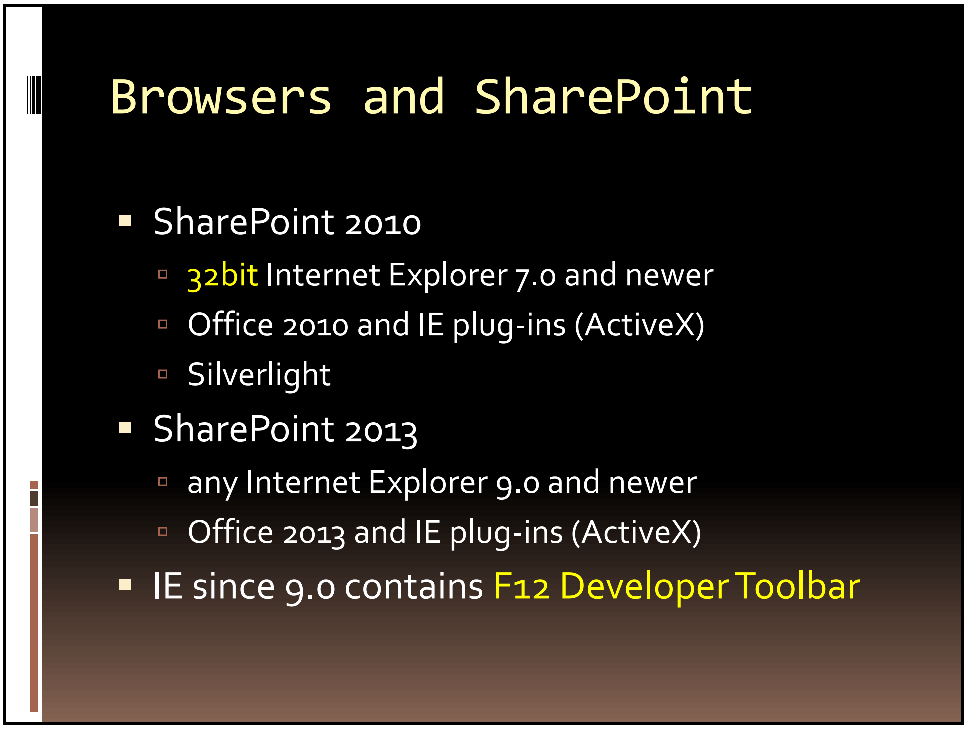
GET vs. POST method

- GET
  - URL (URI) encoded form parameters
  - ?, #
  - bookmarks, history, refresh + reenter
- POST
  - might have URL (URI) encoded parameters as well
  - mostly included inside request body
  - cannot bookmark, no history, invisible in the address bar, F5 asks to resend



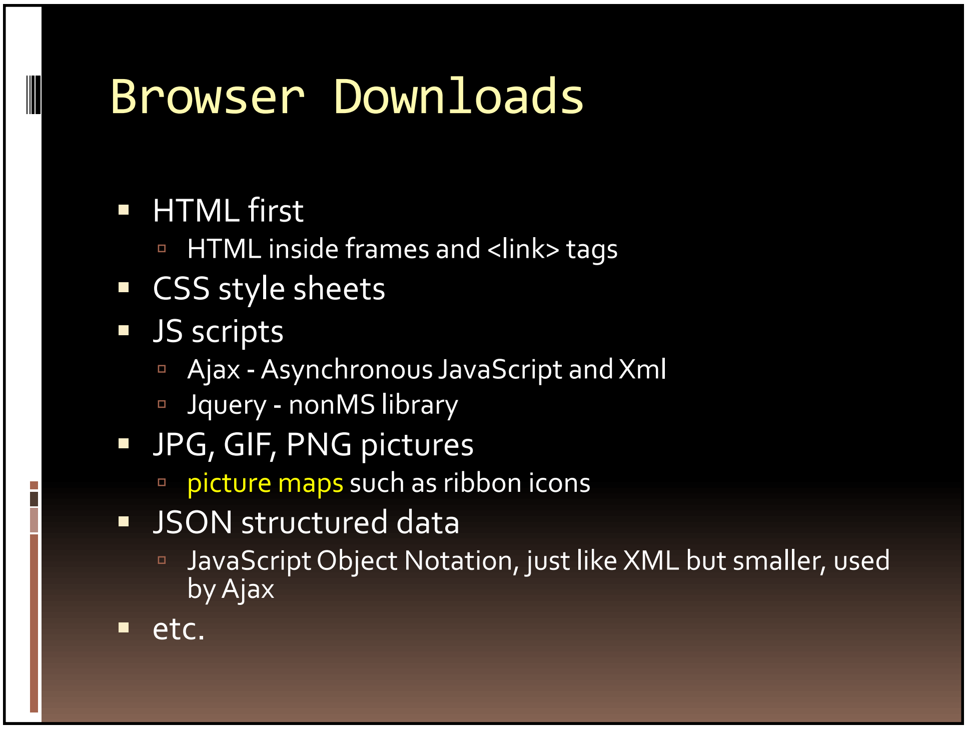
URL examples

- http://web10/default.aspx
  - not an FQDN, cannot be resolved from internet
- https://web10.gopas.cz/default.aspx
  - using FQDN, might be resolvable from internet
- file://C:\MyPages\test.htm
  - local file only
- file://\\fileserver\WebPages\test.htm



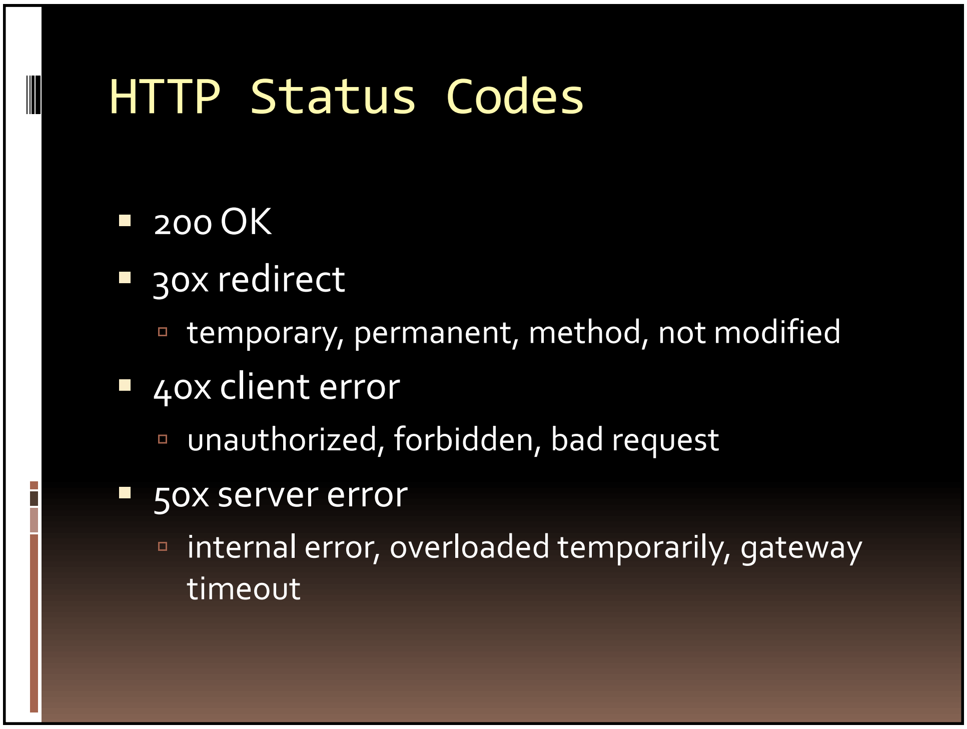
Browsers and SharePoint

- SharePoint 2010
  - 32bit Internet Explorer 7.0 and newer
  - Office 2010 and IE plug-ins (ActiveX)
  - Silverlight
- SharePoint 2013
  - any Internet Explorer 9.0 and newer
  - Office 2013 and IE plug-ins (ActiveX)
- IE since 9.0 contains F12 Developer Toolbar



Browser Downloads

- HTML first
  - HTML inside frames and <link> tags
- CSS style sheets
- JS scripts
  - Ajax - Asynchronous JavaScript and Xml
  - Jquery - nonMS library
- JPG, GIF, PNG pictures
  - picture maps such as ribbon icons
- JSON structured data
  - JavaScript Object Notation, just like XML but smaller, used by Ajax
- etc.



HTTP Status Codes

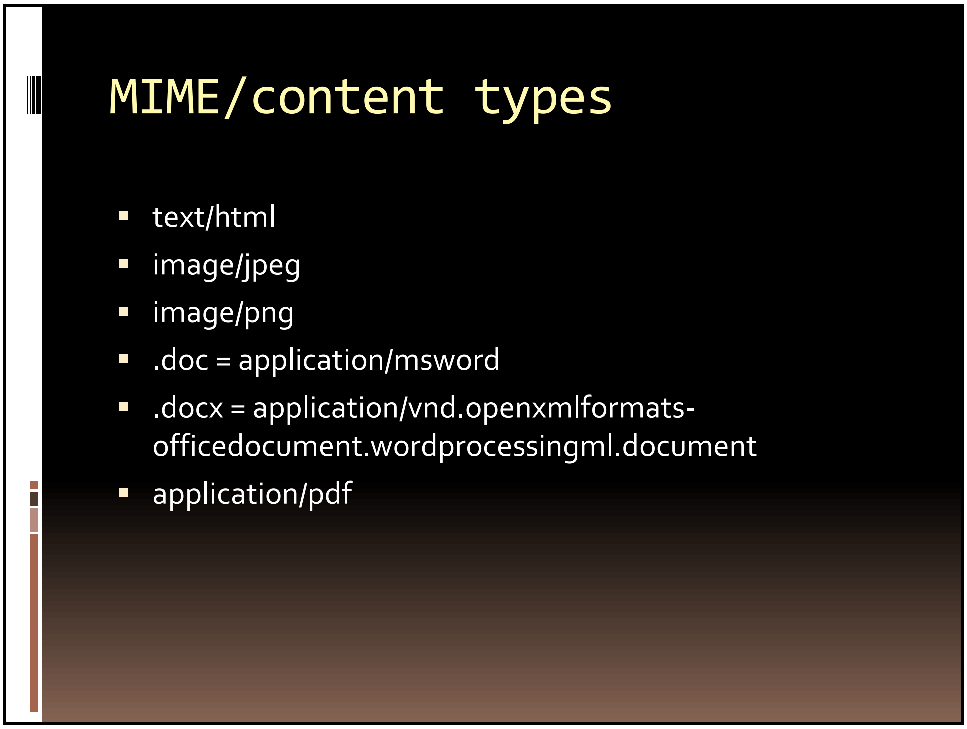
- 200 OK
- 30x redirect
  - temporary, permanent, method, not modified
- 40x client error
  - unauthorized, forbidden, bad request
- 50x server error
  - internal error, overloaded temporarily, gateway timeout

Error status codes in IIS

What	Error code
Site **not found**	404.1
Denied by policy	404.2
Denied by **mime map**	404.3
No handler	404.4
Request Filtering: URL Sequence denied	404.5
Request Filtering: Verb denied	404.6
Request Filtering: File extension denied	404.7
Request Filtering: Denied by hidden segment	404.8
Denied since **hidden file attribute** has been set	404.9
Request Filtering: Denied because request header is too long	404.10
Request Filtering: Denied because URL doubled escaping	404.11
Request Filtering: Denied because of high bit characters	404.12
Request Filtering: Denied because content length too large	404.13
Request Filtering: Denied because URL too long	404.14
Request Filtering: Denied because query string too long	404.15

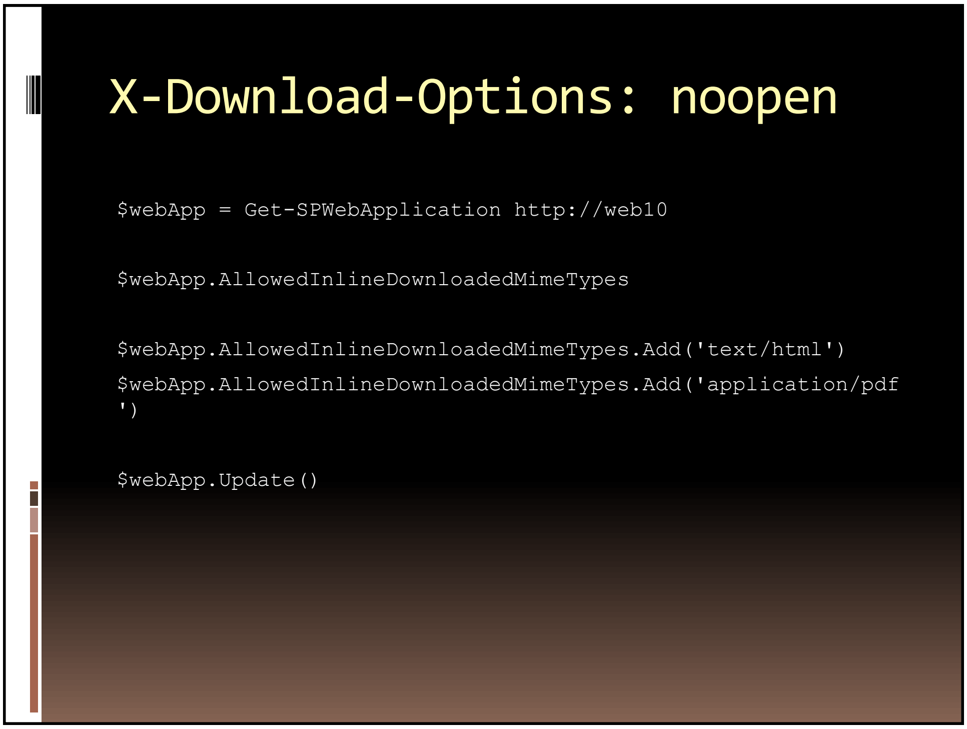
Encoding URI and header characters

- URI and headers must be 7bit US-ASCII only
- URI characters encoded with %xx in hex format
- Header data are usually encoded with Base-64
  - a-z, A-Z, 0-9, =/



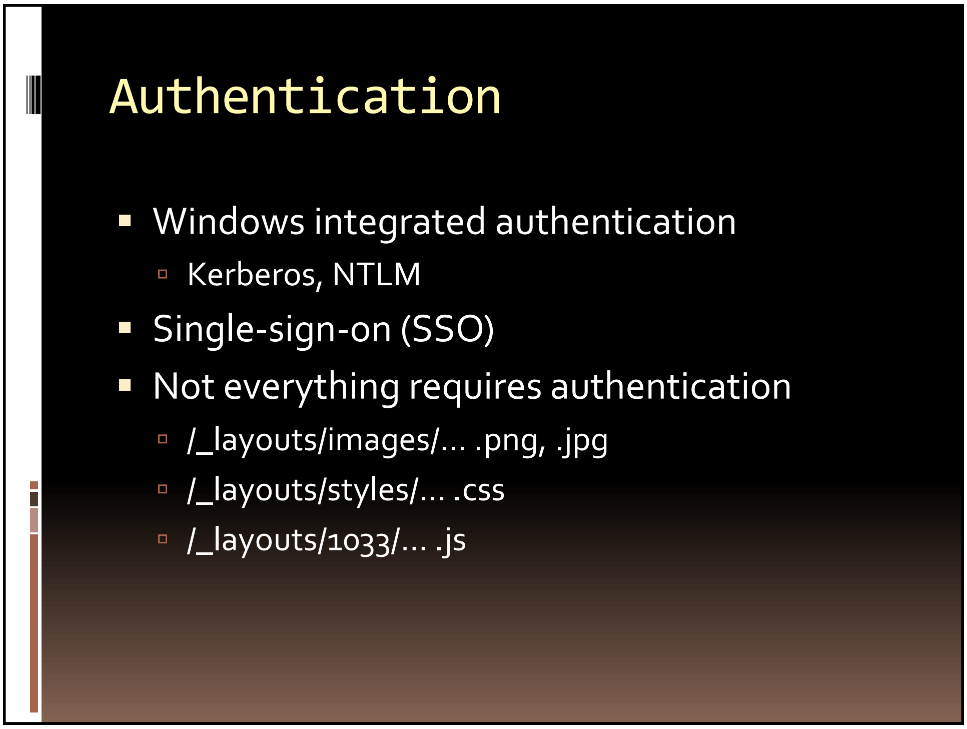
MIME/content types

- text/html
- image/jpeg
- image/png
- .doc = application/msword
- .docx = application/vnd.openxmlformats-officedocument.wordprocessingml.document
- application/pdf



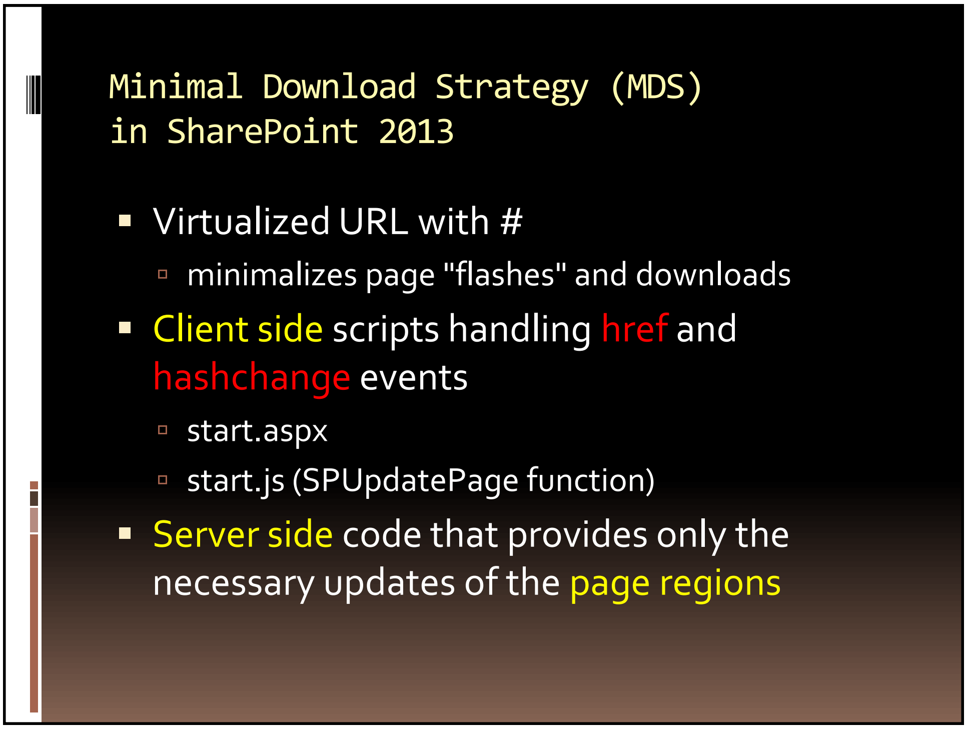
X-Download-Options: noopen

```
$webApp = Get-SPWebApplication http://web10

$webApp.AllowedInlineDownloadedMimeTypes

$webApp.AllowedInlineDownloadedMimeTypes.Add('text/html')
$webApp.AllowedInlineDownloadedMimeTypes.Add('application/pdf
')

$webApp.Update()
```



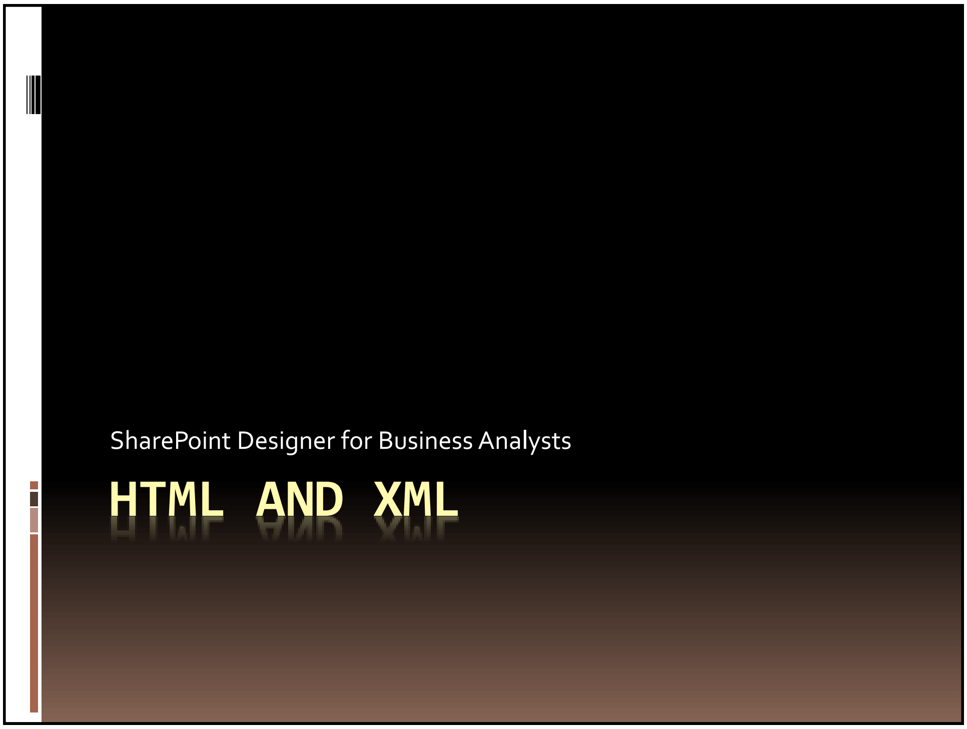
Authentication

- Windows integrated authentication
  - Kerberos, NTLM
- Single-sign-on (SSO)
- Not everything requires authentication
  - /_layouts/images/… .png, .jpg
  - /_layouts/styles/… .css
  - /_layouts/1033/… .js



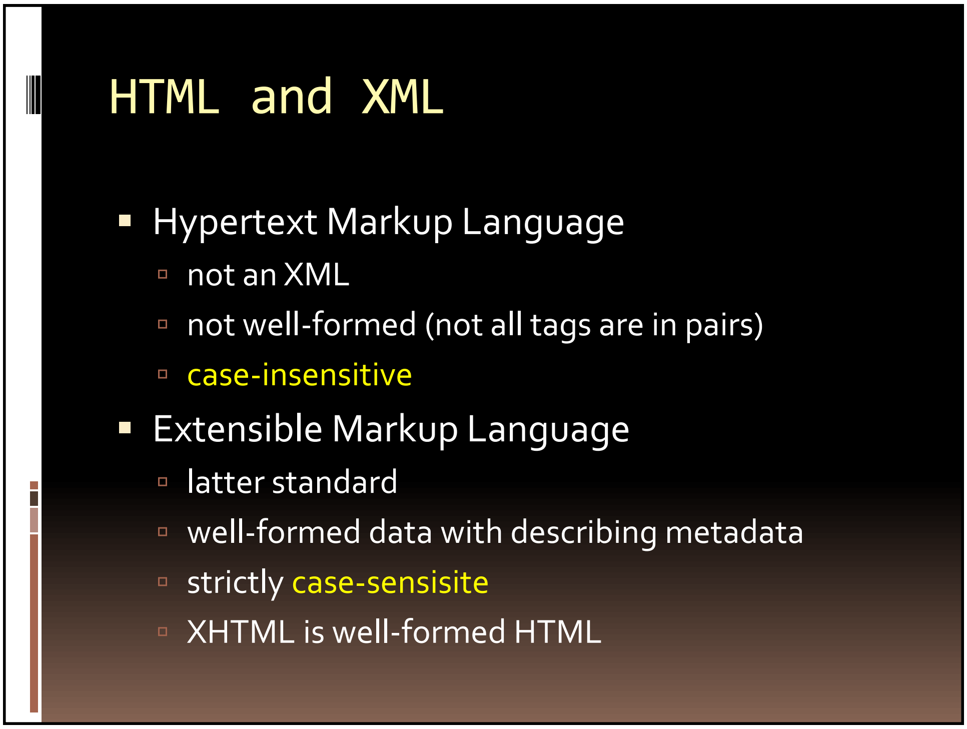
Minimal Download Strategy (MDS) in SharePoint 2013

