# 任意文件下载漏洞复现

任意文件下载漏洞在internet上少之又少，但是如果存在，那么拿webshell会变的非常容易，因为任意文件下载漏洞可以下载一些敏感文件：比如配置文件，数据库文件，登录检验源码等，可以扩大自己的信息资源，从而轻松拿站。

因为找了很久没有找到存在该漏洞的框架或站点，于是自己做了一个存在任意下载漏洞的站点来复现一下，需要的朋友可以找我要源码。

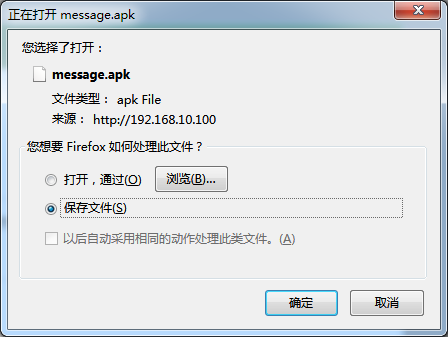
首先登录留言系统，使用的是普通账号登录的



进去到主界面后可以看到旁边有个红色的app下载接口



点击**下载最新版APP**则会弹出下载框。



这个链接提供了下载接口，可以按Ctrl + U查看源码，看看这个链接到底是什么



download.php?dir=software&filename=message.apk

看到这个链接传递了两个GET参数，一个是文件名，另一个是文件位置，那么这种链接很有可能存在任意下载漏洞，为了验证是否存在，我们可以自己构造一下这个链接，比如尝试下载根目录下的index.php代码文件，如下

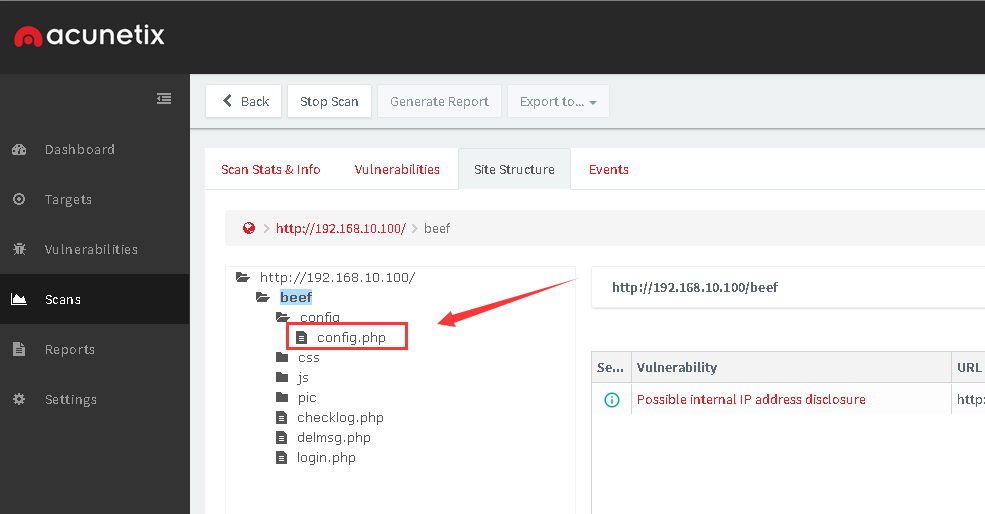
**http://192.168.10.100/beef/download.php?dir=.&filename=index.php**

然后用浏览器访问该地址，就可以弹出index.php的下载框框，惊不惊喜？意不意外？



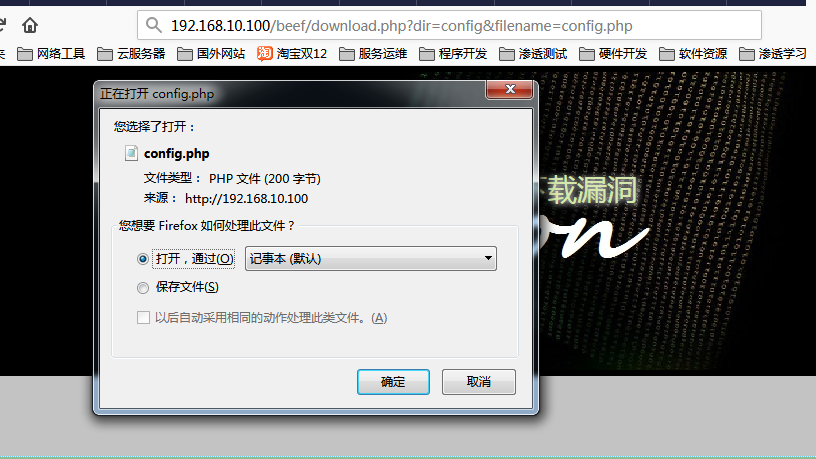
有了这个下载漏洞，我们肯定要想办法把数据库文件或者配置文件下载下来，因为上面有一些敏感的信息

