周报五

sql注入：

sql报错注入：

分为两种：

1.extractvalue

and extractvalue(null,concat(0x7e,(sql_inject),0x7e))

可以理解为，让后台xml故意爆错

2.updatexml

and 1=(updatexml(1,concat(0x7e,(sql_inject)),1))

group_concat函数：

这个函数是拼接的，用法如下

```
CREATE TABLE `zhanghao`.`qq` (
  `username` INT NOT NULL,
  `password` VARCHAR(45) NOT NULL);
insert into zhanghao.qq
values ('1001','zheng')
select *
from zhanghao.qq
insert into zhanghao.qq
values ('1001','cheng')
select username ,group_concat(password)
from zhanghao.qq
group by username
SELECT group_concat(table_name)
FROM information_schema.tables
WHERE table_schema = database();
```

Result Grid | Filter Rows: | Export: | Wrap Cell Content:

username	group_concat(password)
1001	zheng,cheng
1002	li

可以将这个表的两项内容拼接到一块。

假设当前使用的数据库是 `test_db`，并且该数据库中有三张表，分别为 `users`、`orders` 和 `products`，那么执行这个查询语句：

```sql
SELECT group_concat(table_name)
FROM information_schema.tables
WHERE table_schema = database();
```

返回的结果会是：

```plaintext
users,orders,products
```

当然如上图所示，我们可以看到使用group_concat函数还可以用来报数据库的表名。

group_concat(column_name))from(information_schema.columns)where(table_schema)like(database()))

那么这一段就是来用来查表中的属性

TCP/IP协议：

它是传输控制协议/网际协议的简称

是一种允许不同网络之间进行的信息传输控制的协议集合

核心协议：

IP协议（网际互连协议）网络层：将不同类型的物理网络互联在一块

将不同格式的数据帧转换为IP数据包

将不同格式数据包的物理层地址转化为统一的IP地址

TCP协议（传输控制协议）传输层，是面向连接的协议

域名DNS：

一个Ip可以对应一个或者多个域名，用域名接卸Ip，可以使用ping或者直接网上在线域名解析

.uk .fr .jp .co .com .edu .gov .mil .net

分别对应美国，法国，日本，中国，企业，教育机构，政府，军事部门，以及互联网络及信息中心

动态页面与静态页面的主要区别

1.后缀不同

动态页面以asp aspx jsp php perl .cg 结尾

并且在动态页面网址中有个？号