- Virtualized URL with #
  - minimalizes page "flashes" and downloads
- Client side scripts handling href and hashchange events
  - start.aspx
  - start.js (SPUpdatePage function)
- Server side code that provides only the necessary updates of the page regions



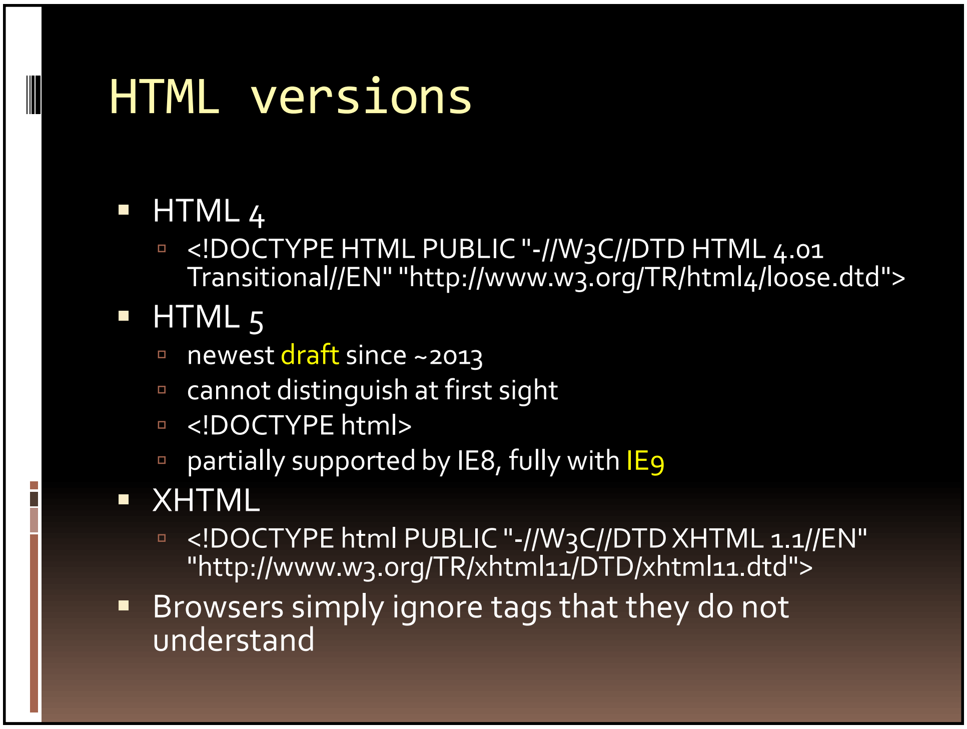
SharePoint Designer for Business Analysts

HTML AND XML



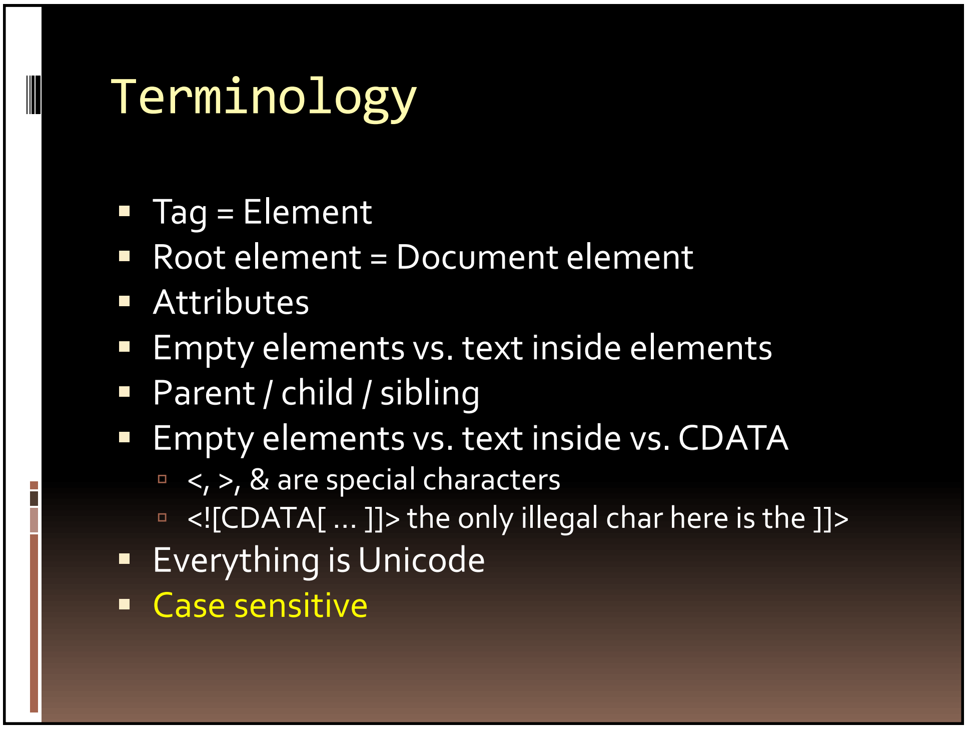
HTML and XML

- Hypertext Markup Language
  - not an XML
  - not well-formed (not all tags are in pairs)
  - case-insensitive
- Extensible Markup Language
  - latter standard
  - well-formed data with describing metadata
  - strictly case-sensisite
  - XHTML is well-formed HTML



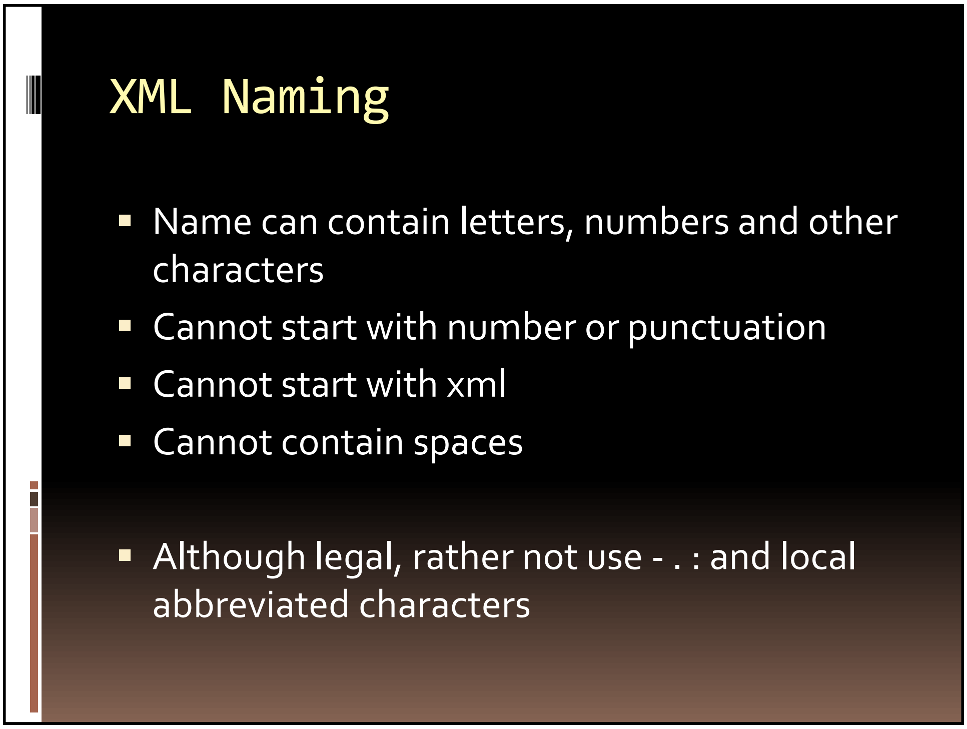
HTML versions

- HTML 4
  - <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
- HTML 5
  - newest draft since ~2013
  - cannot distinguish at first sight
  - <!DOCTYPE html>
  - partially supported by IE8, fully with IE9
- XHTML
  - <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">
- Browsers simply ignore tags that they do not understand



Terminology

- Tag = Element
- Root element = Document element
- Attributes
- Empty elements vs. text inside elements
- Parent / child / sibling
- Empty elements vs. text inside vs. CDATA
  - <, >, & are special characters
  - <![CDATA[…]]> the only illegal char here is the]]>
- Everything is Unicode
- Case sensitive



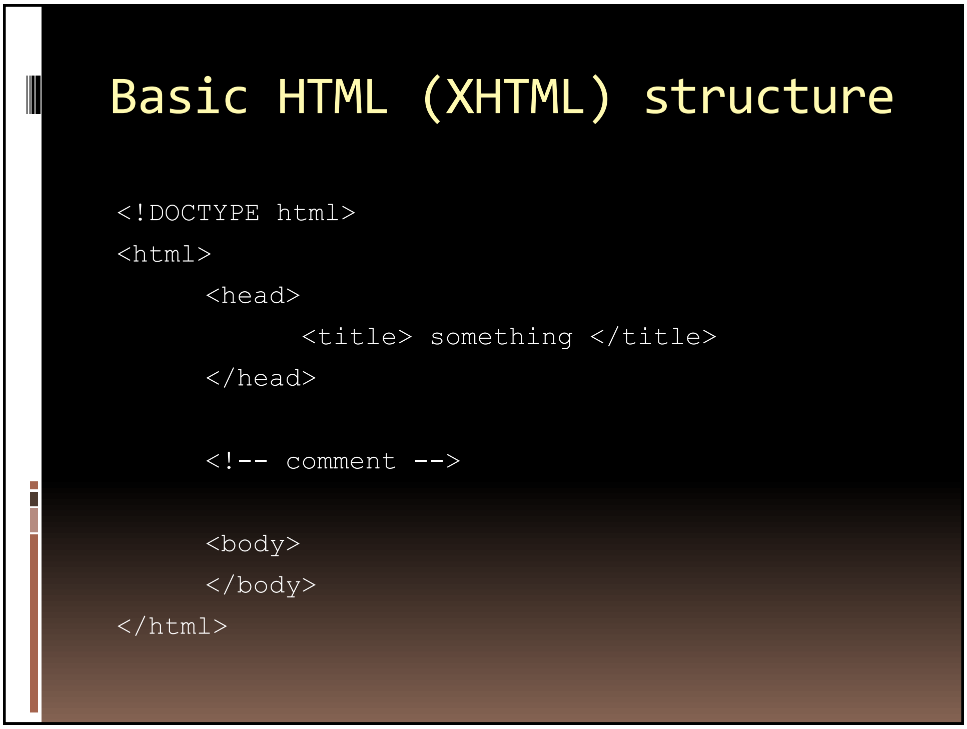
XML Naming

- Name can contain letters, numbers and other characters
- Cannot start with number or punctuation
- Cannot start with xml
- Cannot contain spaces

- Although legal, rather not use - . : and local abbreviated characters

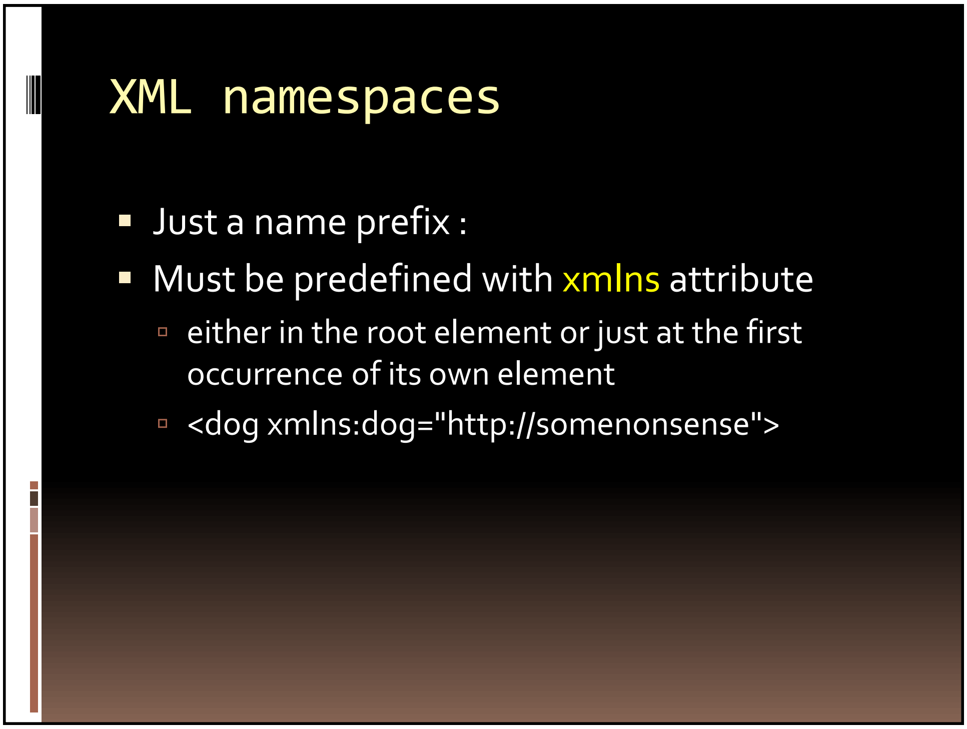
XML/HTML Special Characters

XML	char	XML	char
&quot;	"	&trade;	(TM)
&amp;	&	&copy;	(C)
&nbsp;	space	&reg;	(R)
&gt;	>	&euro;	EUR
&lt;	<	&sect;	§
&le;	<=	&acute;	'
&ge;	>=		



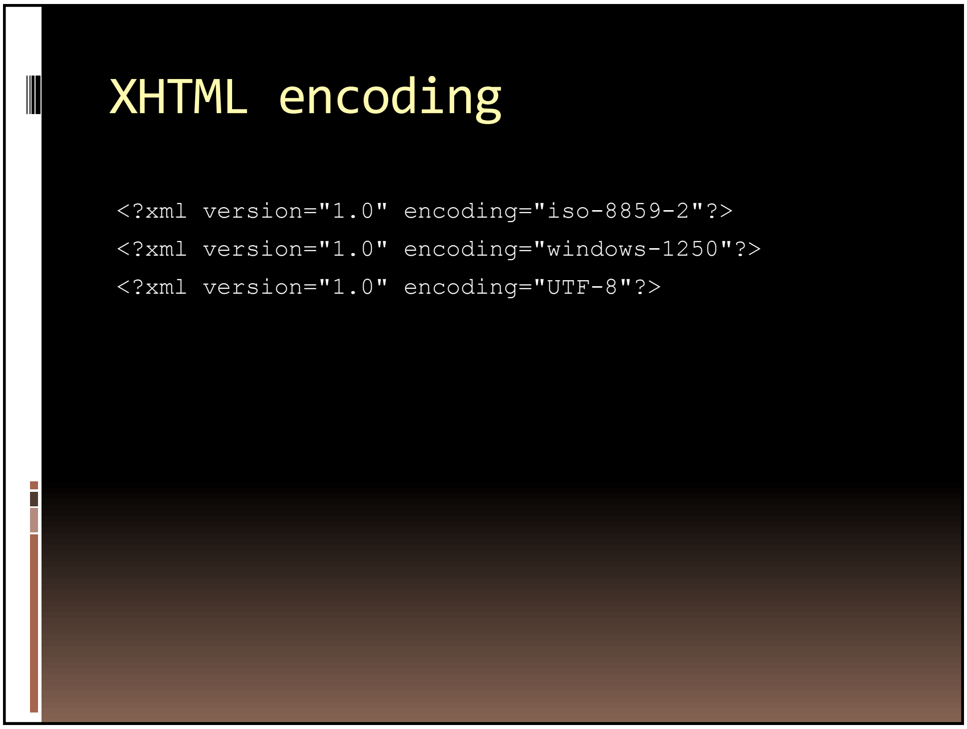
Basic HTML (XHTML) structure

```
<!DOCTYPE html>
<html>
     <head>
           <title> something </title>
     </head>

     <!-- comment -->

     <body>
     </body>
</html>
```



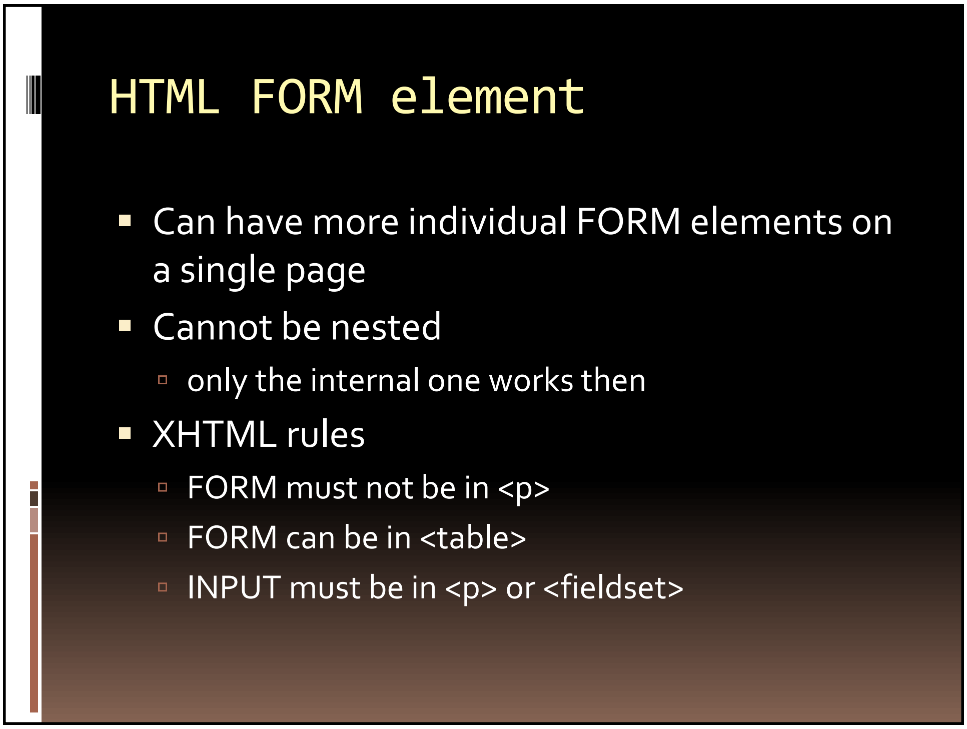
XML namespaces

- Just a name prefix :
- Must be predefined with xmlns attribute
  - either in the root element or just at the first occurrence of its own element
  - <dog xmlns:dog="http://somenonsense">



XHTML encoding

```
<?xml version="1.0" encoding="iso-8859-2"?>
<?xml version="1.0" encoding="windows-1250"?>
<?xml version="1.0" encoding="UTF-8"?>
```

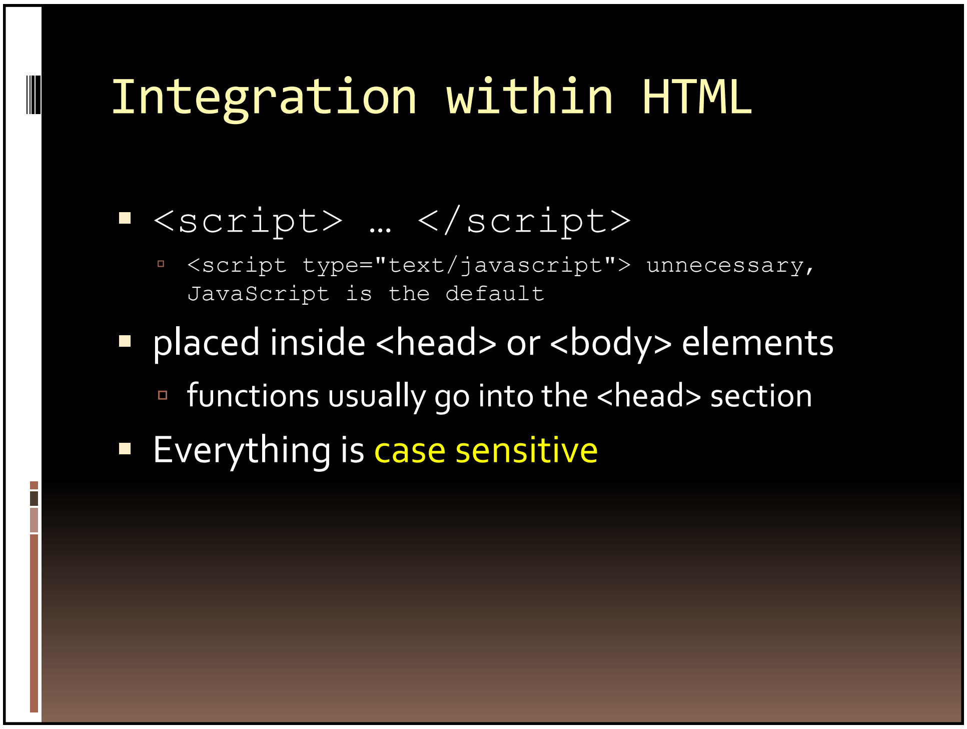


HTML FORM element

- Can have more individual FORM elements on a single page
- Cannot be nested
  - only the internal one works then
- XHTML rules
  - FORM must not be in <p>
  - FORM can be in <table>
  - INPUT must be in <p> or <fieldset>