为了效率，我们直接用AWVS放蜘蛛对他爬取一下，看看有哪些敏感目录

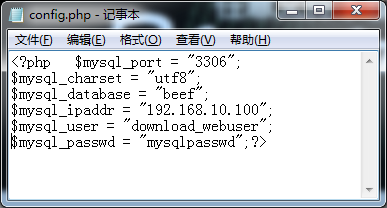


可以看到config目录下面有个config.php，使用漏洞下载他

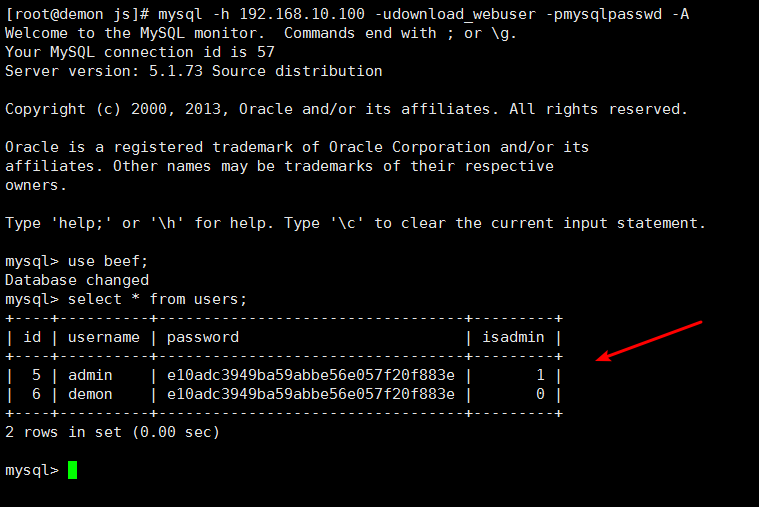
**http://192.168.10.100/beef/download.php?dir=config&filename=config.php**

****

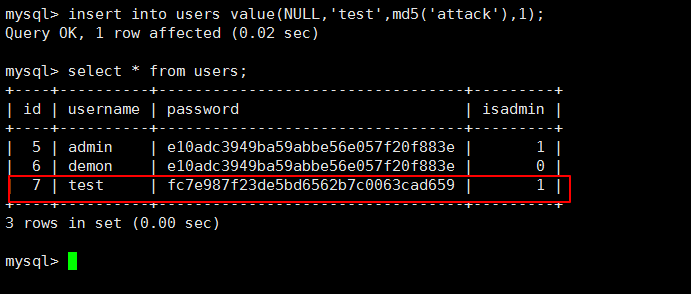
打开后可以发现里面有数据库连接的地址和账号密码

****

然后随便找个带mysql客户端的shell来连接一下这个数据库，拿数据



这里可以看到有个字段 isadmin 标记是否为管理员，因此可以留给后门管理员账号



创建好后，我们返回来登录留言系统，就可以享受管理员的删除留言操作了





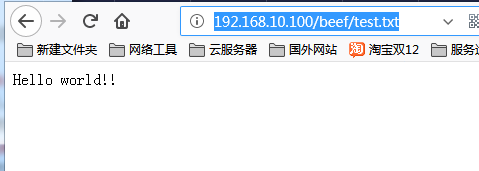
整个过程很简单，但这个漏洞难找，另外需要说明一下的是，下面这种形式的链接是没有下载漏洞的。

<a href="http://192.168.10.100/beef/message.apk">下载最新版APP</a>

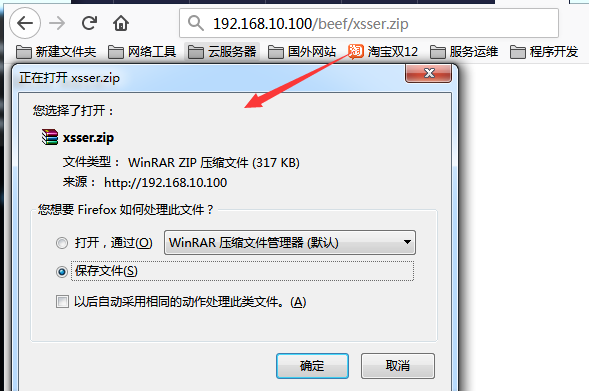
因为他没有传递参数，也就无法自己决定下载什么文件，也许你会想到可以直接修改URL来发送请求下载，比如假设web站点下有个文本文件test.txt，然后在浏览器上访问他

**http://192.168.10.100/beef/test.txt**

这样访问是不会弹出下载的，只会把它的内容解析出来



这是因为浏览器如果发现请求的文件是文本文件或者是图片等文件，就会以类似text/html去解析显示他，对于其他的格式如 .exe .zip 文件如果去访问他就可以下载



那么如果就是想下载文本文件或者图片，该怎么做呢？很简单服务器上需要修改HTTP返回报文头部的一个字段Content-Disposition: attachment; filename=<your filename> 让浏览器以文件流的形式访问和下载，关于本次测试页面的下载漏洞的下载代码如下：

