# 短文件名漏洞复现

Win2003上安装apache集成环境 wampserver，上传discuz论坛的upload目录改名成discuz浏览器访问安装discuz



检测环境，一般缺少那个就去php.ini开启相应的功能，或者权限给足即可



下面是具体安装步骤，比较简单不一一赘述了





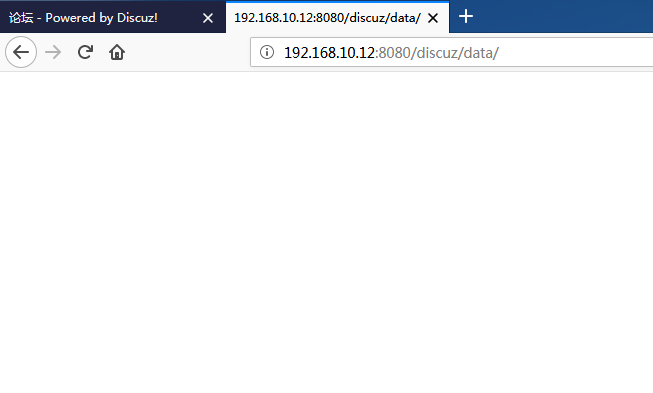




安装好后开始短文件名漏洞复现下载数据库拿管理员账号密码

Discuz为了数据安全，提供了数据备份接口，如果我们知道这个数据库备份文件的名字，那么我们直接访问这个文件，就可以拿到管理员和密码了

使用浏览器访问http://192.168.10.12:8080/discuz/data



此时页面为空，然后查看今天的日期为 2017-12-09 那么假如今天管理员对数据进行备份了，就会有命名如下的数据库文件

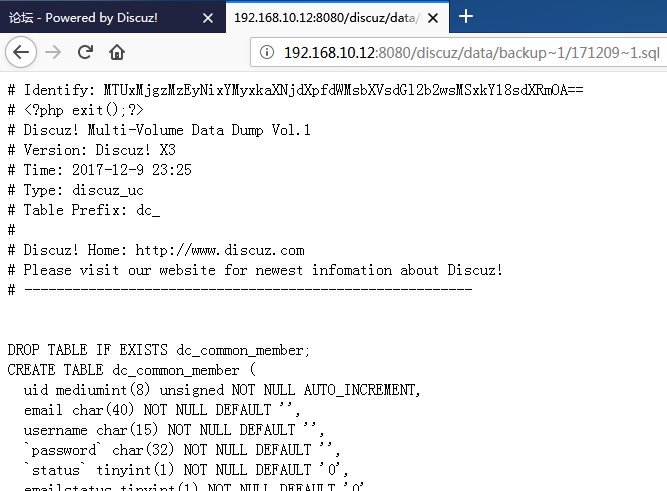
backup\_xxxxxx/171209\_xxxxxx-n.sql

绿色是固定名称不改变

蓝色是当前的时间简写

黄色是会随机产生防止被访问

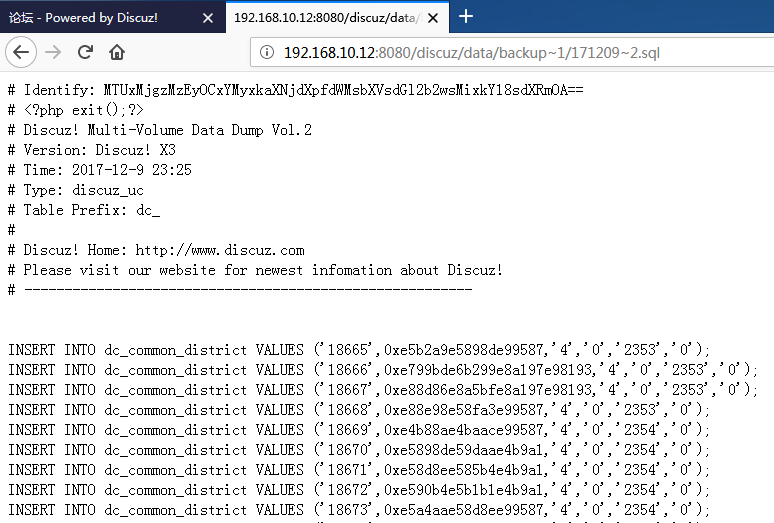
但是xxxxxx是随机改变的，我们并不知道，不过没关系，windows支持短文件名来表示一个长文件，也就是说只要前6位固定，其他用~n （n表示数字）代替就行，然后访问URL