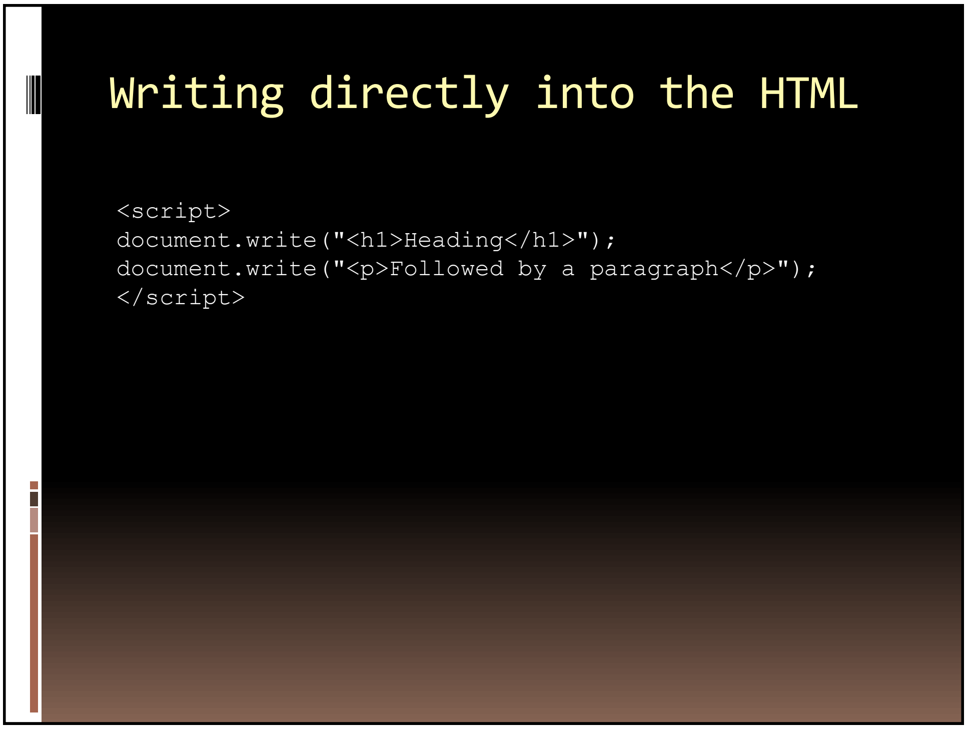
SharePoint Designer for Business Analysts

JAVASCRIPT



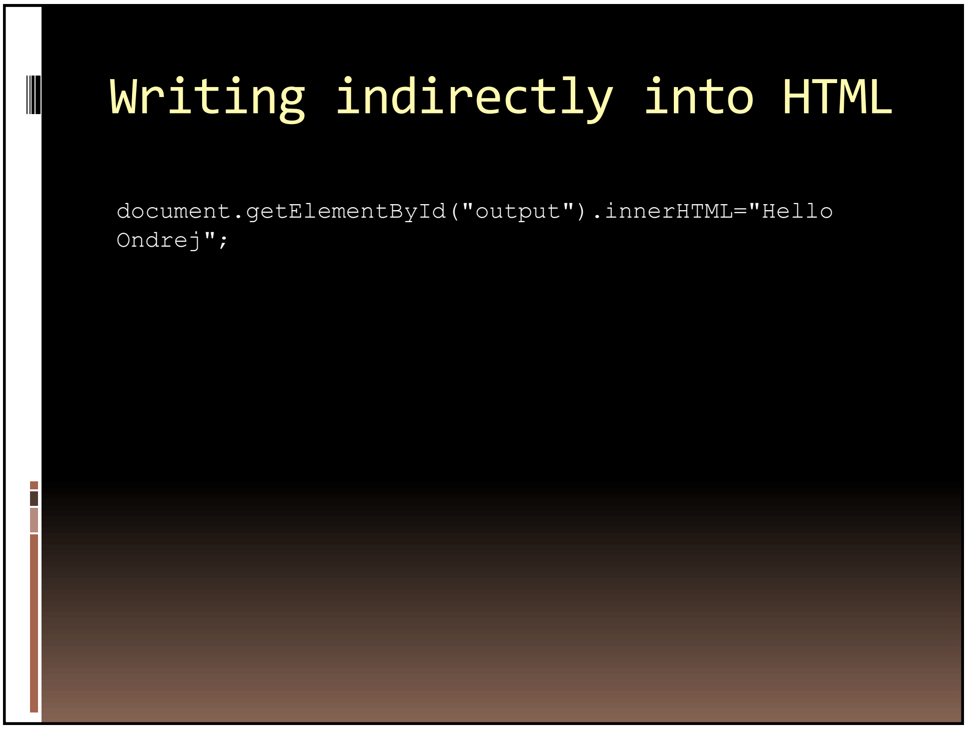
Integration within HTML

- `<script> … </script>`
  - `<script type="text/javascript"> unnecessary, JavaScript is the default`
- placed inside <head> or <body> elements
  - functions usually go into the <head> section
- Everything is case sensitive



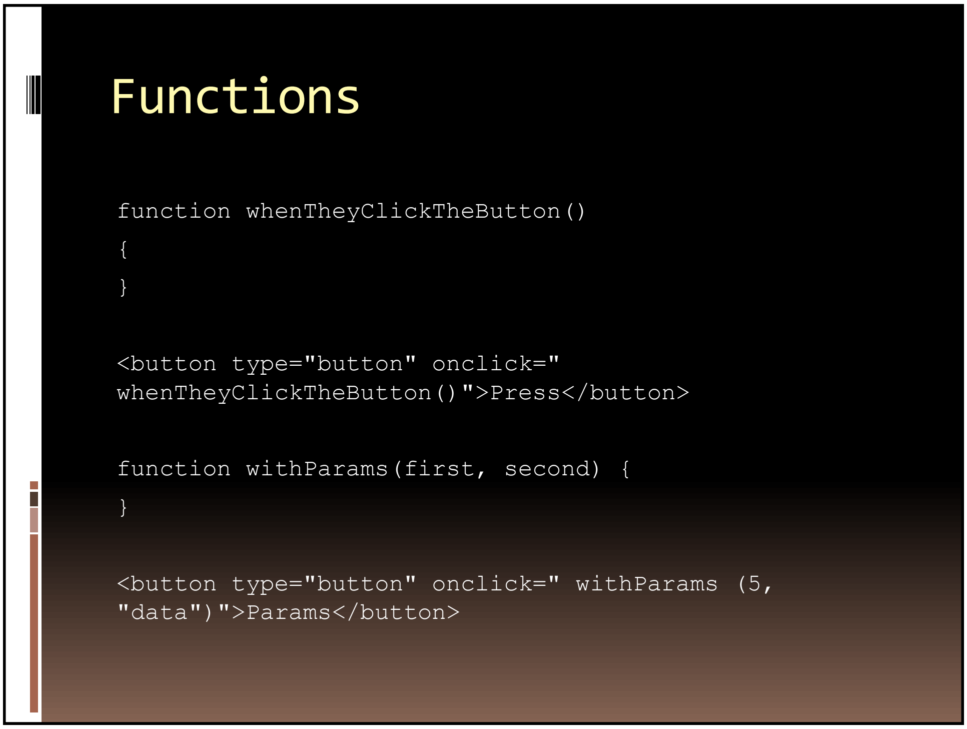
Writing directly into the HTML

```
<script>
document.write("<h1>Heading</h1>");
document.write("<p>Followed by a paragraph</p>");
</script>
```



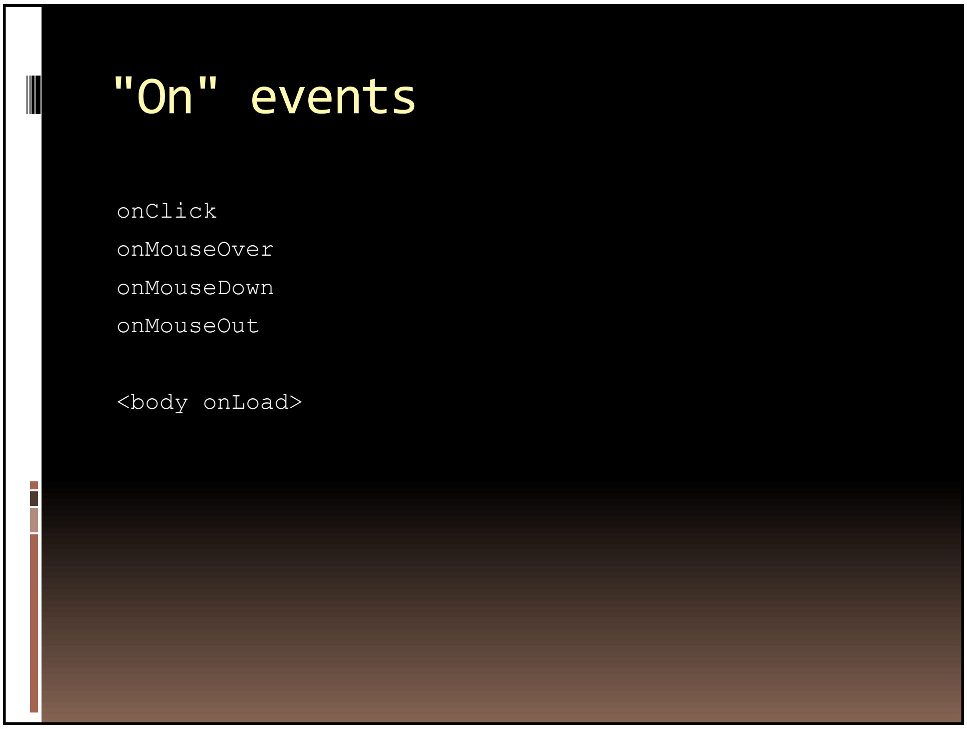
Writing indirectly into HTML

```
document.getElementById("output").innerHTML="Hello
Ondrej";
```



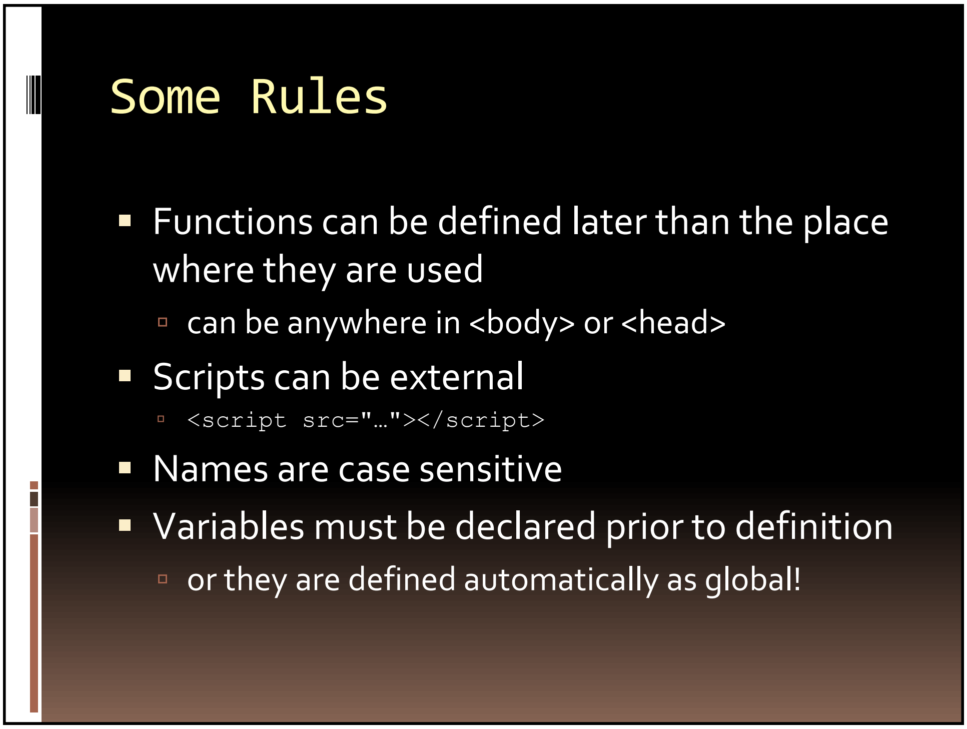
Functions

```
function whenTheyClickTheButton()
{
}

<button type="button" onclick="
whenTheyClickTheButton()">Press</button>

function withParams(first, second) {
}

<button type="button" onclick=" withParams (5,
"data")">Params</button>
```



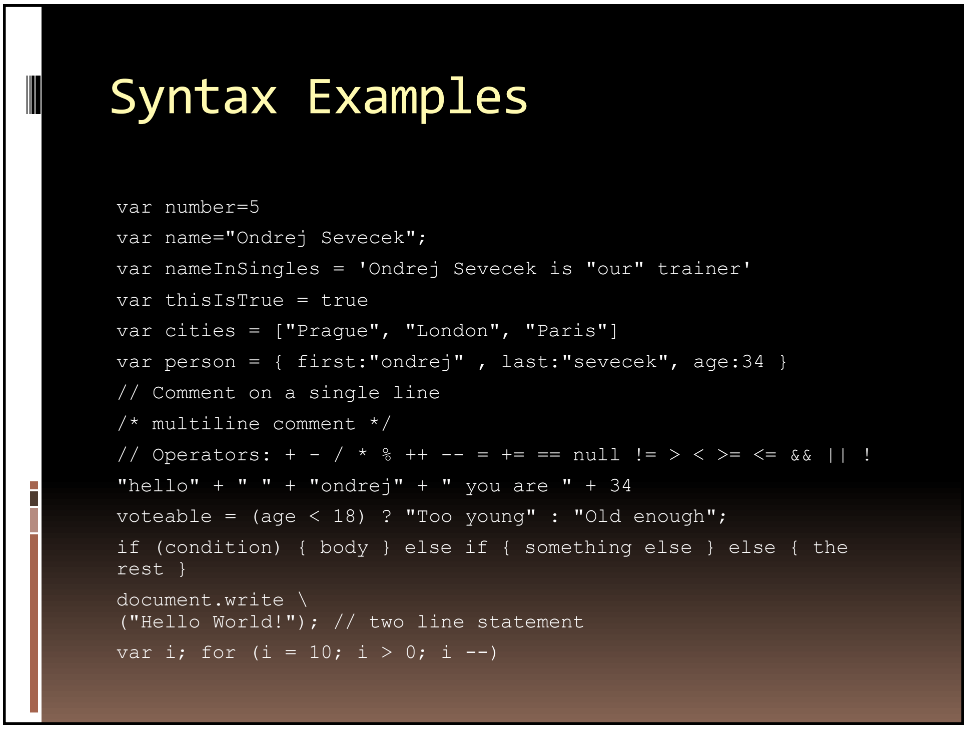
"On" events

```
onClick
onMouseOver
onMouseDown
onMouseOut

<body onLoad>
```



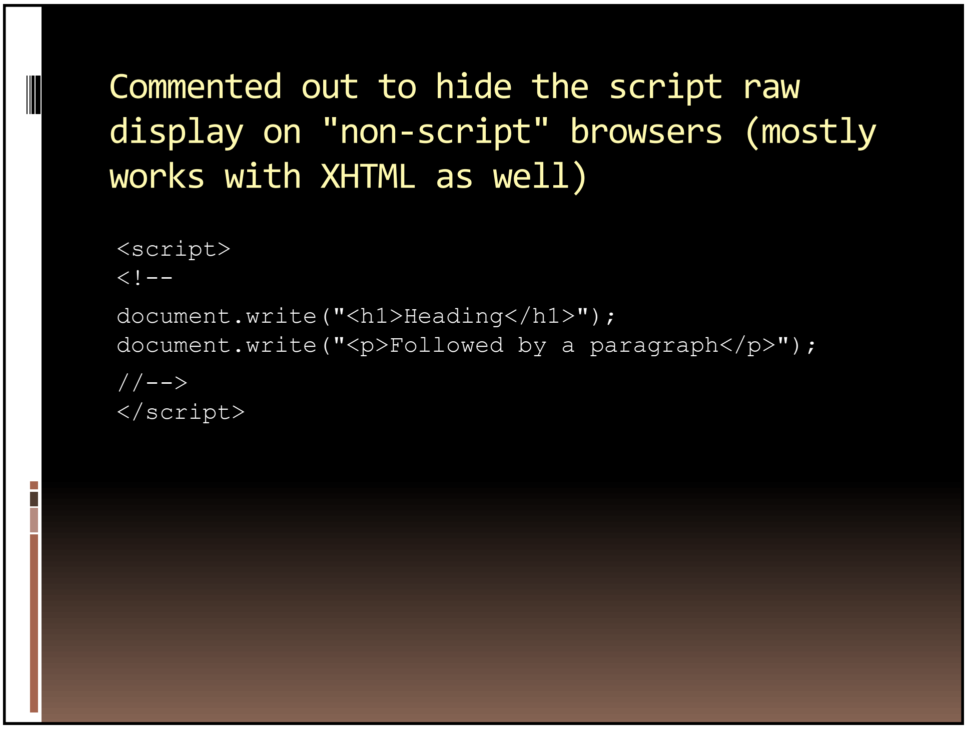
Some Rules

- Functions can be defined later than the place where they are used
  - can be anywhere in <body> or <head>
- Scripts can be external
  - `<script src="…"></script>`
- Names are case sensitive
- Variables must be declared prior to definition
  - or they are defined automatically as global!



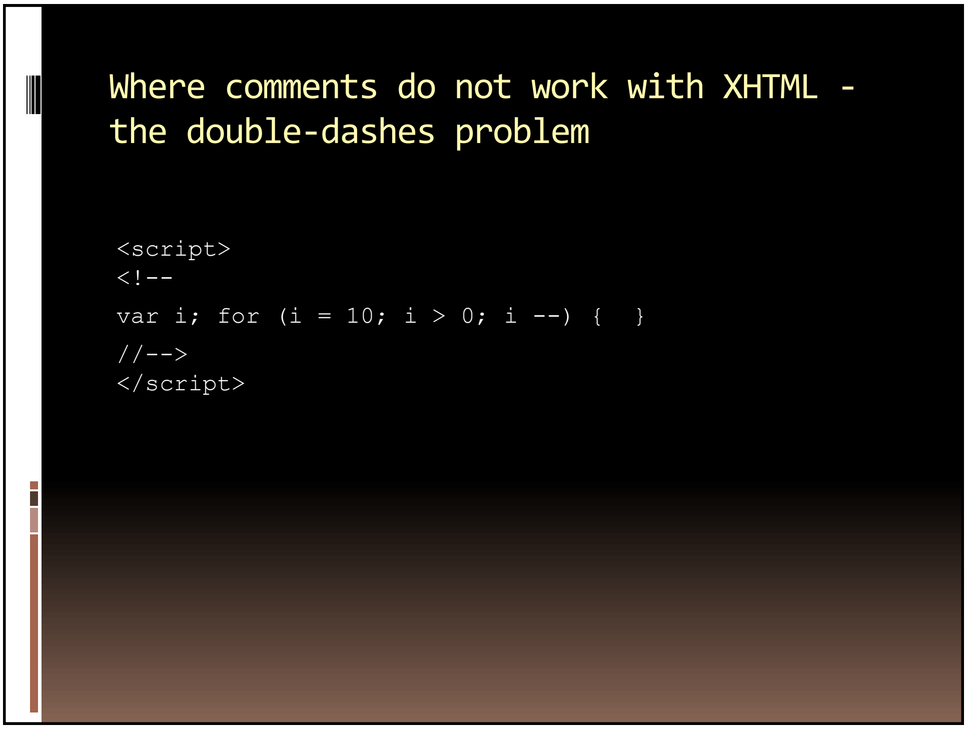
Syntax Examples

```
var number=5
var name="Ondrej Sevecek";
var nameInSingles = 'Ondrej Sevecek is "our" trainer'
var thisIsTrue = true
var cities = ["Prague", "London", "Paris"]
var person = { first:"ondrej" , last:"sevecek", age:34 }
// Comment on a single line
/* multiline comment */
// Operators: + - / * % ++ -- = += == null != > < >= <= && || !
"hello" + " " + "ondrej" + " you are " + 34
voteable = (age < 18) ? "Too young" : "Old enough";
if (condition) { body } else if { something else } else { the
rest }
document.write \
("Hello World!"); // two line statement
var i; for (i = 10; i > 0; i --)
```



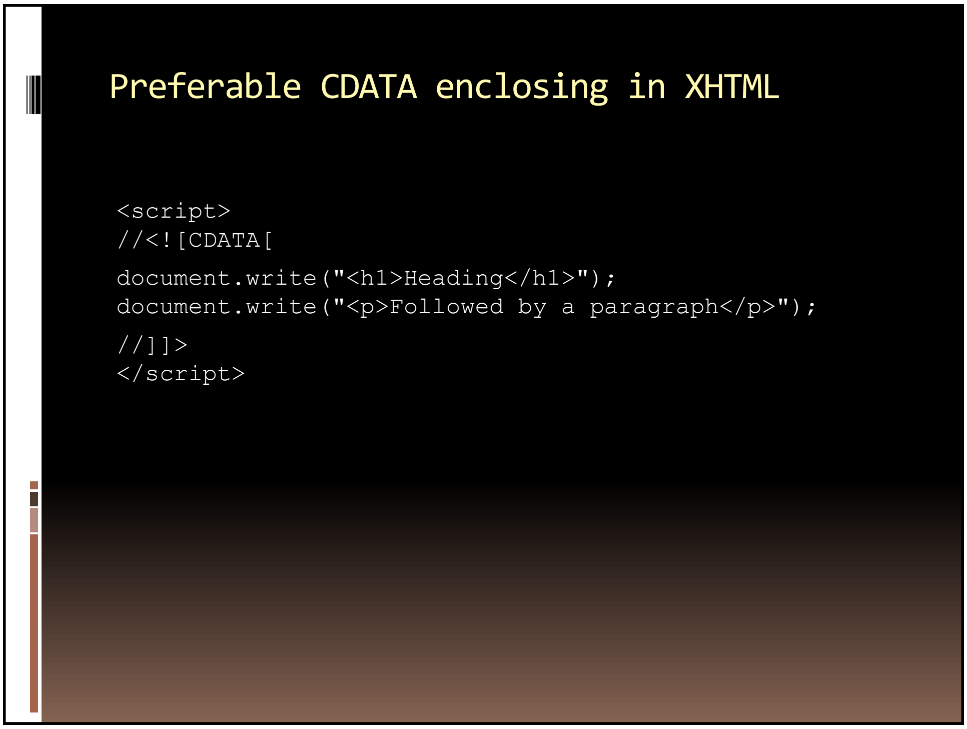
Commented out to hide the script raw display on "non-script" browsers (mostly works with XHTML as well)

```
<script>
<!--
document.write("<h1>Heading</h1>");
document.write("<p>Followed by a paragraph</p>");
//-->
</script>
```



