作者：A11riseforme

来自：法客论坛（F4ckTeam）

Q　Q：1075005528

邮箱：a11riseforme0217@gmail.com

其实也不是什么新鲜的技术，写出来就当作是普及下姿势好了。

昨天玩命写了个检测报告，发给我看了下，写的挺不错的~这里鼓励鼓励。然后他说还有个问题，就是大马传不上去，大马传上去了也不解析。我就觉得很奇怪，一句话都能解析，大马为什么不能解析，于是我叫他把一句话发给我让我看看。

地址 http://www.xxzhiyuan.cn/zyadmin/databackup/razgriz.asp 密码我就不说了，因为是别人的 shell。

自己试着上传一个大马然后访问，如图。

要看的不是满页的乱码，注意前两行

出现了一个 url 和一个邮箱，我到我上传的马里查找，却没有查找到这个 url 和邮箱，下面的内容均是大马的加密内容

把 url 放到百度上搜了下，呵呵，知道怎么回事了。

彩瓦机械资料站 - 汇总国内主要彩瓦机厂家、彩瓦机参数、配制、性...

文件被禁止,请联系管理员!如果您是代理商请联系我们1、http://support.xirang.com/ 2、400-668-0991；如果您是马儿爱好者，请联系wanglubo@foxmail.com。...

caiwaji.net/ 2011-12-16 - 百度快照

黑龙江伊春金春阁木雕工艺品厂

文件被禁止,请联系管理员!如果您是代理商请联系我们1、http://support.xirang.... 邮箱：271208514@QQ.com QQ:271208514 地址:黑龙江伊春市峰园路 1180号 ...

jinchunge.com/ 2011-12-18 - 百度快照

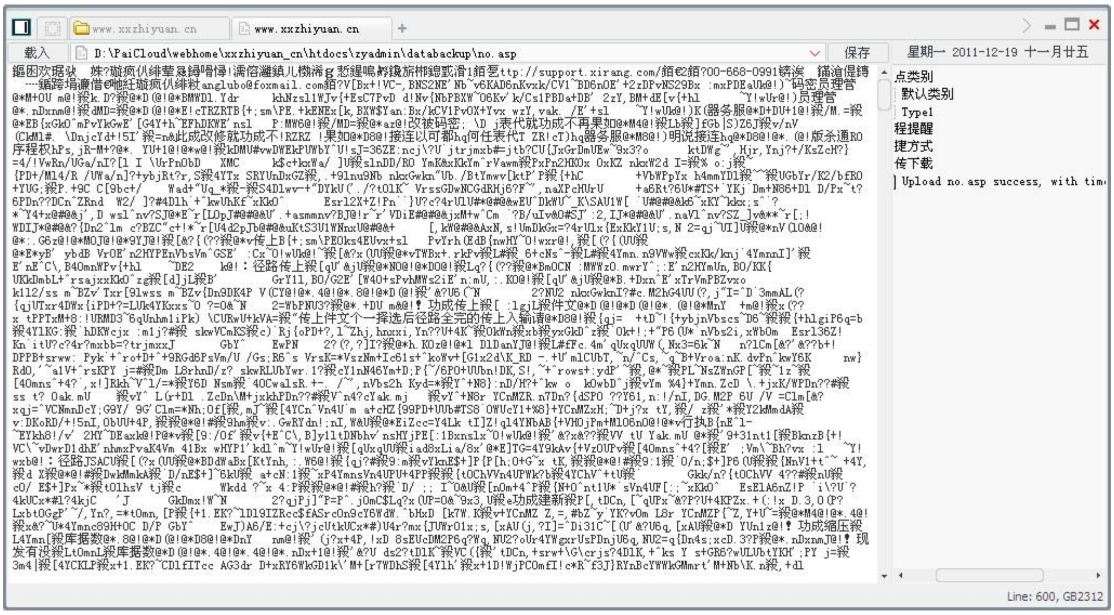
Search Search: - 彩瓦机械资料站

濡傛灉镇人槲浠ｇ惄鍟呜 鑲旗郴鎴戓滑1銆乏ttp://support.xirang.com/銆€2銆?00-668-0991锌涘 鐩沧偍鎼 ···鍎跨捐濂借€呫紝璇疯仈绯粊anglubo@...