**http://192.168.10.12:8080/discuz/data/backup~1/171209~1.sql**

然后可以看到第一个数据库文件被我们拿到了

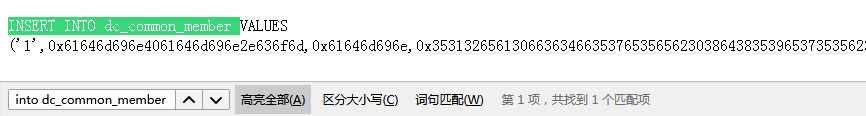
如果想下载第二个数据库文件，把1改成2即可，如下

**http://192.168.10.12:8080/discuz/data/backup~1/171209~2.sql**

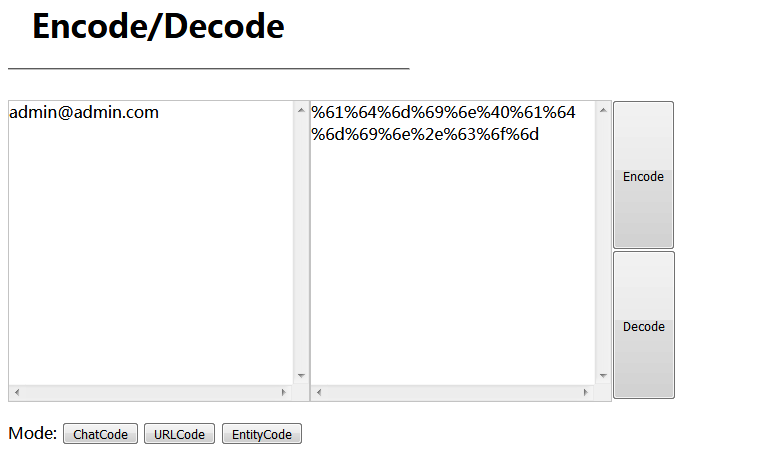
****

如果懒得导入查看数据库，可以直接搜数据库语句，用户存放的表为 dc\_common\_member

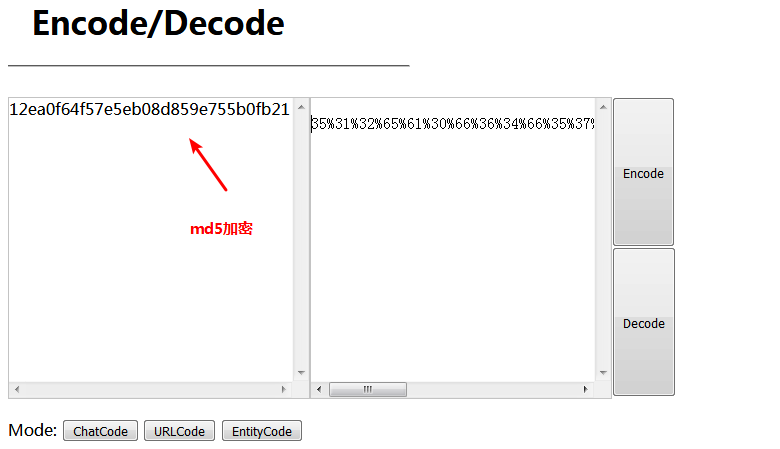
dc是表前缀，每个人可能不一样，搜insert操作，如下



可以得到一串16进制的数据，把它解开一下，密码还有一层特殊的md5加密，去http://www.chamd5.org/?mst解一下就可以拿到管理员的账号密码了，这里可以用我写的解密工具来解16进制ASCII码（小小装逼一下）