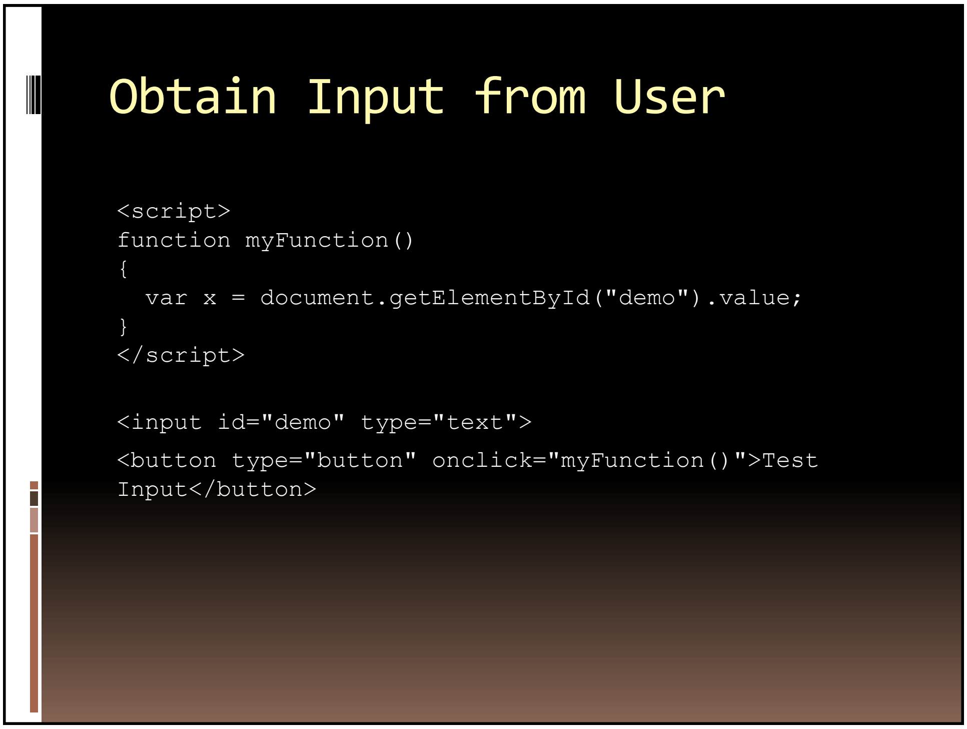
Where comments do not work with XHTML - the double-dashes problem

```
<script>
<!--
var i; for (i = 10; i > 0; i --) {   }
//-->
</script>
```



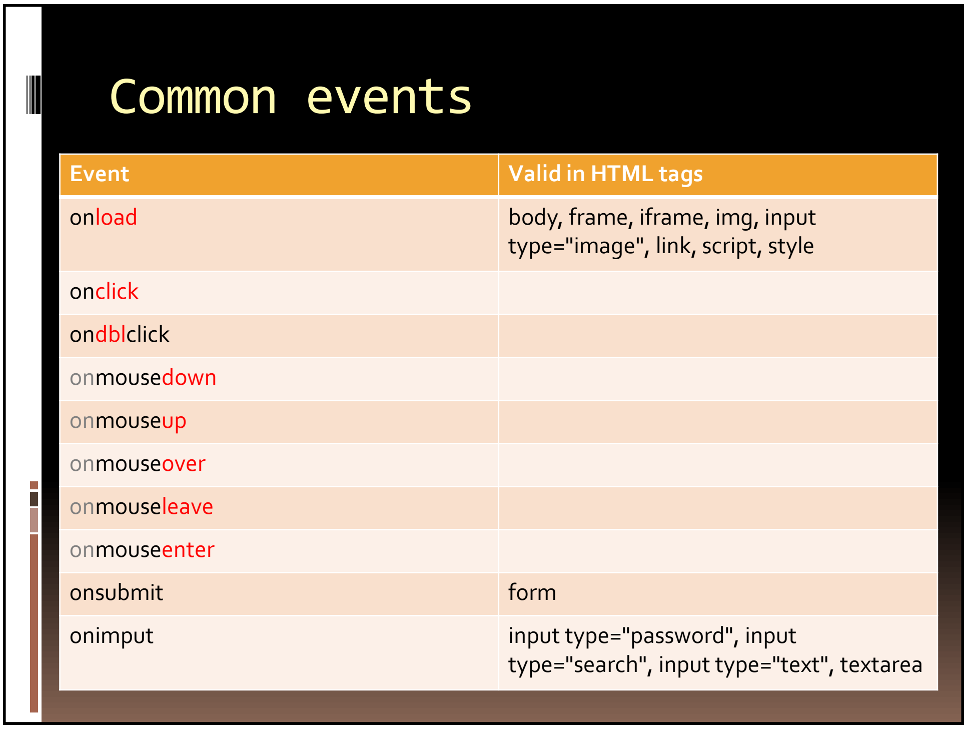
Preferable CDATA enclosing in XHTML

```
<script>
//<![CDATA[
document.write("<h1>Heading</h1>");
document.write("<p>Followed by a paragraph</p>");
//]]>
</script>
```



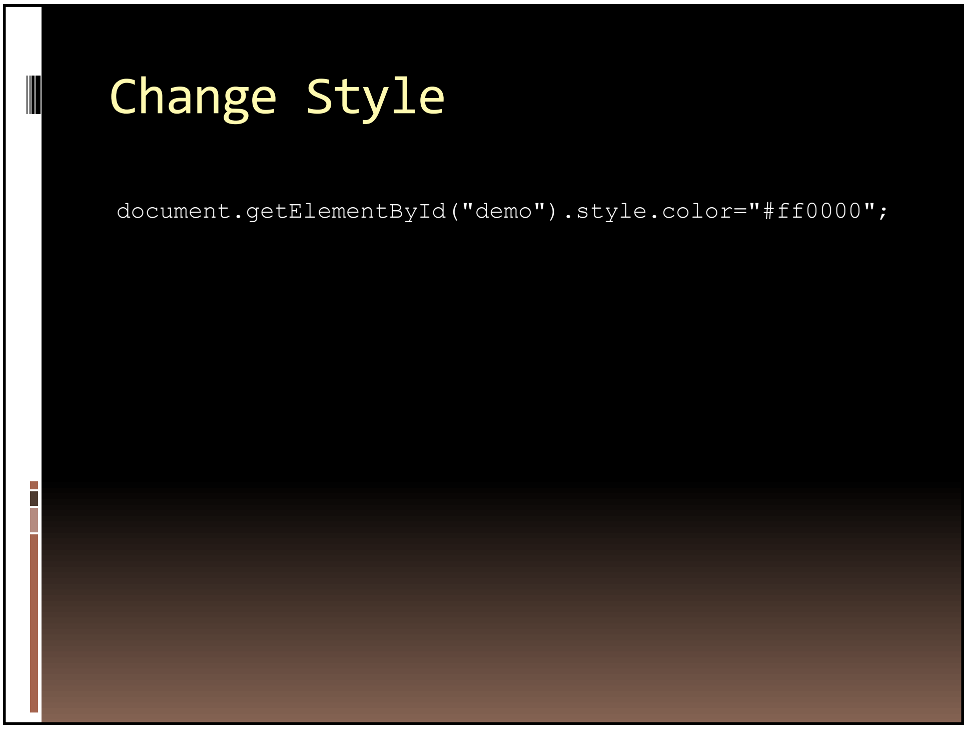
Obtain Input from User

```
<script>
function myFunction()
{
  var x = document.getElementById("demo").value;
}
</script>

<input id="demo" type="text">
<button type="button" onclick="myFunction()">Test
Input</button>
```



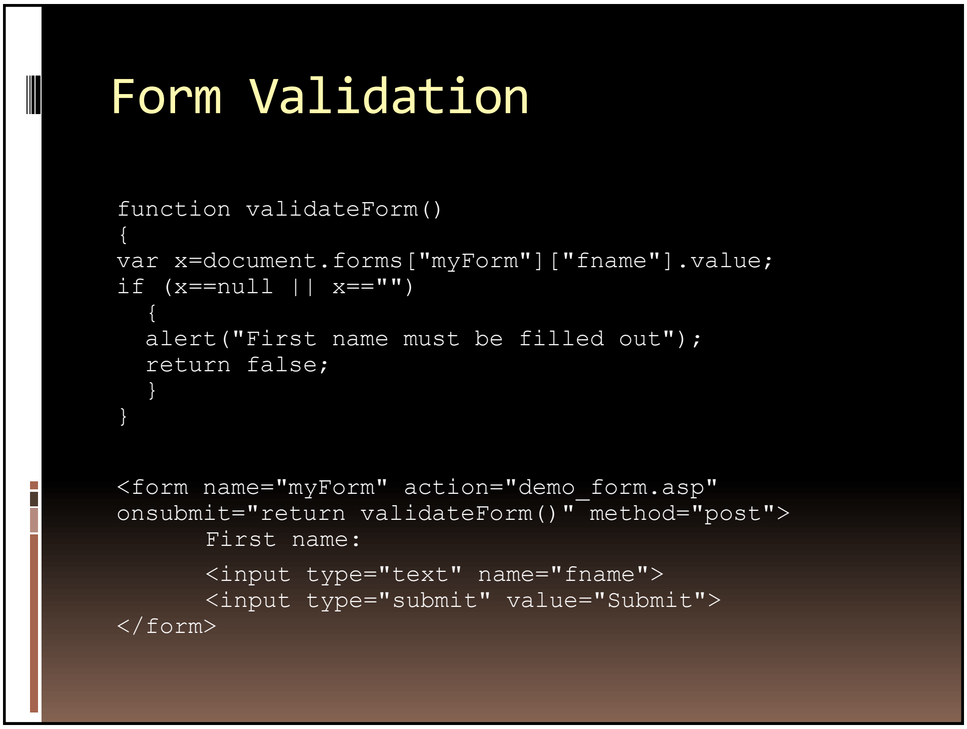
Common events

Event	Valid in HTML tags
onload	body, frame, iframe, img, input type="image", link, script, style
onclick	
ondblclick	
onmousedown	
onmouseup	
onmouseover	
onmouseleave	
onmouseenter	
onsubmit	form
onimput	input type="password", input type="search", input type="text", textarea



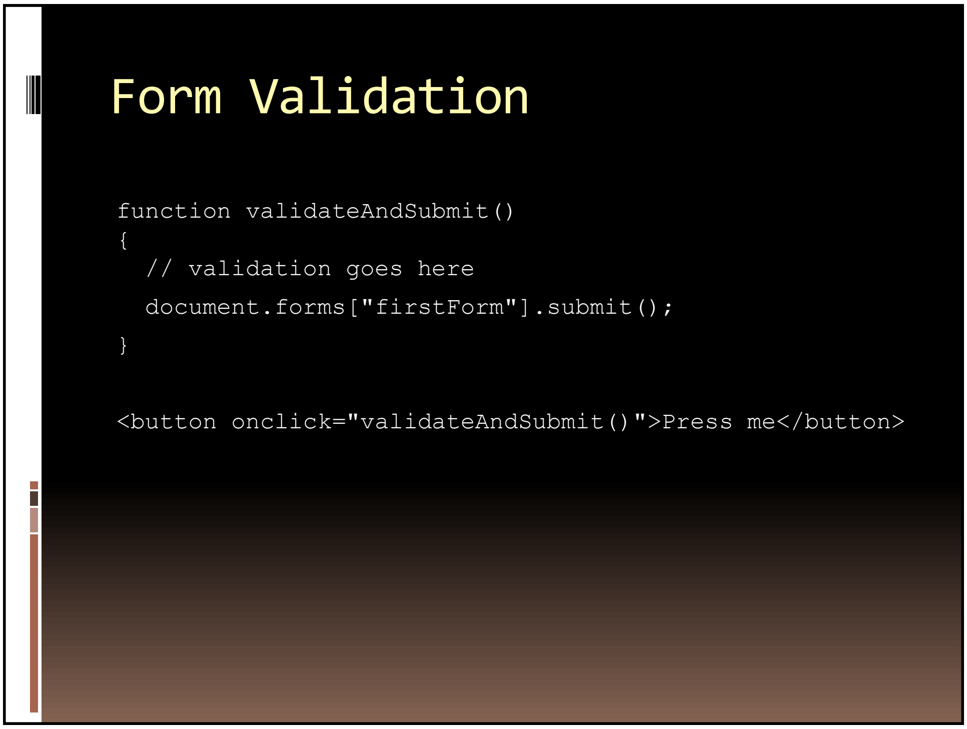
Change Style

```
document.getElementById("demo").style.color="#ff0000";
```



Form Validation

```
function validateForm()
{
var x=document.forms["myForm"]["fname"].value;
if (x==null || x=="")
  {
  alert("First name must be filled out");
  return false;
  }
}


<form name="myForm" action="demo_form.asp"
onsubmit="return validateForm()" method="post">
      First name:
      <input type="text" name="fname">
      <input type="submit" value="Submit">
</form>
```



Form Validation

```
function validateAndSubmit()
{
  // validation goes here
  document.forms["firstForm"].submit();
}


<button onclick="validateAndSubmit()">Press me</button>
```

Script Security

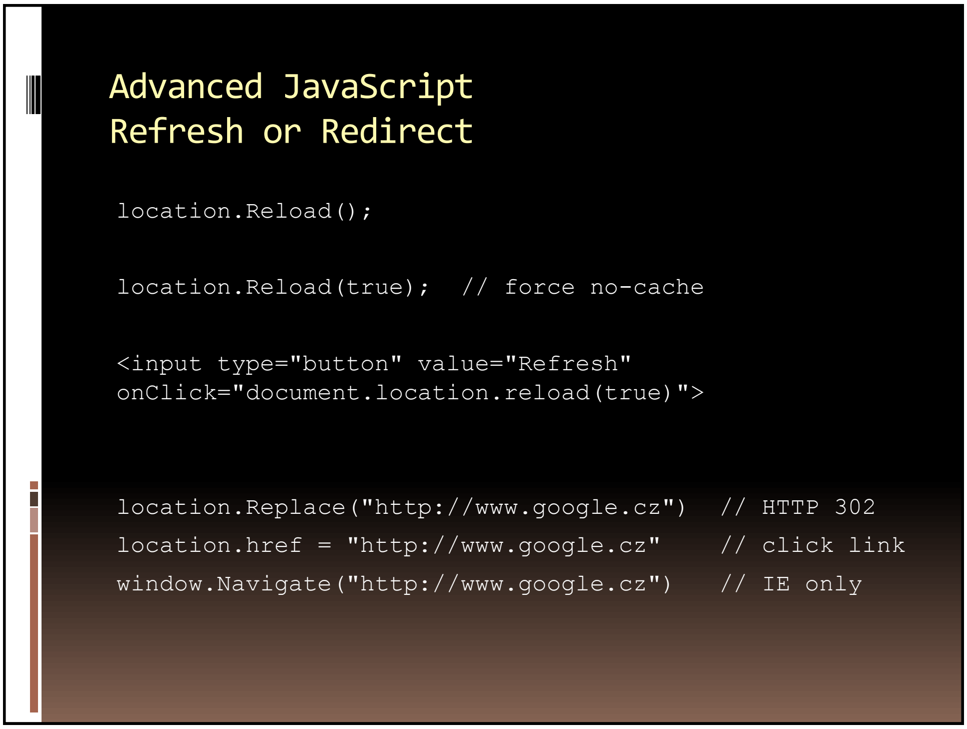
- Browser places every page into a security zone according to its URL

  `<noscript> … </noscript>`

- Local Machine Zone Lockdown zone
  - extremely restricted over Local Machine
  - no scripts, no ActiveX
- Internet zone
- Local Intranet zone
- Trusted Sites zone
- Restricted Sites

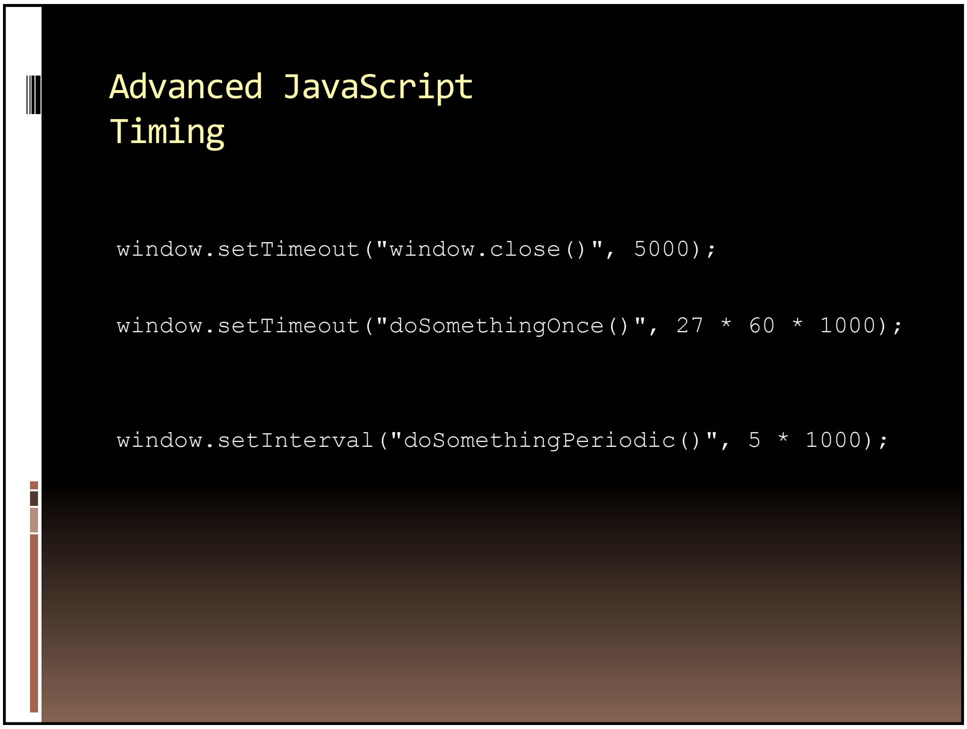
Advanced JavaScript
Obtain current URL

```
document.write(location.host + "<br/>");
document.write(location.pathname + "<br/>");
document.write(location.href + "<br/>");
```



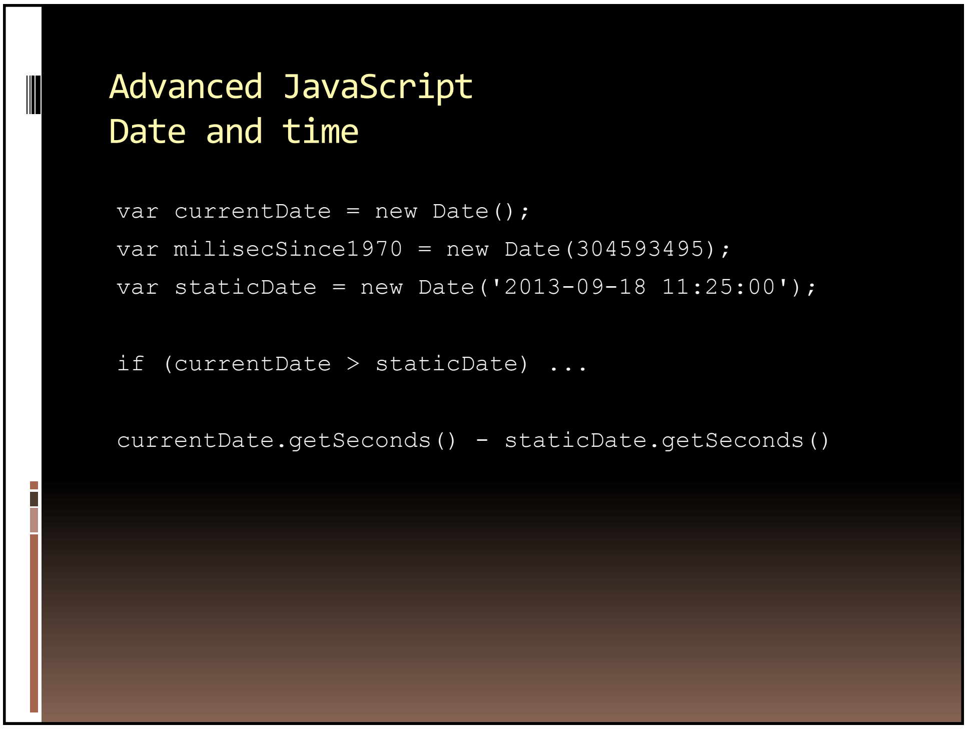
Advanced JavaScript
Refresh or Redirect

```
location.Reload();

location.Reload(true);  // force no-cache

<input type="button" value="Refresh"
onClick="document.location.reload(true)">


location.Replace("http://www.google.cz")  // HTTP 302
location.href = "http://www.google.cz"    // click link
window.Navigate("http://www.google.cz")   // IE only
```



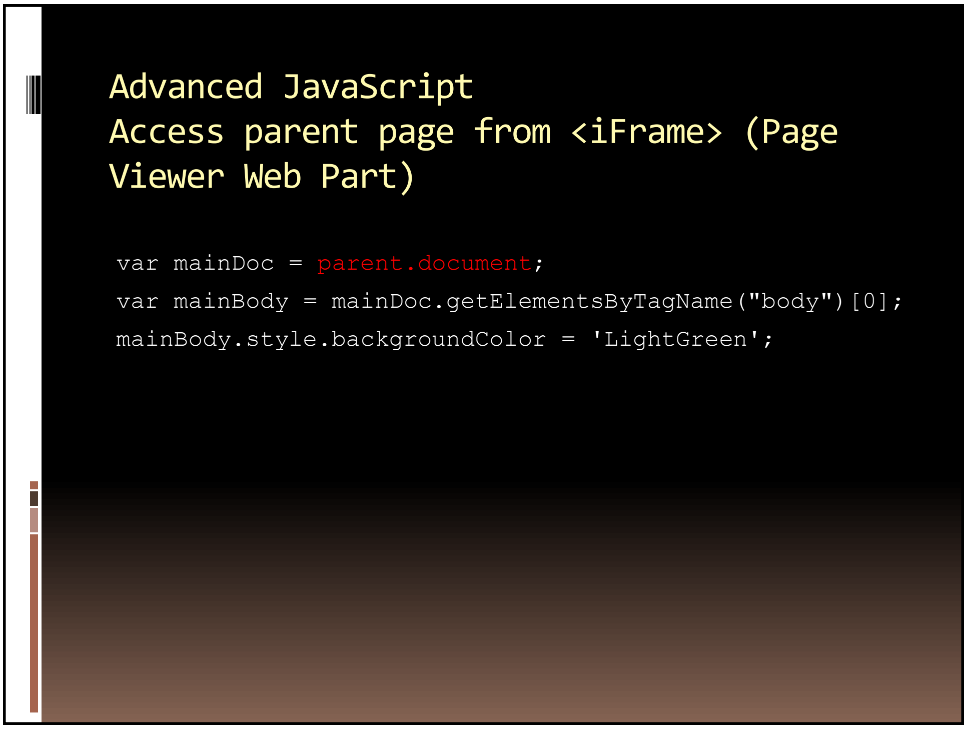
Advanced JavaScript
Timing

```
window.setTimeout("window.close()", 5000);

window.setTimeout("doSomethingOnce()", 27 * 60 * 1000);


window.setInterval("doSomethingPeriodic()", 5 * 1000);
```



Advanced JavaScript
Date and time

```
var currentDate = new Date();
var milisecSince1970 = new Date(304593495);
var staticDate = new Date('2013-09-18 11:25:00');

if (currentDate > staticDate) ...

currentDate.getSeconds() - staticDate.getSeconds()
```



Advanced JavaScript
Access parent page from <iFrame> (Page Viewer Web Part)