www.caiwaji.net/search.asp 2011-12-9 - 百度快照

没有见过这种的过滤监控系统（见过也忘了），跑到菜刀里编辑我上传的大马

果然，我的大马的内容被替换了一部分。这个监控真猥琐。

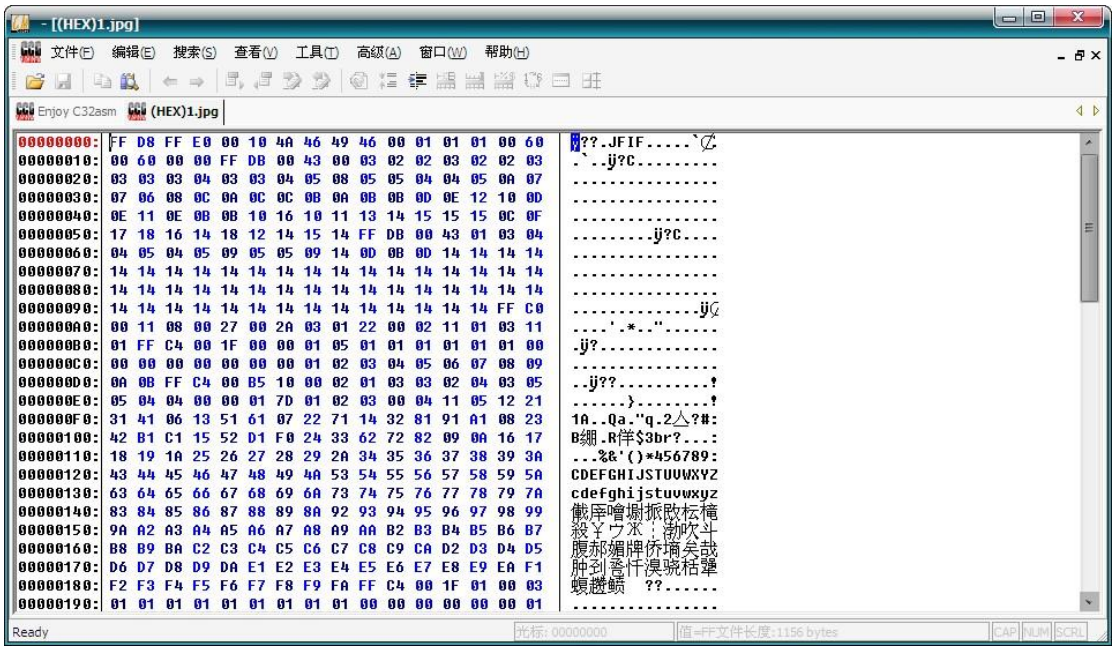


换一个 gif 伪装的图片马试试，加上 GIF 头，gif89a，利用 iis6.0 解析漏洞，后缀为 asp;.jpg，上传，访问。

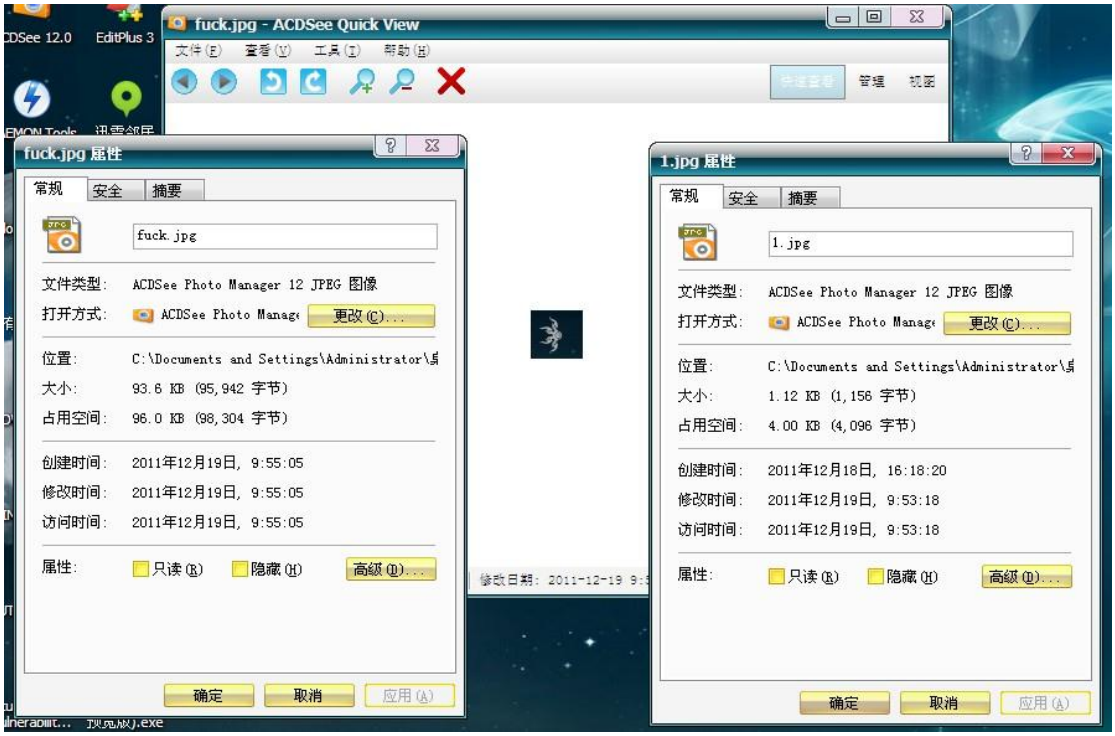
还是被过滤了。

没办法，出大招了，祭出杀器。。。。。。。。。。。。。。。。。。。。。。。。 C32ASM。。。。。。。。。。

随便截了一张图，保证体积尽量小点，原因你后面会知道的。用 c32 以 16 进制打开