在线md5解密网站可能解密不出来，因为discuz对密码用了一些特殊的算法，所以这里就不继续研究如何解密了，有兴趣的朋友可以去查下discuz密码加密算法

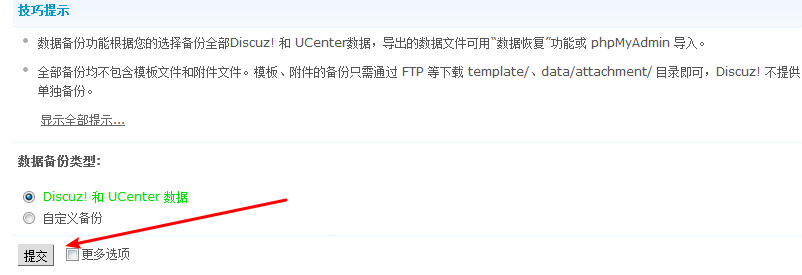
那么这个漏洞是怎么来的呢？

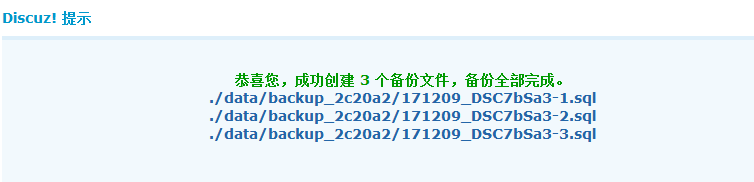
主要是跟discuz的数据库命名规则和windows短文件的特性有关，如下

登录后台管理界面









观察一下这三个数据库的命名规则

backup\_xxxxxx/171209\_xxxxxx-n.sql

绿色是固定名称不改变

蓝色是当前的时间简写

黄色是会随机产生防止被访问

windwos为了兼容以前的fat系统，继承了8dot3命名法，规则如下：

1.取完整文件名前6个字符加上 ~1 形成短文件名，再加上点和后缀

2.如果已经存在这个名字的文件~符号后面的数字会增加

3.任何包含小写字母名都被看做长文件名（不管长度多少），若有非法字符用下划线代替

4. 长文件名存储在属性标志为OFH的32字节目录登记项中（这是与短文件名目录项的区别）。用Unicode格式编码，每个字符（无论是英文或是汉字）均占2字节

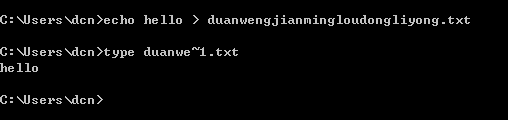
5每个目录登记项用26个字节存储13个字符（序号由第1字节指定）。位置多余时，先用00表示结束，再用FFH填充

6长文件名用若干个长名目录项保存，长文件名目录项倒序排在文件短目录项前面

看不懂没关系，举个例子

现在加入有个文件名为： duanwengjianmingloudongliyong.txt

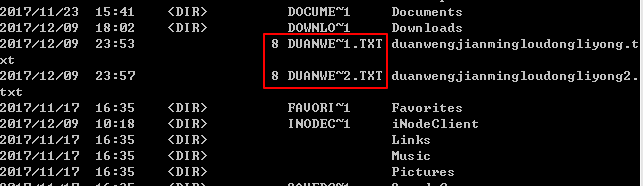
利用短文件名，我们可以直接访问： duanwe~1.txt



另外检测是否开启 8dot3兼容的命令 dir /x 如果有显示当前目录的子目录和文件



如果存在多个前6个字母相同则数字加一



规则就是这样，所以漏洞利用了短文件名去代表这些未知符号，防御方法也很简单，只要备份的数据库命名规则针对一下这个短文件名的规则去更改就行，比如前6个字母不一样，另外记得这个漏洞只在兼容8dot3的windows有效，其他系统则没有用。