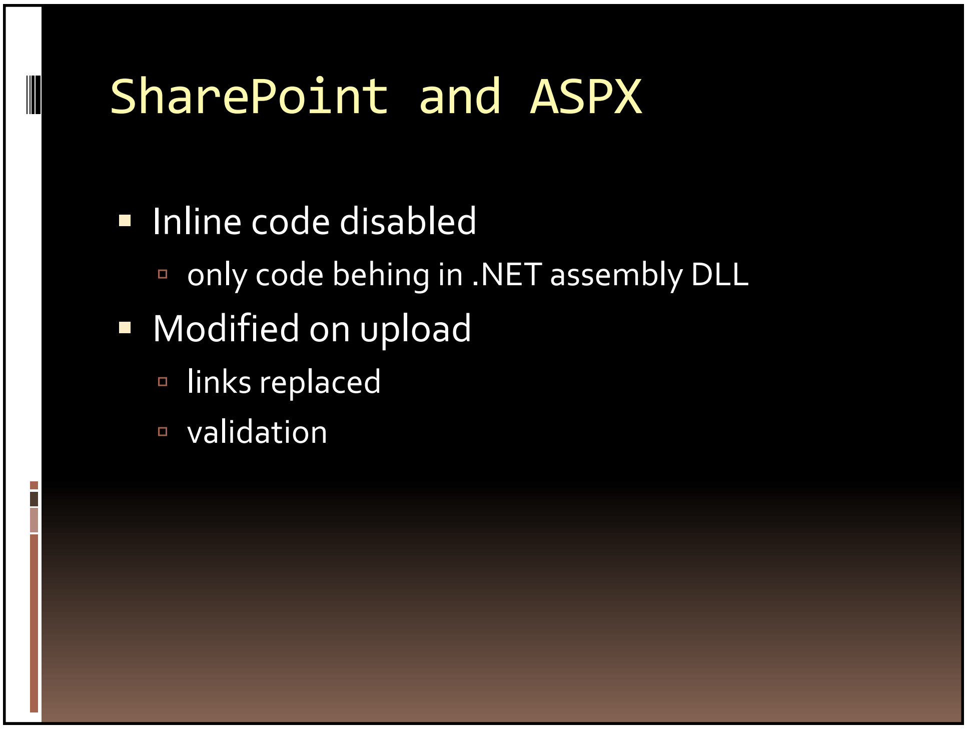
```
var mainDoc = parent.document;
var mainBody = mainDoc.getElementsByTagName("body")[0];
mainBody.style.backgroundColor = 'LightGreen';
```

SharePoint Designer for Business Analysts

ASPX

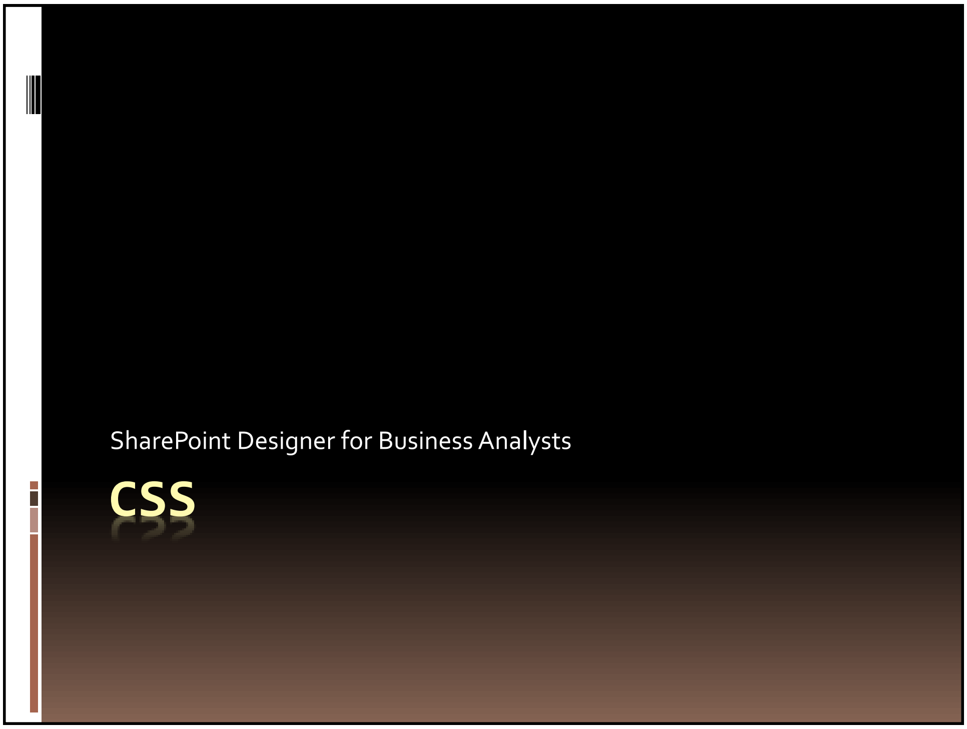
Server Side Scripting

- Active Server Pages (.NET)
  - newer technology than ASP
- Scripts inside the HTML are processed on the server side
  - <% … %>
- Only pure HTML + <script> is returned to client
- Page starts with `<%@ Page %>`



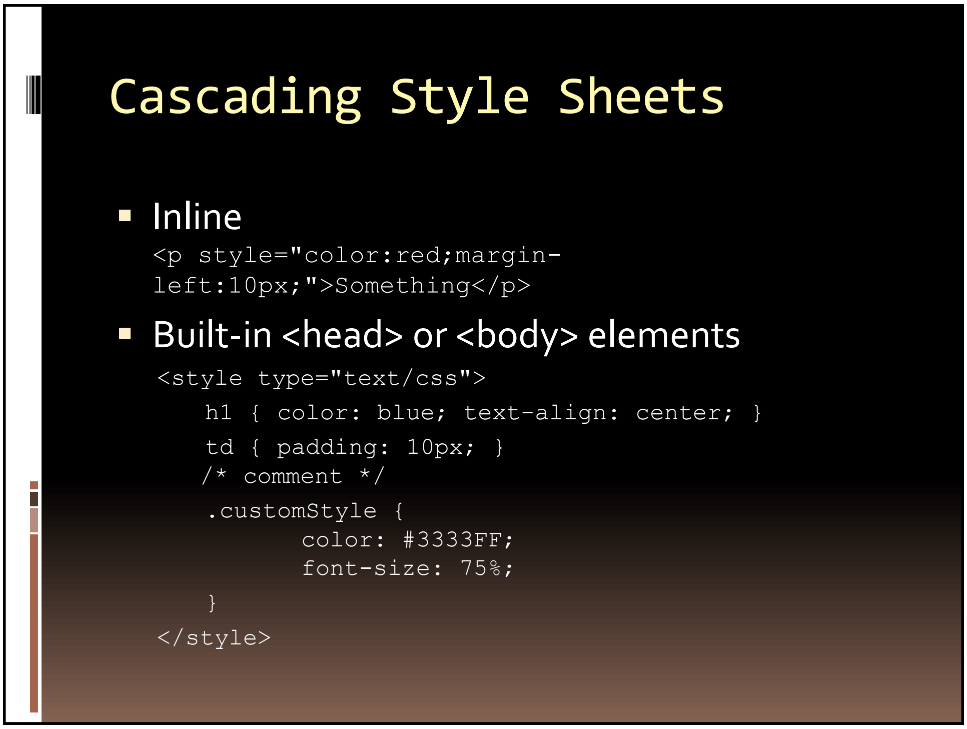
SharePoint and ASPX

- Inline code disabled
  - only code behing in .NET assembly DLL
- Modified on upload
  - links replaced
  - validation



SharePoint Designer for Business Analysts

CSS



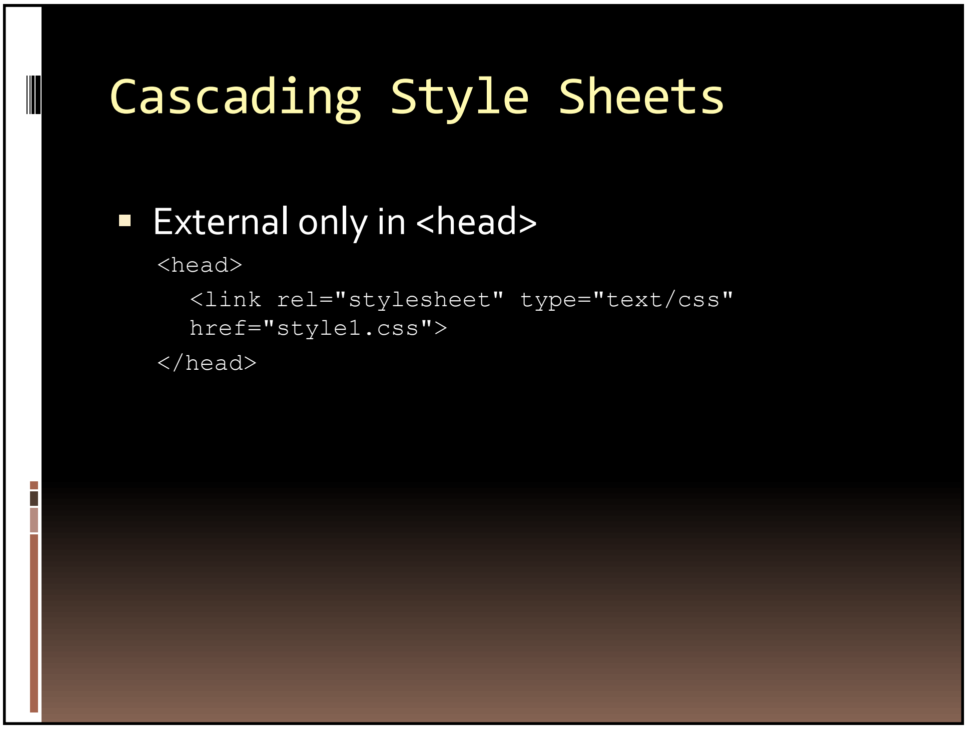
Cascading Style Sheets

- Inline

```
<p style="color:red;margin-
left:10px;">Something</p>
```

- Built-in <head> or <body> elements

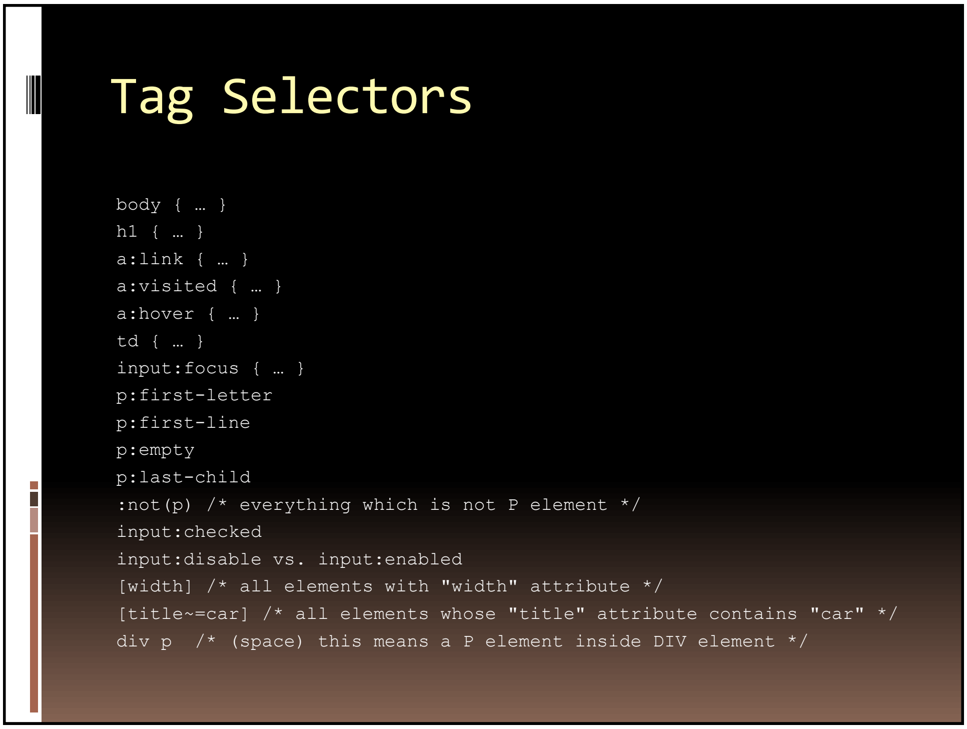
```
<style type="text/css">
    h1 { color: blue; text-align: center; }
    td { padding: 10px; }
    /* comment */
    .customStyle {
            color: #3333FF;
            font-size: 75%;
    }
</style>
```



Cascading Style Sheets

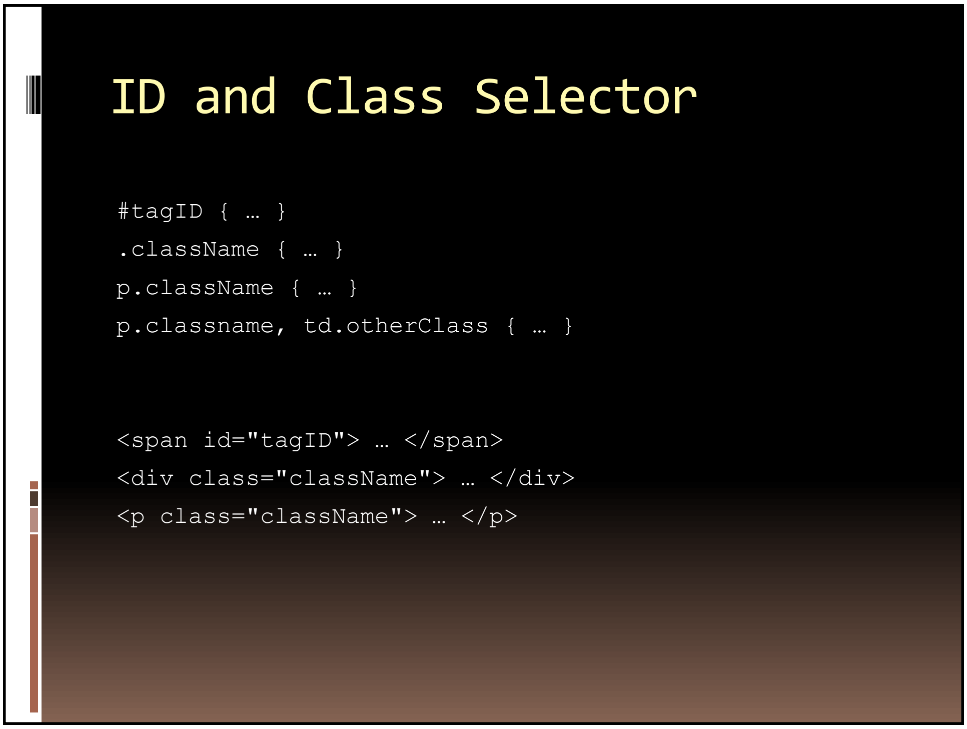
- External only in <head>

```
<head>
  <link rel="stylesheet" type="text/css"
  href="style1.css">
</head>
```



Tag Selectors

```
body { … }
h1 { … }
a:link { … }
a:visited { … }
a:hover { … }
td { … }
input:focus { … }
p:first-letter
p:first-line
p:empty
p:last-child
:not(p) /* everything which is not P element */
input:checked
input:disable vs. input:enabled
[width] /* all elements with "width" attribute */
[title~=car] /* all elements whose "title" attribute contains "car" */
div p  /* (space) this means a P element inside DIV element */
```



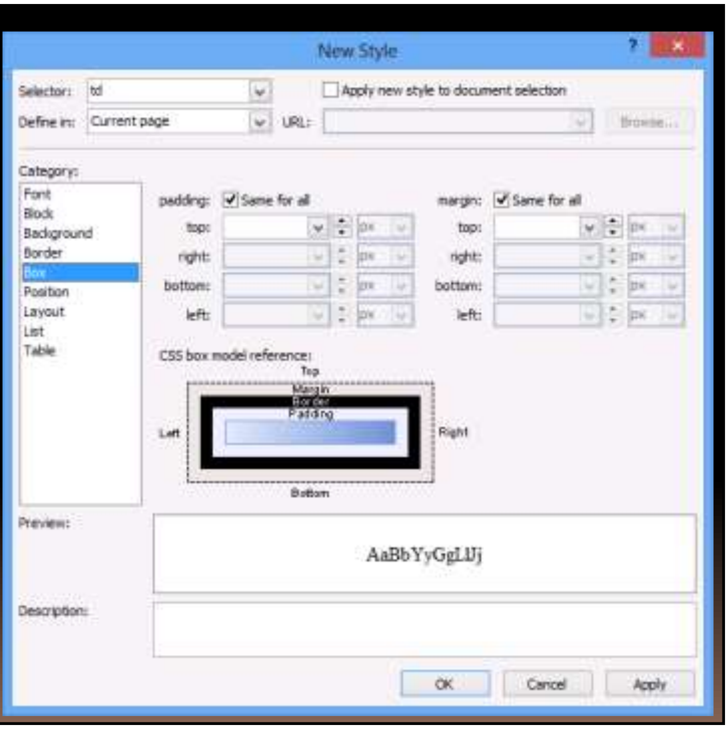
ID and Class Selector

```
#tagID { … }
.className { … }
p.className { … }
p.classname, td.otherClass { … }


<span id="tagID"> … </span>
<div class="className"> … </div>
<p class="className"> … </p>
```

Some Property Examples

```
color: blue;
color: #3333FF;
font-size: 75%;
font-family: Verdana;
font-weight:bold
background-color: #FFFFF0;
margin: 10px;
background-image: url('tile.png');
background-repeat: repeat-x;
ul { list-style: circle; }
*height: 100px;
display: none; /* hidden */
```

Border
margin
padding



New Style

Selector: td

Define in: Current page

□ Apply new style to document selection

URL:

Category: Box

padding: ☑ Same for all

margin: ☑ Same for all

CSS box model reference:

Preview:

AaBbYyGgLlJj

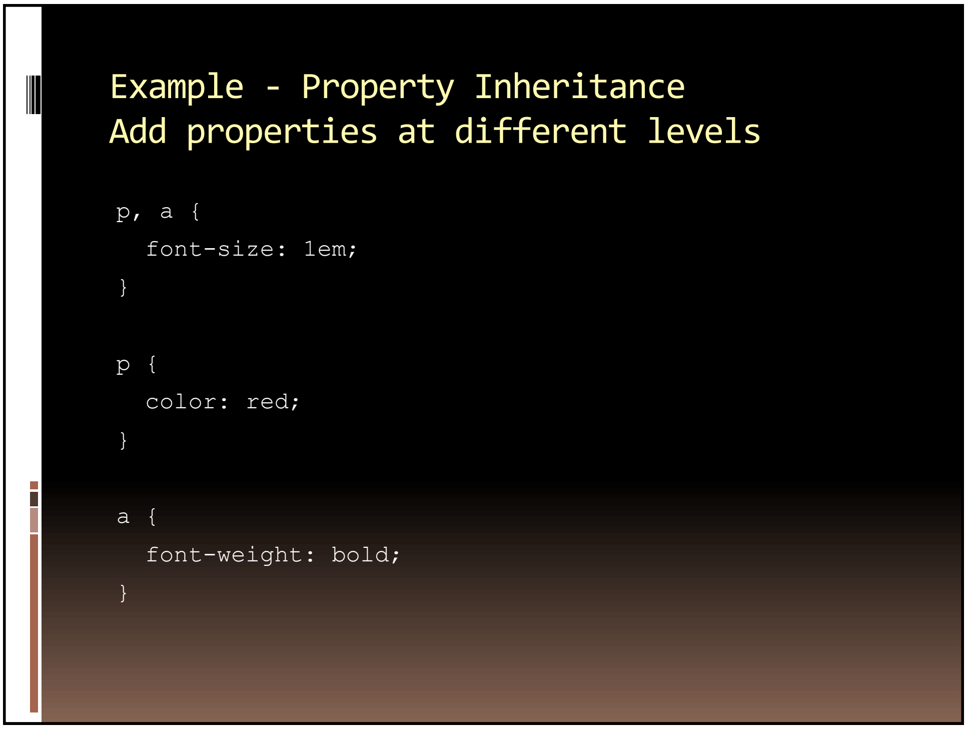
Description:

Property Inheritance

- The same selector specified several times
- More specific selector overwrites the less specific properties
    - overwrites on property level

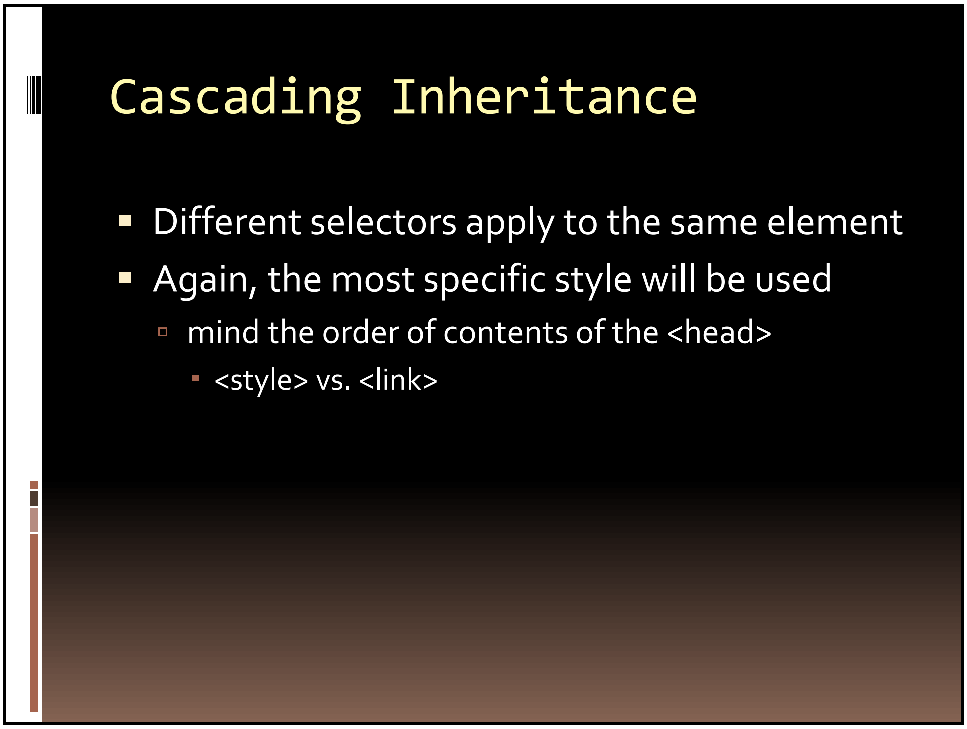
Example - Property Inheritance
Use inheritance instead of the same def.

```
body, div, header, footer, p, li {
  font-size: 18px;
}

/* well sufficient */
body {
  font-size: 18px;
}
```