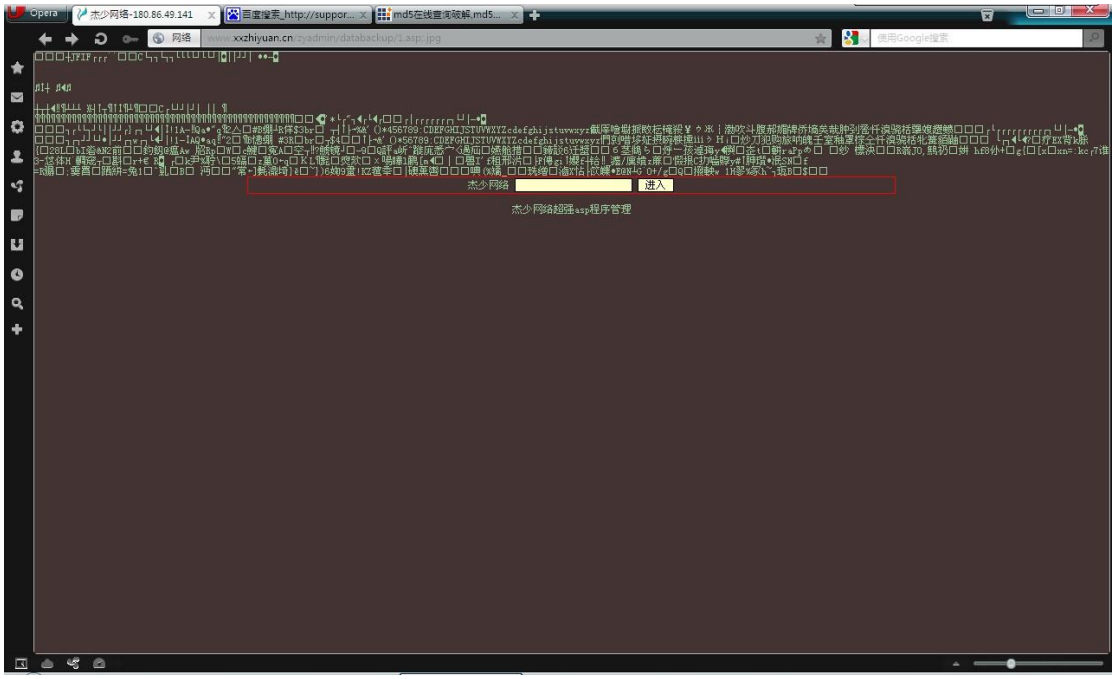


直接拖到最后面，加一个空格之后把我们的大马内容复制进去。然后另存为一张 jpg 图片。



大家可以看看效果，打开仍然可以正常打开，看上去是一张正常的图片，但是看属性，大小就增加了很多。（fuck.jpg 是经过编辑的图片，1.jpg 是原图片） 样本图片马我待会儿会发出来。把制作好的图片马重命名为 1.asp;.jpg

访问



成功，没有被杀，上面那几行乱码就是原图片的内容了，现在知道为什么开始说尽量选一张比较小的图片了吧。就是这个原因，如果图片大了，可能乱码就看着头晕了。

就到这里，顺便提一下，我记得还有一个方法是做一张 jpg 的图片马，然后在另外一个 asp 中 include 一下，但是这里应该也是不成功的。因为他检测到图片里有木马代码直接就给你替换了内容。