文章很烂，赏脸的将就着看下吧....！

路过某赌博站过程

自己记录下，感觉做什么事都是一个耐心的过程！

前段时间[null](http://www.helloroot.net/)发给我个URL  说x W。奔着这个数字在被跨省被砍的风险看了下

目标站: [http://www.fuck.com](http://www.fuck.com/) ip:1.1.1.203

随意的看了下，这站做的还满不错，听说做的满大！



感觉像这样的大站，主站是不会有什么明显的漏洞的！

但还是抱着一丝希望，用Netsparker 扫扫，Netsparker速度可能比较慢，但功能还是很全，只不过是免费版的有很多限制 !

同时看了下目标C段比较临近的50个IP(跨度太大很可能不在同一网关或交换下，如果服务器是在机房的话)

发现也只有3个站！其中两个还得翻墙，而且是\*nix 服务器，由于对linux 不是很熟悉，只能果断的选择最后而且是唯一的站(xxx.com ---ip 1.1.1.234)下手了。

弱口令进入后台，IIS6解析漏洞拿下此站。发现是星外的虚拟主机，只支持asp 和php ..

并且都不能执行命令。正准备放弃的时候发现E:\Program Files\MySQL\ 目录可写.。

到T00LS看了下，发现最近[Rices](http://www.hkrices.com/) 发了个lpk.dll 后门...果断下载设置好热键丢到上面！

试试asp php 循环的代码，想至服务器死机、重启。发现完全木有效果！

可能只有用最猥琐的方法了，那便是DDOS..如果木有硬防神马的一般死翘翘 ！

Q上很久木联系黑阔 某某。。叫他帮忙DDOS下。。无果。把shell 丢给null。

看看时间已经8点多了。果断出去吃饭！

后来null 找人用10多台服务器和某某一起把目标打死了，这么邪恶，完全不是我的风格！

连接终端，可爱的sethc.exe 不出意外的被替换鸟。嘿嘿，小小的笑一下！

可惜啊，ping 目标IP & arp -a  发现木有获取到目标mac

难道就这么悲剧么，不甘心的nslookup ip 看了下 ， 还真不在同一网关...

唉！ 回来看看Netsparker 的扫描结果，



惊现注射....，我有点不淡定了。。于是post 了个没完..(刚开始俺还脑残般的用nc 一次次的改包，提交，/囧)，用寂寞的刺猬的post 工具post了半天。数据目录什么都没能列出来，头很晕，技术有限啊！。

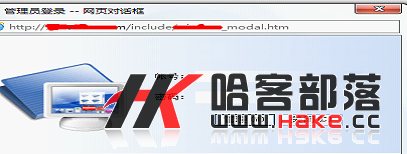
蛋疼的操上收集的字典扫它后台试试，有时RP这东西真是没发说清。

和null 讨论着仓老师的时候，无意的打开扫描界面

看到红色的/sysmanage/index.aspx

打开看了下，还有些页面没做权限设置！可惜也只能看，不能操作！

可惜被我注意到了个小细节，每次打开一些做了权限判断的页面时他会弹出如下页面



邪恶的在google.com.sb 搜索之，发现某站上显示的是广州市xx计算机有限公司

目标是自己修改了。

找到那公司网站，



一共四套，也不知道目标用的是哪套，不过有一套可以试用，在后台翻了半天终于被俺发现了两搜索型注射，SA权限，直接exec master.dbo.xp\_cmdshell ’你懂的’;  
日下，远程终端连接之，神马后门的往上丢了个遍...源码打包！继续探讨仓老师睡觉！

N天后，继续

经过对比后发现目标为0A政府版。

对N个文件测试 终于被俺找到几个未判断权限滴页面

SysManage/sys\_sql.aspx 可执行SQL 命令，可惜没回显，没啥结果！

/include/install.aspx 这个就不一样了



Telnet ip 1433 无果，尝试着用日下OA系统的 webshell(aspxspy)竟然可以连接，！

Sa权限，恢复组件没成功。那就列目录呗，log备份得到shell.。日下后才发现只有部分数据在服务器上面。

于是。。。黄了！。。

PS：简单的记录了下，其中可能还有很多细节也没能写出来，也忘记的差不多了！