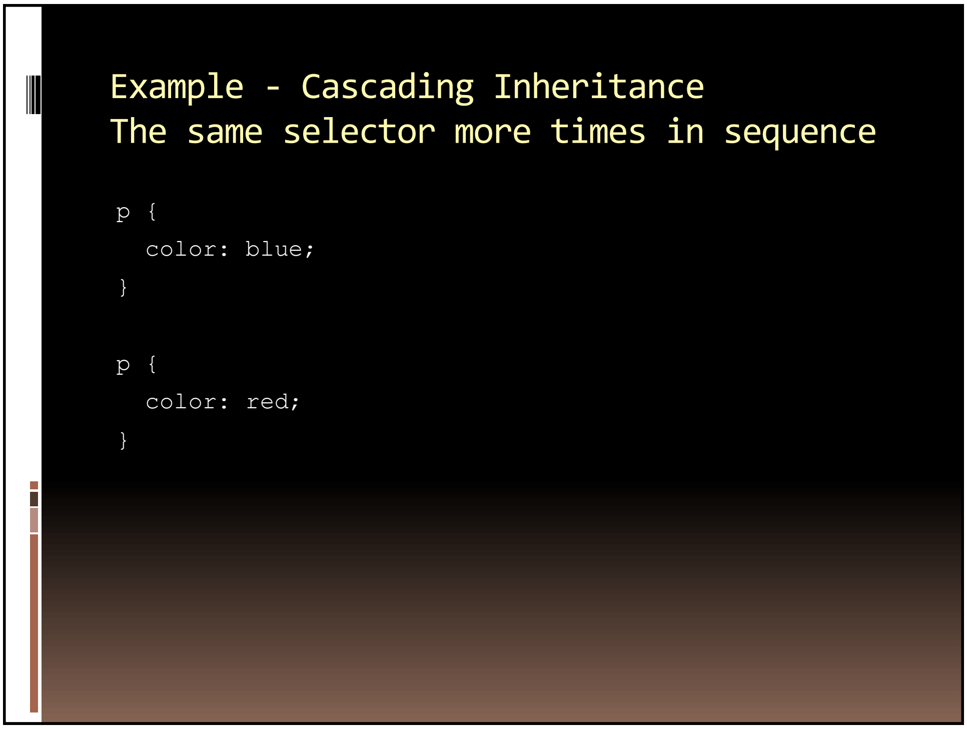
Example - Property Inheritance
Add properties at different levels

```
p, a {
  font-size: 1em;
}

p {
  color: red;
}

a {
  font-weight: bold;
}
```



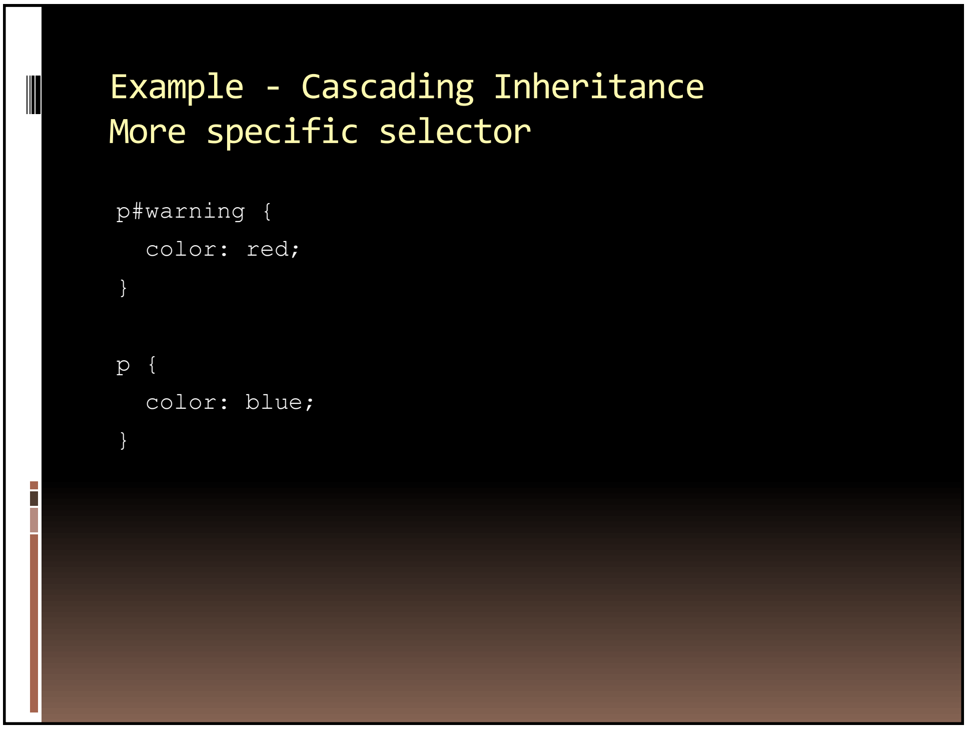
Cascading Inheritance

- Different selectors apply to the same element
- Again, the most specific style will be used
  - mind the order of contents of the <head>
    - <style> vs. <link>



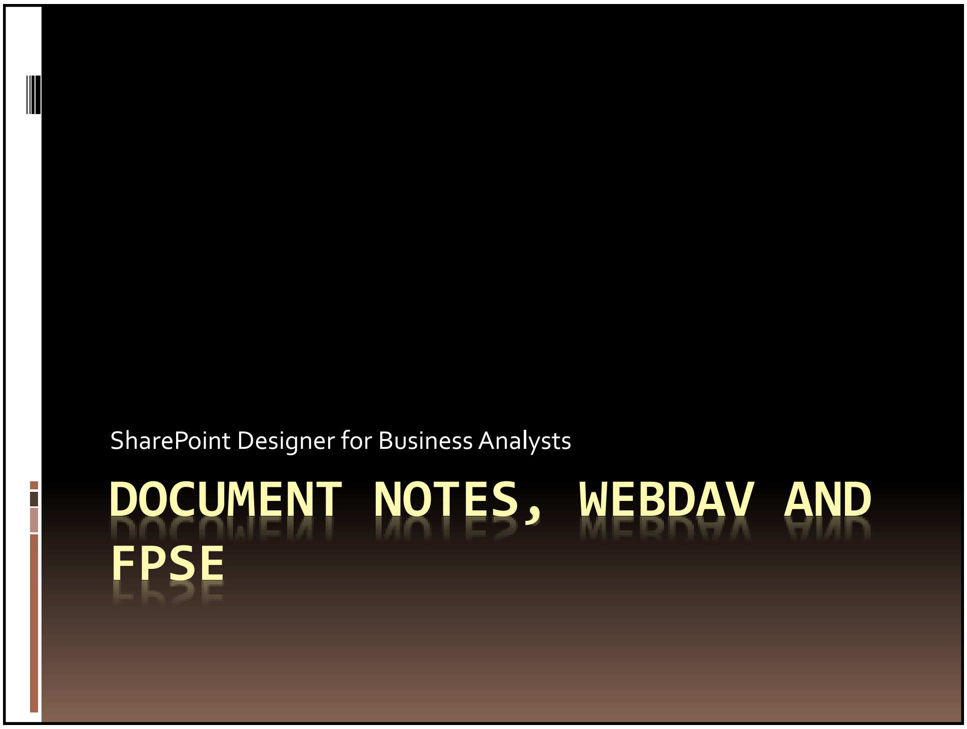
Example - Cascading Inheritance The same selector more times in sequence

```
p {
  color: blue;
}

p {
  color: red;
}
```



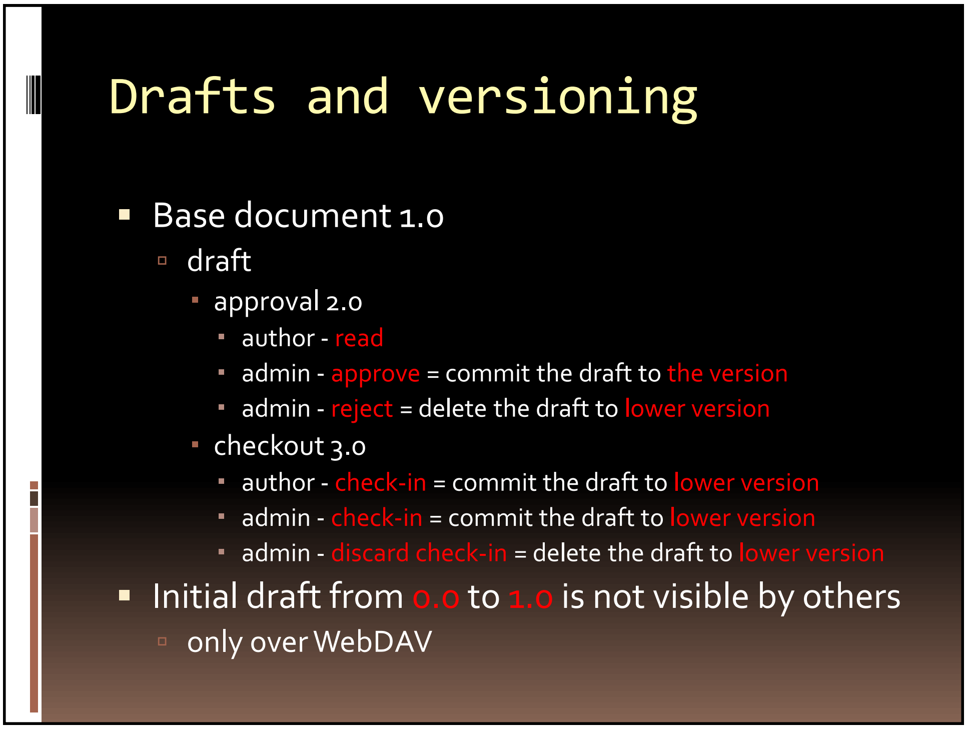
Example - Cascading Inheritance More specific selector

```
p#warning {
  color: red;
}

p {
  color: blue;
}
```



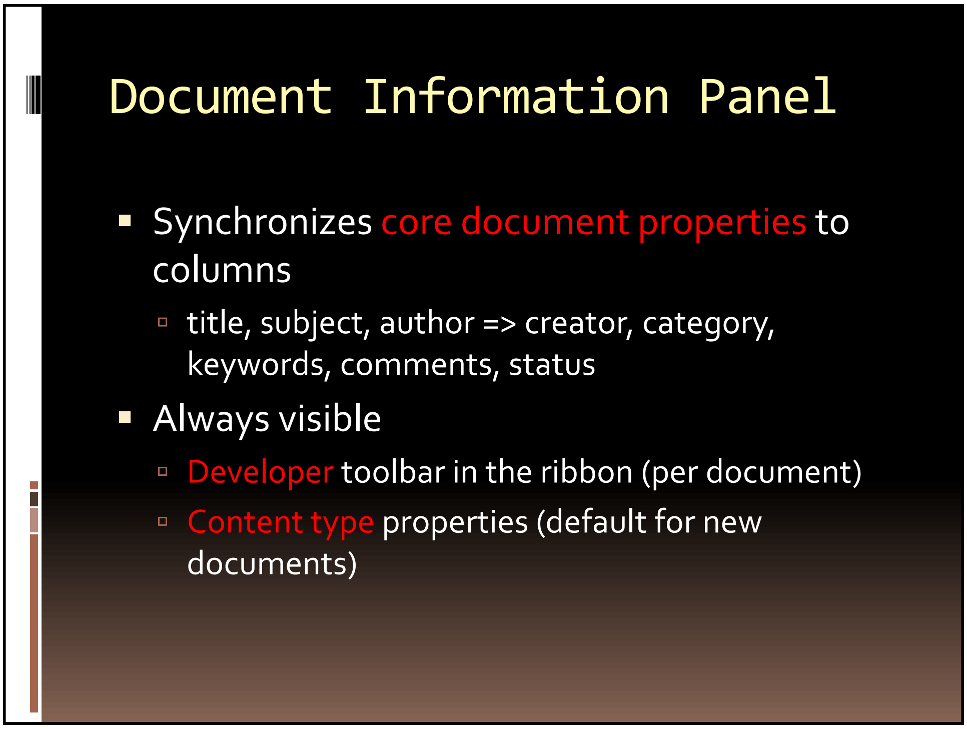
SharePoint Designer for Business Analysts

DOCUMENT NOTES, WEBDAV AND FPSE



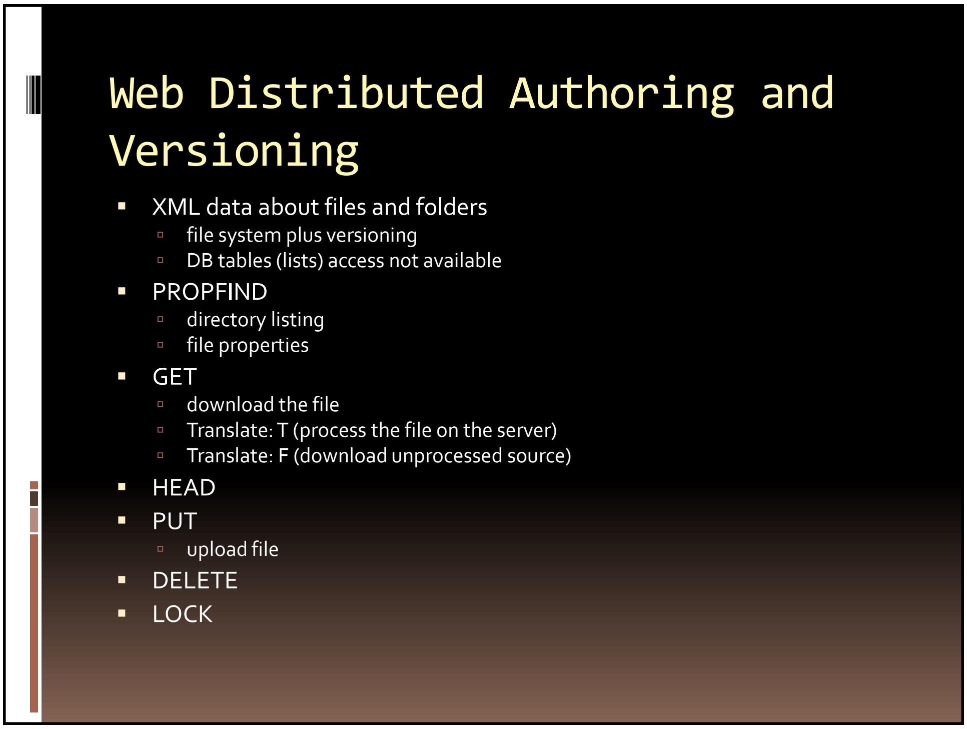
Drafts and versioning

- Base document 1.0
  - draft
    - approval 2.0
      - author - read
      - admin - approve = commit the draft to the version
      - admin - reject = delete the draft to lower version
    - checkout 3.0
      - author - check-in = commit the draft to lower version
      - admin - check-in = commit the draft to lower version
      - admin - discard check-in = delete the draft to lower version
- Initial draft from 0.0 to 1.0 is not visible by others
  - only over WebDAV



Document Information Panel

- Synchronizes core document properties to columns
  - title, subject, author => creator, category, keywords, comments, status
- Always visible
  - Developer toolbar in the ribbon (per document)
  - Content type properties (default for new documents)

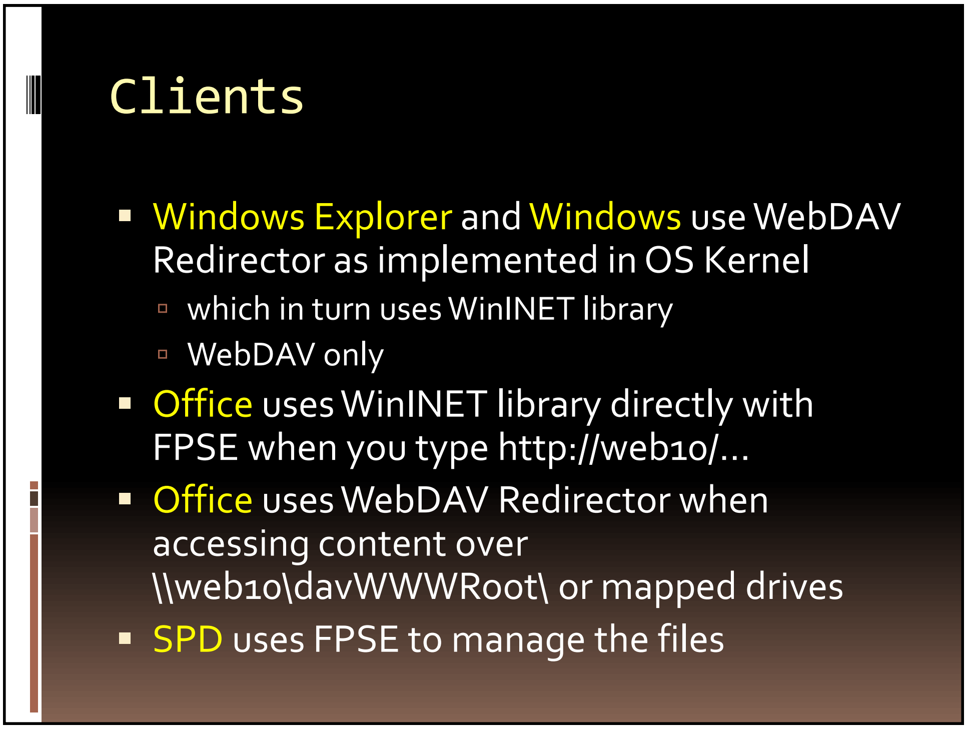


Web Distributed Authoring and Versioning

- XML data about files and folders
  - file system plus versioning
  - DB tables (lists) access not available
- PROPFIND
  - directory listing
  - file properties
- GET
  - download the file
  - Translate: T (process the file on the server)
  - Translate: F (download unprocessed source)
- HEAD
- PUT
  - upload file
- DELETE
- LOCK

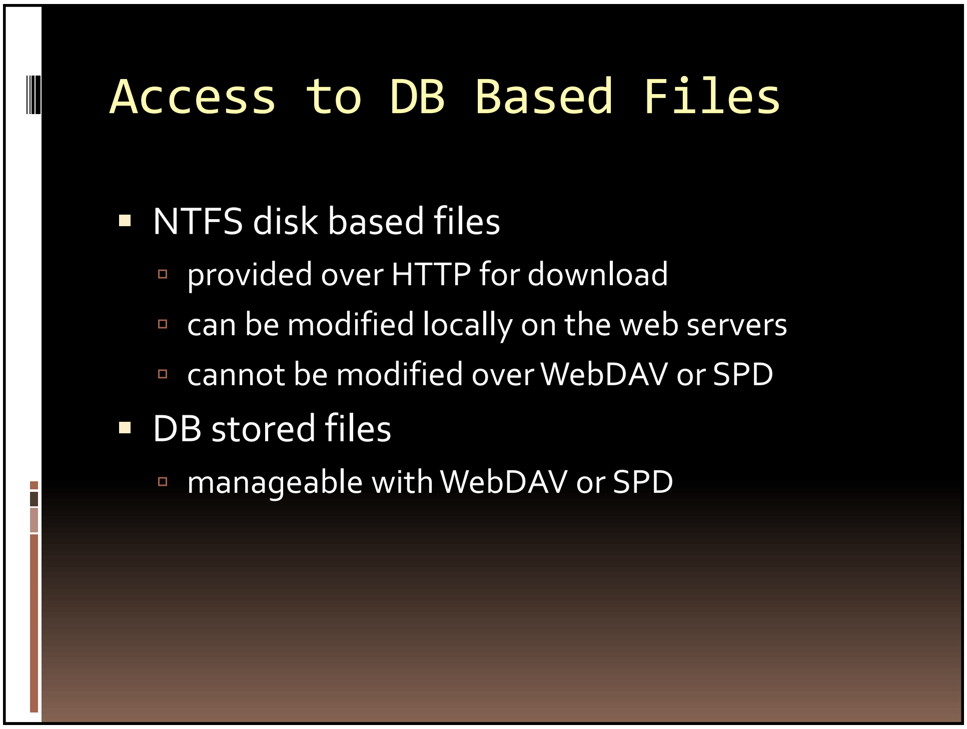
Frontpage Server Extensions

- Custom XML requests using SOAP
  - manage files/folders and database data (lists, etc.)
- HTTP POST, HEAD and OPTIONS requests only



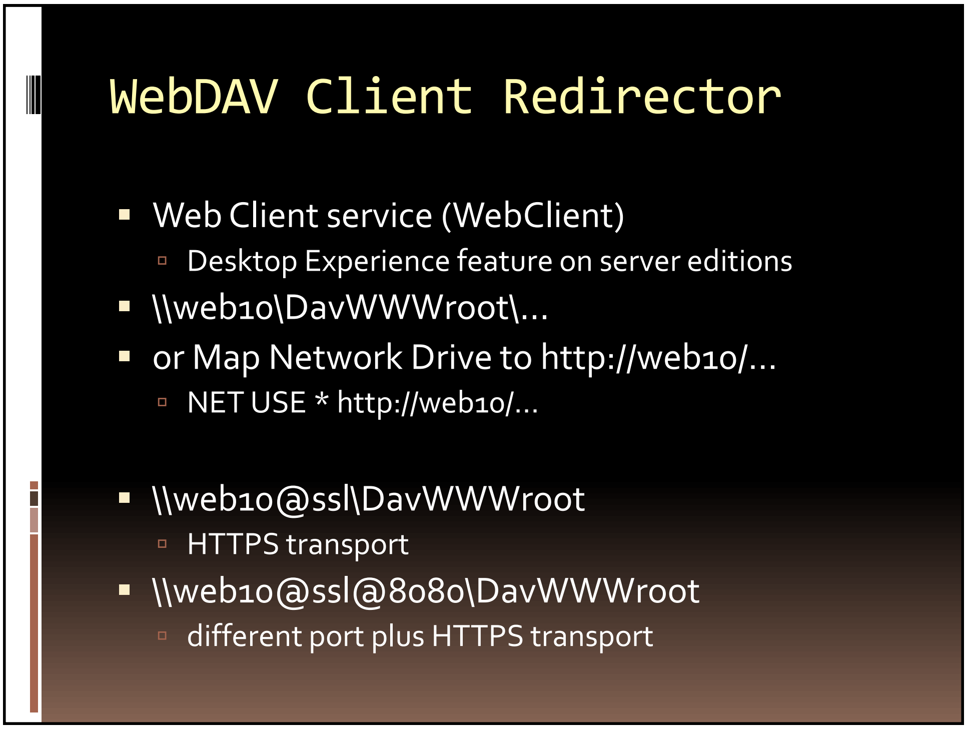
Clients

- Windows Explorer and Windows use WebDAV Redirector as implemented in OS Kernel
  - which in turn uses WinINET library
  - WebDAV only
- Office uses WinINET library directly with FPSE when you type http://web10/…
- Office uses WebDAV Redirector when accessing content over \\web10\davWWWRoot\ or mapped drives
- SPD uses FPSE to manage the files



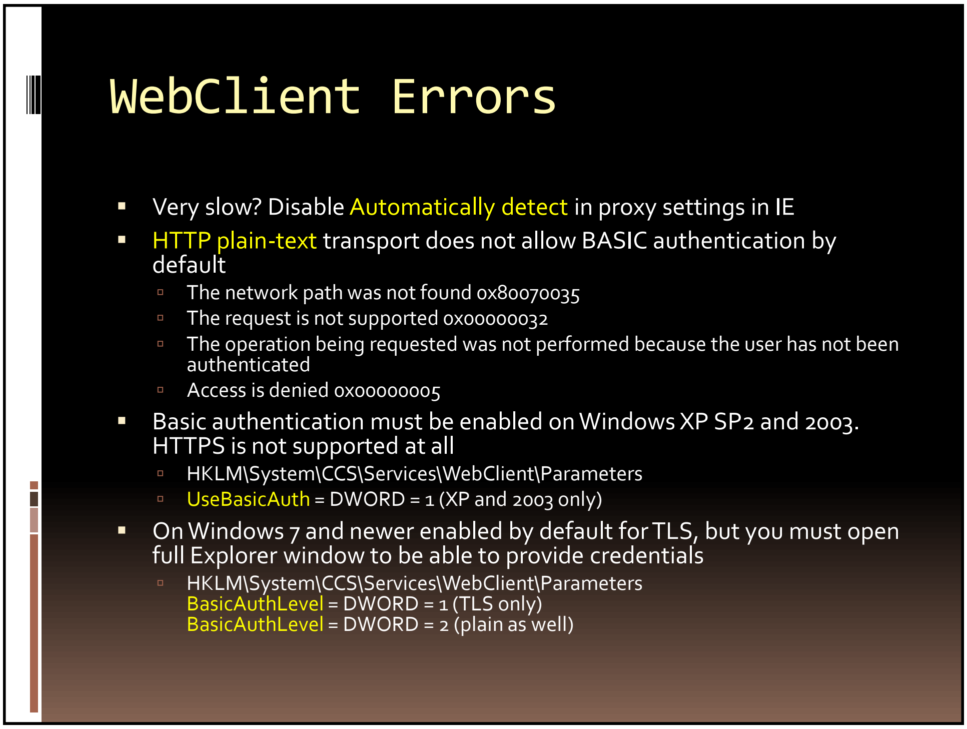
Access to DB Based Files

- NTFS disk based files
  - provided over HTTP for download
  - can be modified locally on the web servers
  - cannot be modified over WebDAV or SPD
- DB stored files
  - manageable with WebDAV or SPD



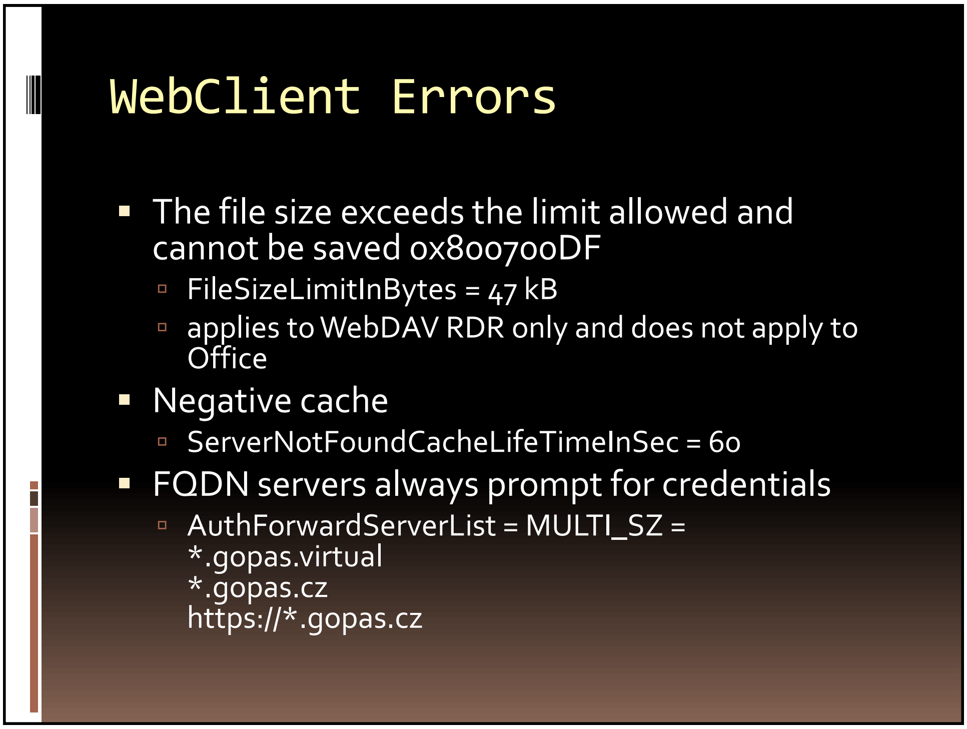
WebDAV Client Redirector

- Web Client service (WebClient)
  - Desktop Experience feature on server editions
- \\web10\DavWWWroot\...
- or Map Network Drive to http://web10/...
  - NET USE * http://web10/...
- \\web10@ssl\DavWWWroot
  - HTTPS transport
- \\web10@ssl@8080\DavWWWroot
  - different port plus HTTPS transport



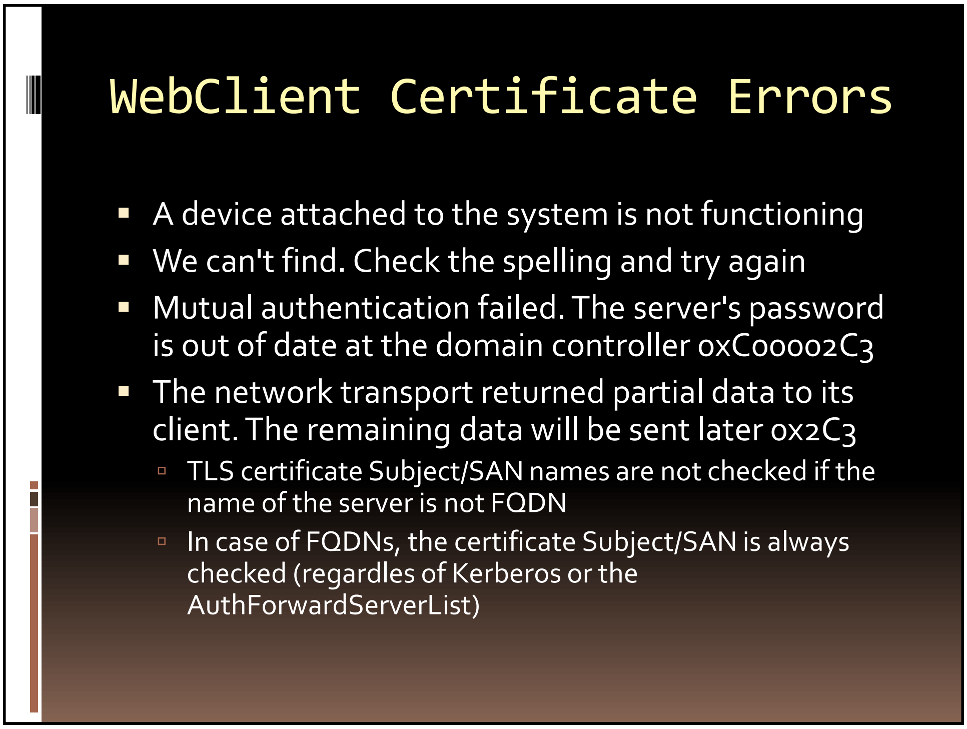
WebClient Errors

- Very slow? Disable Automatically detect in proxy settings in IE
- HTTP plain-text transport does not allow BASIC authentication by default
  - The network path was not found 0x80070035
  - The request is not supported 0x00000032
  - The operation being requested was not performed because the user has not been authenticated
  - Access is denied 0x00000005
- Basic authentication must be enabled on Windows XP SP2 and 2003. HTTPS is not supported at all
  - HKLM\System\CCS\Services\WebClient\Parameters
  - UseBasicAuth = DWORD = 1 (XP and 2003 only)
- On Windows 7 and newer enabled by default for TLS, but you must open full Explorer window to be able to provide credentials
  - HKLM\System\CCS\Services\WebClient\Parameters
BasicAuthLevel = DWORD = 1 (TLS only)
BasicAuthLevel = DWORD = 2 (plain as well)



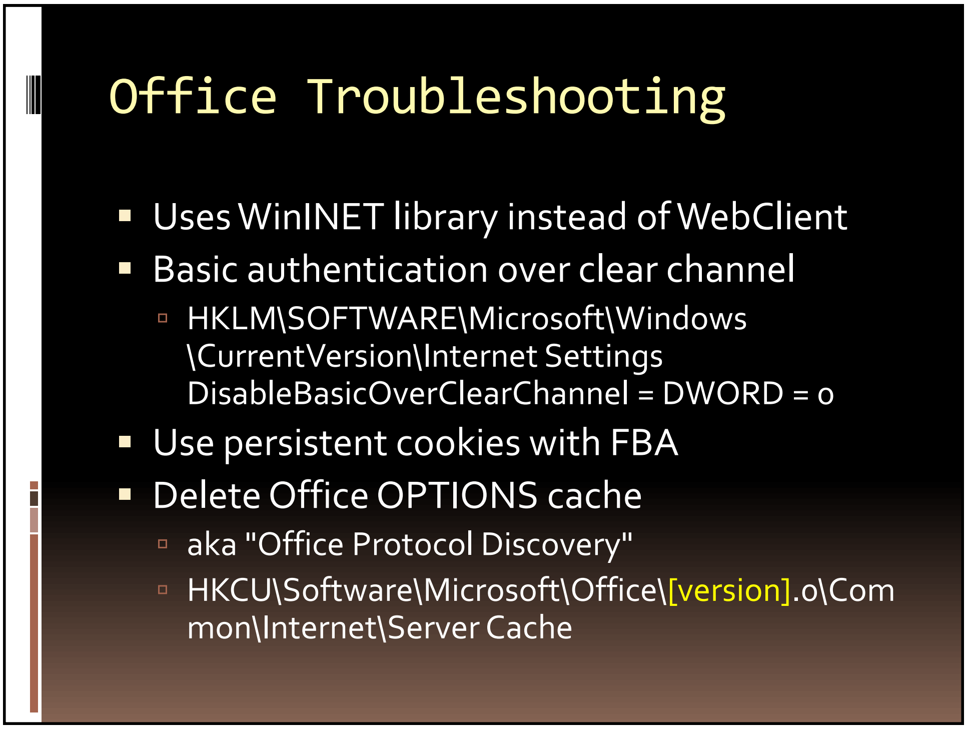
WebClient Errors

- The file size exceeds the limit allowed and cannot be saved 0x800700DF
  - FileSizeLimitInBytes = 47 kB
  - applies to WebDAV RDR only and does not apply to Office
- Negative cache
  - ServerNotFoundCacheLifeTimeInSec = 60
- FQDN servers always prompt for credentials
  - AuthForwardServerList = MULTI_SZ =
    *.gopas.virtual
    *.gopas.cz
    https://*.gopas.cz



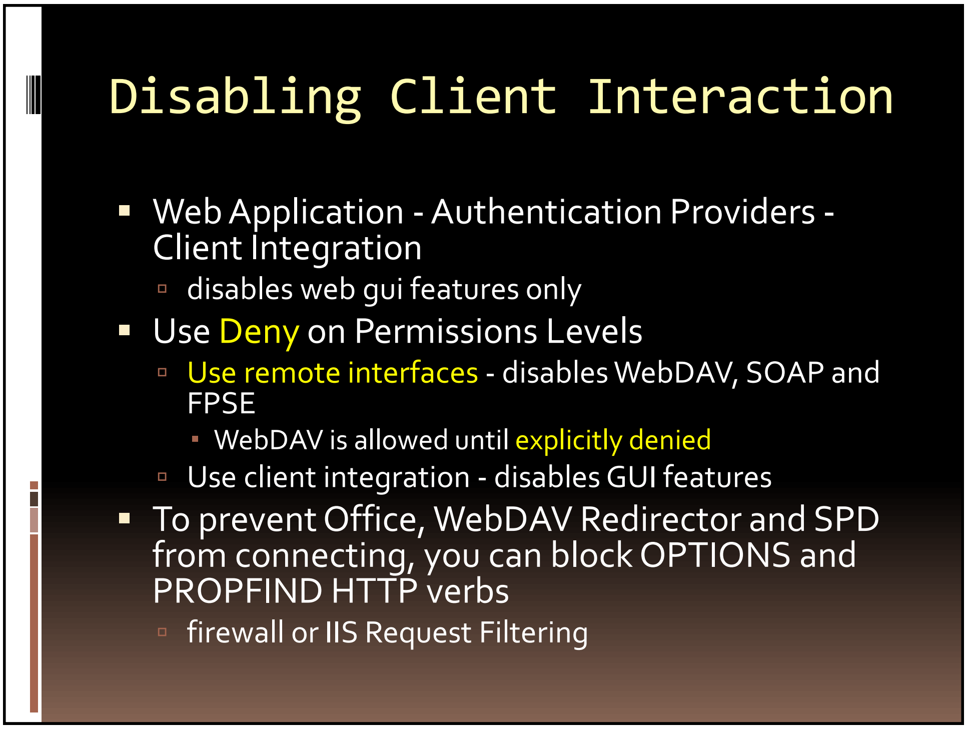
WebClient Certificate Errors

- A device attached to the system is not functioning
- We can't find. Check the spelling and try again
- Mutual authentication failed. The server's password is out of date at the domain controller 0xC00002C3
- The network transport returned partial data to its client. The remaining data will be sent later 0x2C3
  - TLS certificate Subject/SAN names are not checked if the name of the server is not FQDN
  - In case of FQDNs, the certificate Subject/SAN is always checked (regardles of Kerberos or the AuthForwardServerList)



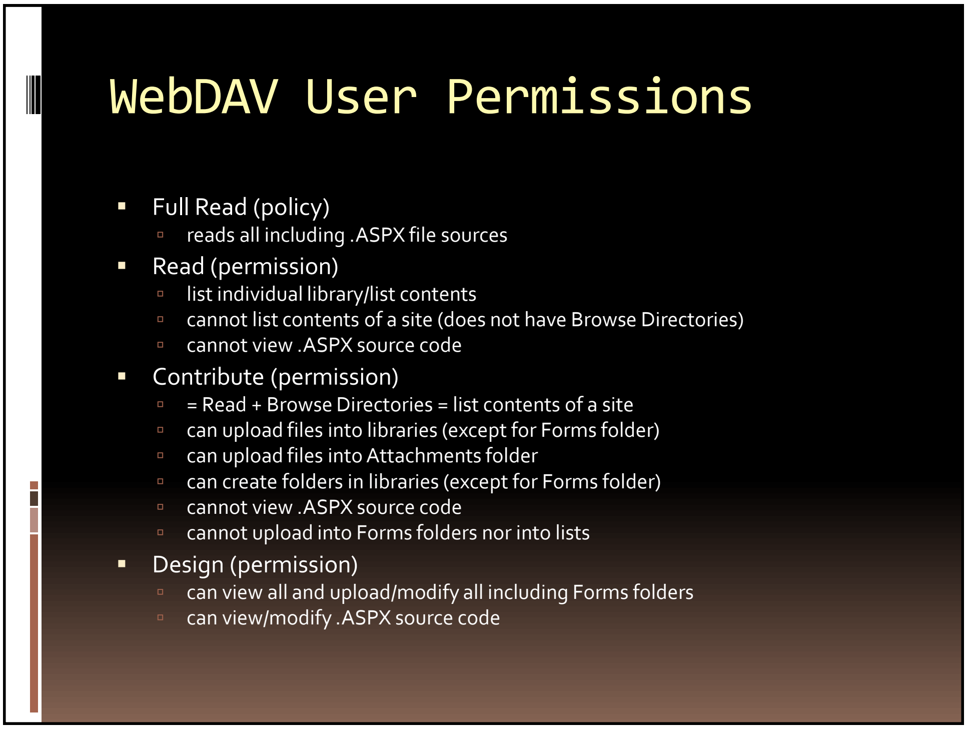
Office Troubleshooting

- Uses WinINET library instead of WebClient
- Basic authentication over clear channel
  - HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\Internet Settings DisableBasicOverClearChannel = DWORD = 0
- Use persistent cookies with FBA
- Delete Office OPTIONS cache
  - aka "Office Protocol Discovery"
  - HKCU\Software\Microsoft\Office\[version].0\Common\Internet\Server Cache



Disabling Client Interaction

- Web Application - Authentication Providers - Client Integration
  - disables web gui features only
- Use Deny on Permissions Levels
  - Use remote interfaces - disables WebDAV, SOAP and FPSE
    - WebDAV is allowed until explicitly denied
  - Use client integration - disables GUI features
- To prevent Office, WebDAV Redirector and SPD from connecting, you can block OPTIONS and PROPFIND HTTP verbs
  - firewall or IIS Request Filtering

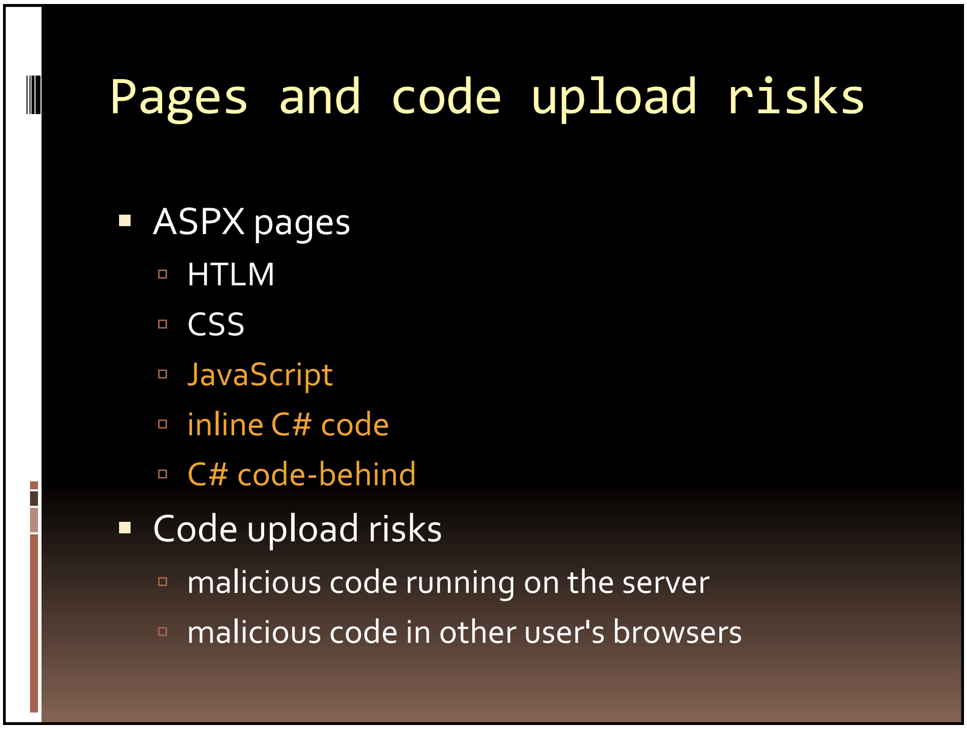


WebDAV User Permissions

- Full Read (policy)
  - reads all including .ASPX file sources
- Read (permission)
  - list individual library/list contents
  - cannot list contents of a site (does not have Browse Directories)
  - cannot view .ASPX source code
- Contribute (permission)
  - = Read + Browse Directories = list contents of a site
  - can upload files into libraries (except for Forms folder)
  - can upload files into Attachments folder
  - can create folders in libraries (except for Forms folder)
  - cannot view .ASPX source code
  - cannot upload into Forms folders nor into lists
- Design (permission)
  - can view all and upload/modify all including Forms folders
  - can view/modify .ASPX source code

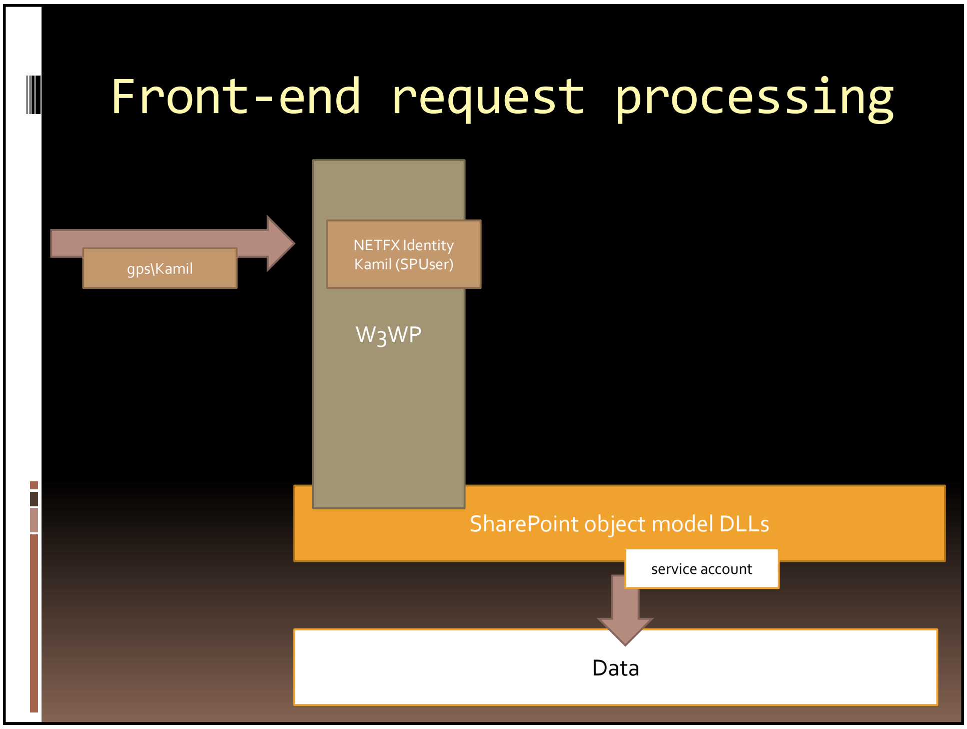
SharePoint Designer for Business Analysts

HTML CODE IN SHAREPOINT



Pages and code upload risks

- ASPX pages
  - HTLM
  - CSS
  - JavaScript
  - inline C# code
  - C# code-behind
- Code upload risks
  - malicious code running on the server
  - malicious code in other user's browsers



Front-end request processing

gps\Kamil

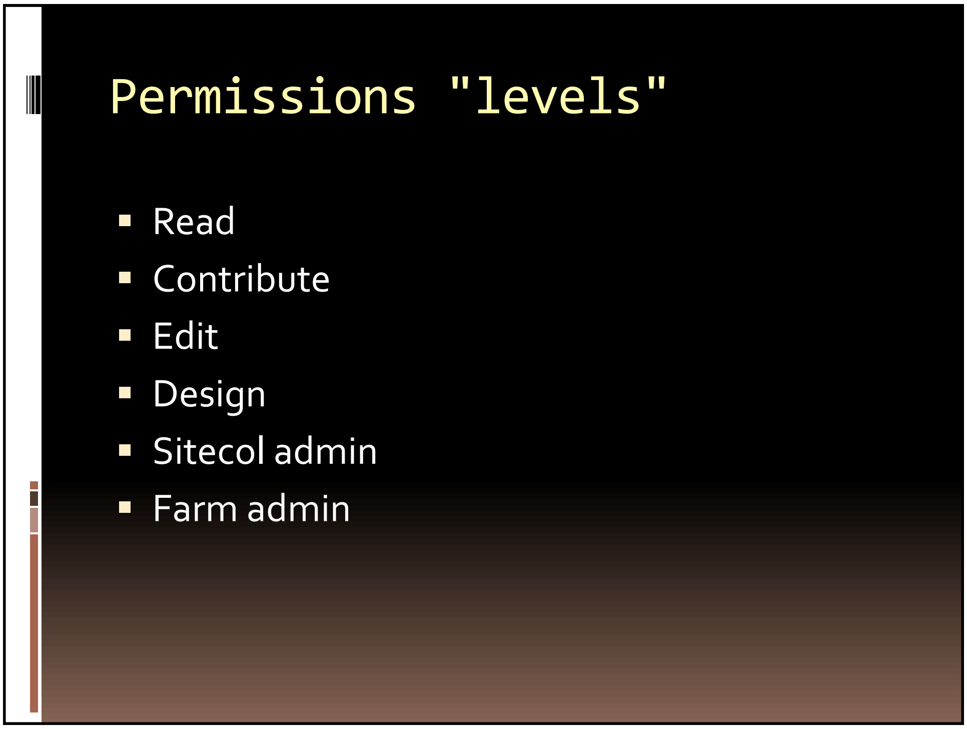
NETFX Identity
Kamil (SPUser)

W3WP

SharePoint object model DLLs

service account

Data

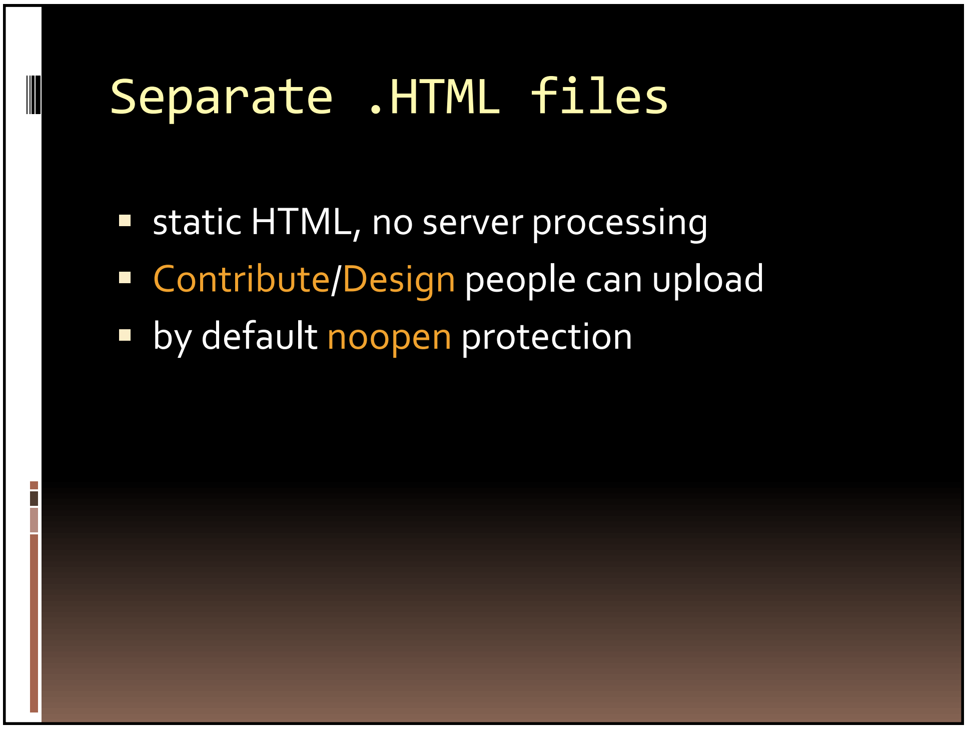


Permissions "levels"

- Read
- Contribute
- Edit
- Design
- Sitecol admin
- Farm admin

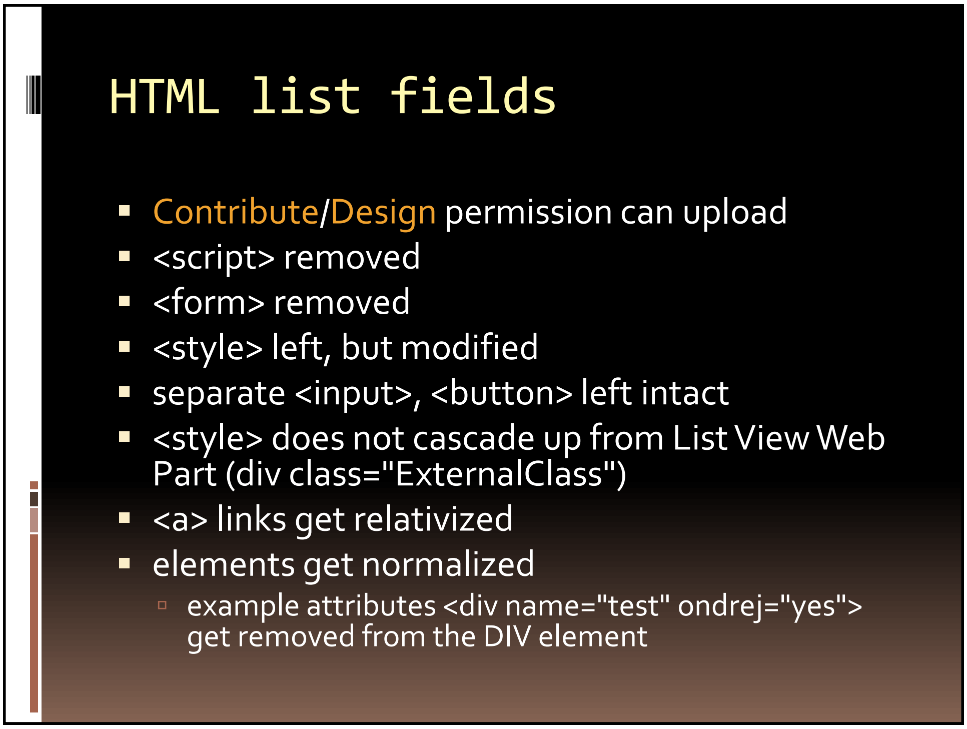
Content and code upload

- Raw HTML file
- List HTLM fields
- Content editor web part
- Wiki page web page
- Raw ASPX code through WebDAV or SPD
- Features and solutions with DLL
  - sandboxed solutions - sitecol admins
  - farm solutions - farm admins
  - https://msdn.microsoft.com/en-us/library/ff798382.aspx



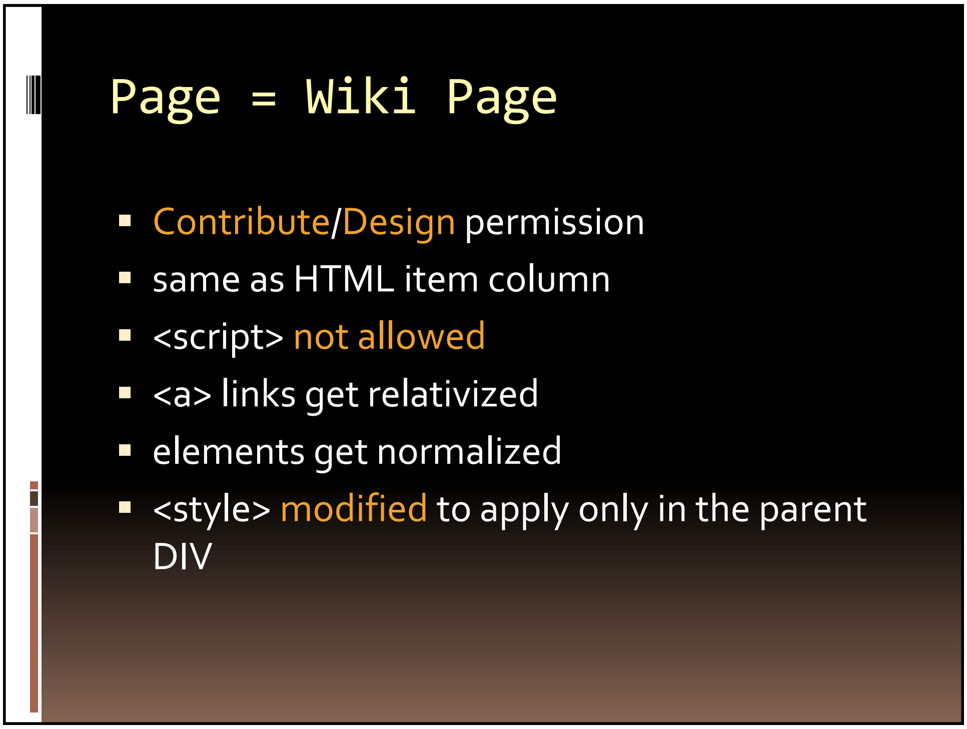
Separate .HTML files

- static HTML, no server processing
- Contribute/Design people can upload
- by default noopen protection



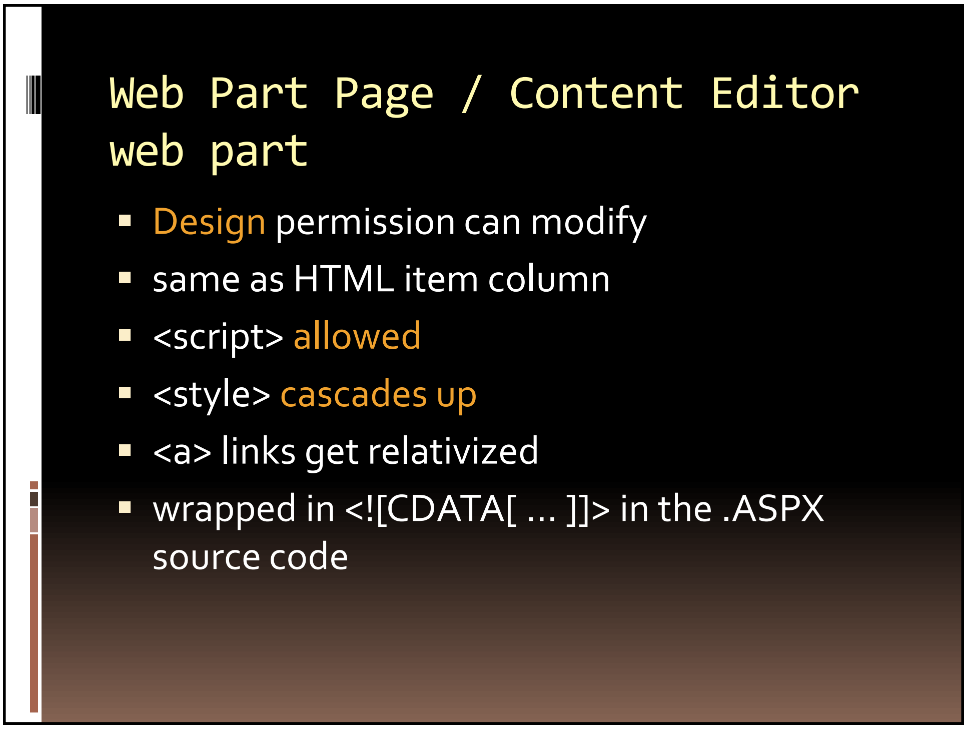
HTML list fields

- Contribute/Design permission can upload
- <script> removed
- <form> removed
- <style> left, but modified
- separate <input>, <button> left intact
- <style> does not cascade up from List View Web Part (div class="ExternalClass")
- <a> links get relativized
- elements get normalized
  - example attributes <div name="test" ondrej="yes"> get removed from the DIV element



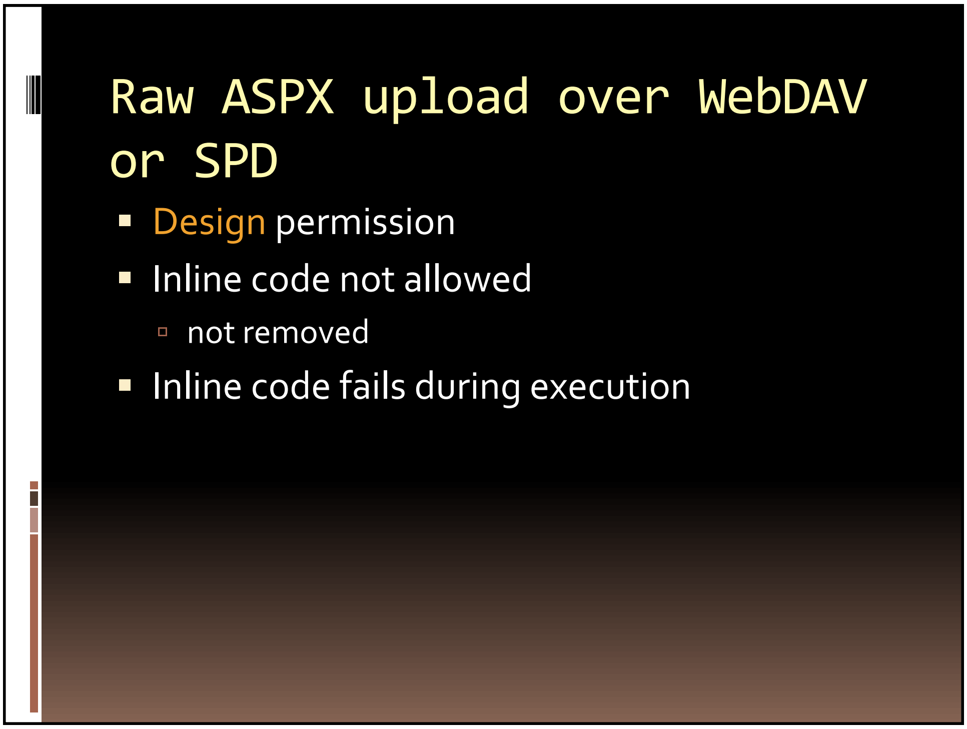
Page = Wiki Page

- Contribute/Design permission
- same as HTML item column
- <script> not allowed
- <a> links get relativized
- elements get normalized
- <style> modified to apply only in the parent DIV



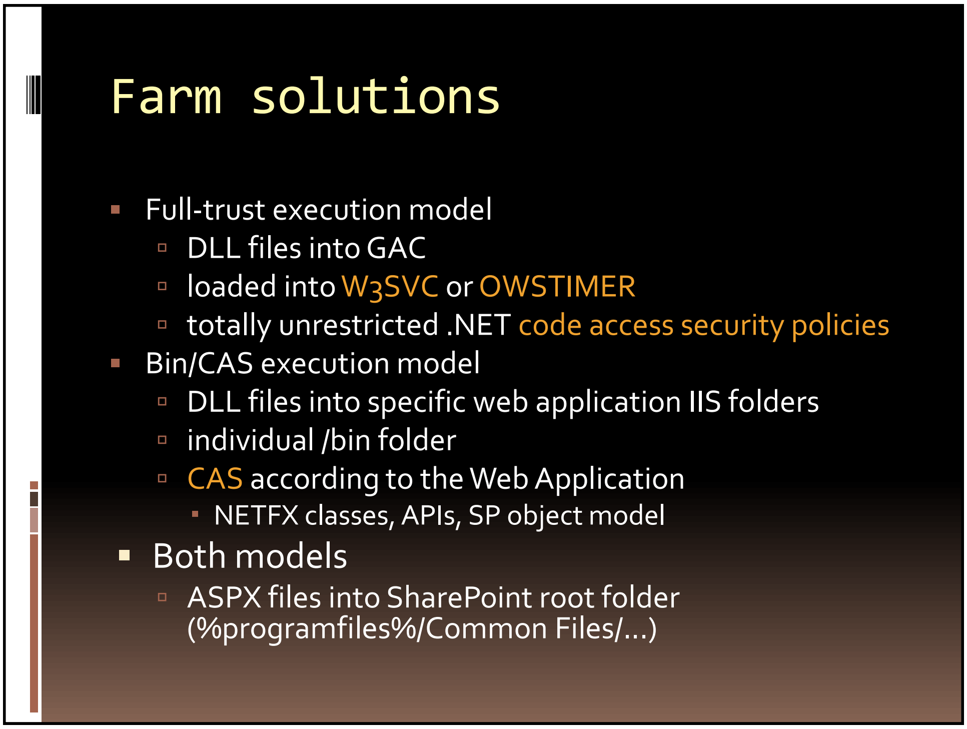
Web Part Page / Content Editor web part

- Design permission can modify
- same as HTML item column
- <script> allowed
- <style> cascades up
- <a> links get relativized
- wrapped in <![CDATA[…]]> in the .ASPX source code



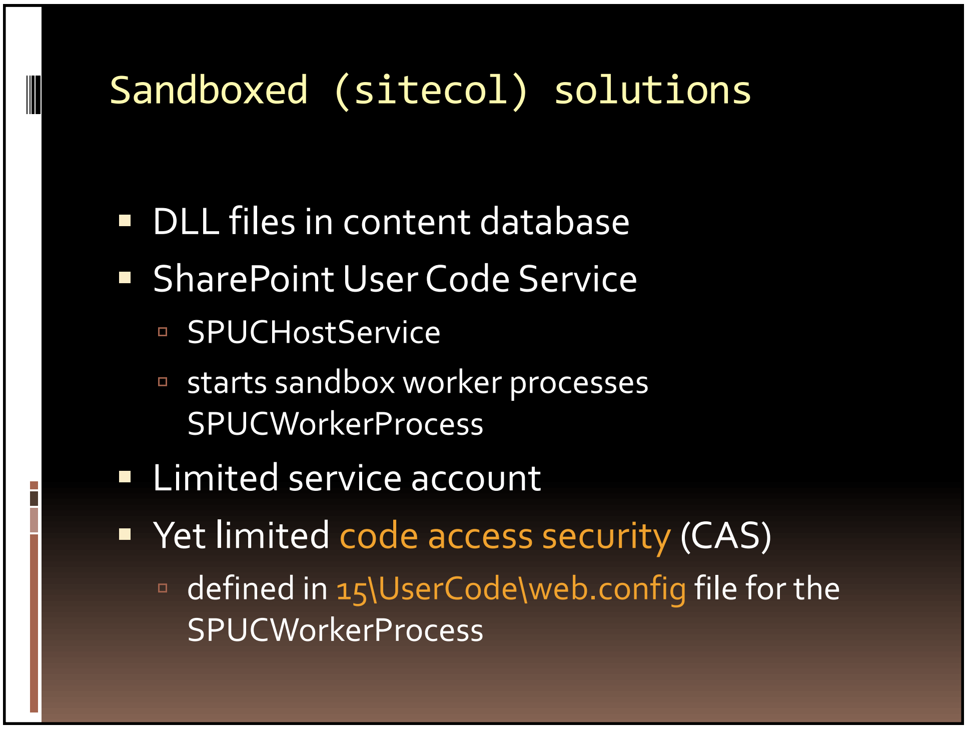
Raw ASPX upload over WebDAV or SPD

- Design permission
- Inline code not allowed
  - not removed
- Inline code fails during execution



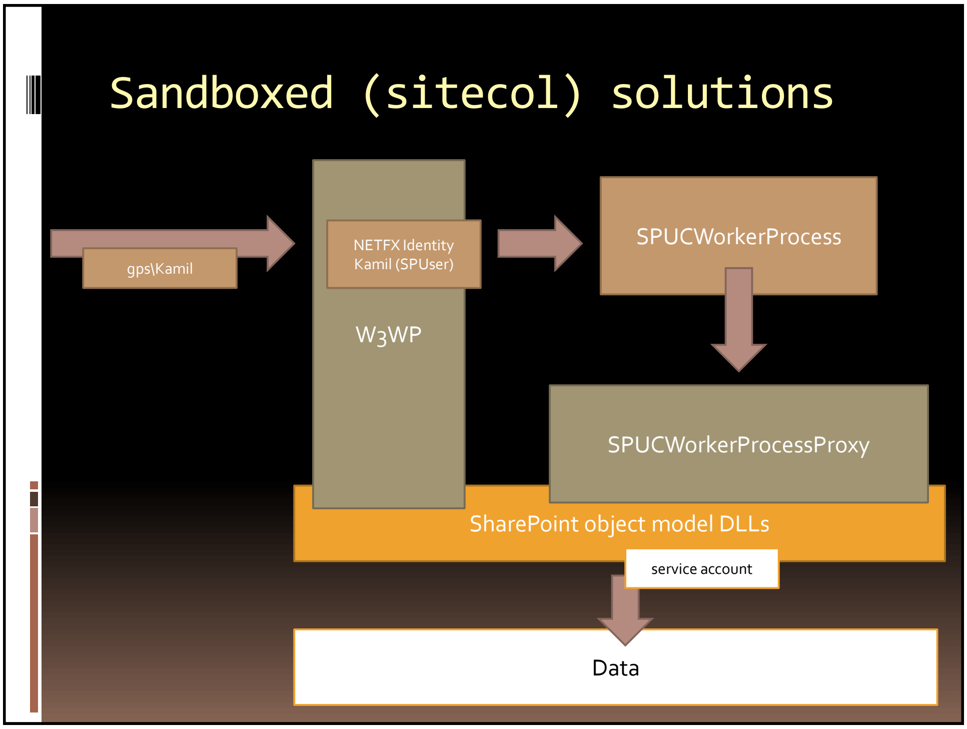
Farm solutions

- Full-trust execution model
  - DLL files into GAC
  - loaded into W3SVC or OWSTIMER
  - totally unrestricted .NET code access security policies
- Bin/CAS execution model
  - DLL files into specific web application IIS folders
  - individual /bin folder
  - CAS according to the Web Application
    - NETFX classes, APIs, SP object model
- Both models
  - ASPX files into SharePoint root folder (%programfiles%/Common Files/...)



Sandboxed (sitecol) solutions

- DLL files in content database
- SharePoint User Code Service
  - SPUCHostService
  - starts sandbox worker processes SPUCWorkerProcess
- Limited service account
- Yet limited code access security (CAS)
  - defined in 15\UserCode\web.config file for the SPUCWorkerProcess



Sandboxed (sitecol) solutions

gps\Kamil

NETFX Identity
Kamil (SPUser)

W3WP

SPUCWorkerProcess

SPUCWorkerProcessProxy

SharePoint object model DLLs

service account

Data