关于铜仁学院网络安全

事件（漏洞）通报

根据教育行业漏洞通报平台安全通报，发现你单位信息系统（网站）存在sql注入漏洞（事件），漏洞详情见（附件）。请你单位尽快对发现在的安全隐患进行核实与整改，于12月7日前将核实、修复情况以书面形式报至我中心。

开展安全监测是及时发现安全隐患的有效手段，可有效降低因安全隐患演化成为安全事件的机率。今后，请你单位高度重视信息技术安全工作，切实保障教育行业网络安全，满足《网络安全法》要求。

联系人：杨燕

联系电话：0851-85283616 邮箱：gzjyglxxzx@sina.com

附件：1. 贵州省教育行业网络安全事件（漏洞）通知单

2. 贵州省教育行业网络安全事件（漏洞）整改反

馈单

贵州省教育管理信息中心

2024年12月5日

附件1

贵州省教育行业网络安全事件（漏洞）通知单

|  |  |  |  |
| --- | --- | --- | --- |
| **预警单位** | 铜仁学院 | | |
| **事件状态** | 已通报 | **通报单位人员** | 铜仁学院网络中心安全人员 |
| **通知人员** | 信息中心 | **通知时间** | 2024年12月5日 |
| **网站标题** | 铜仁学院智慧机房动力环境监测系统 | | |
| **网站漏洞URl** | http://pop.gztrc.edu.cn:9091/login/login/index/ | | |
| **事件类型** | sql注入 | **安全等级** | 中 |
| **整改期限** | 2024年12月7日 | | |
| **事件描述** | 1.弱口令admin1/admin1登录网站。2.抓包测试，发现存在sql注入 | | |
| **处理方案** | **限制一小时内关闭外网访问** | | |
| **整改建议** | 对进入数据库的特殊字符（’”<>&\*;等）进行转义处理，或编码转换。数据长度应该严格规定，能在一定程度上防止比较长的SQL注入语句无法正确执行。过滤危险字符。‌ | | |
| **事件取证** | null | | |

资产所在网段：互联网

漏洞验证所需账号：admin1

漏洞验证所需密码：admin1

漏洞URL：

http://pop.gztrc.edu.cn:9091/login/login/index/

1. 弱口令登录网站

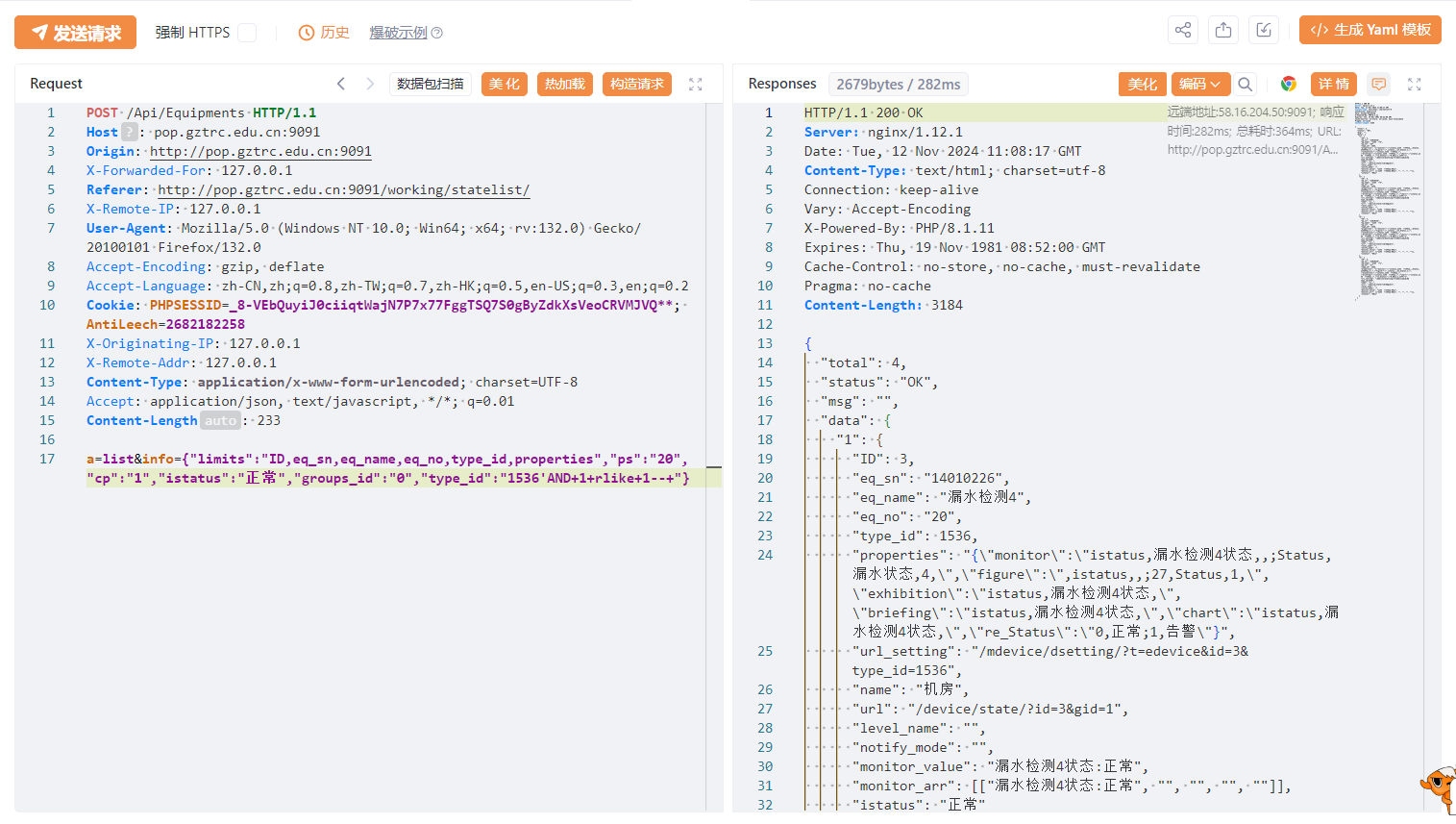


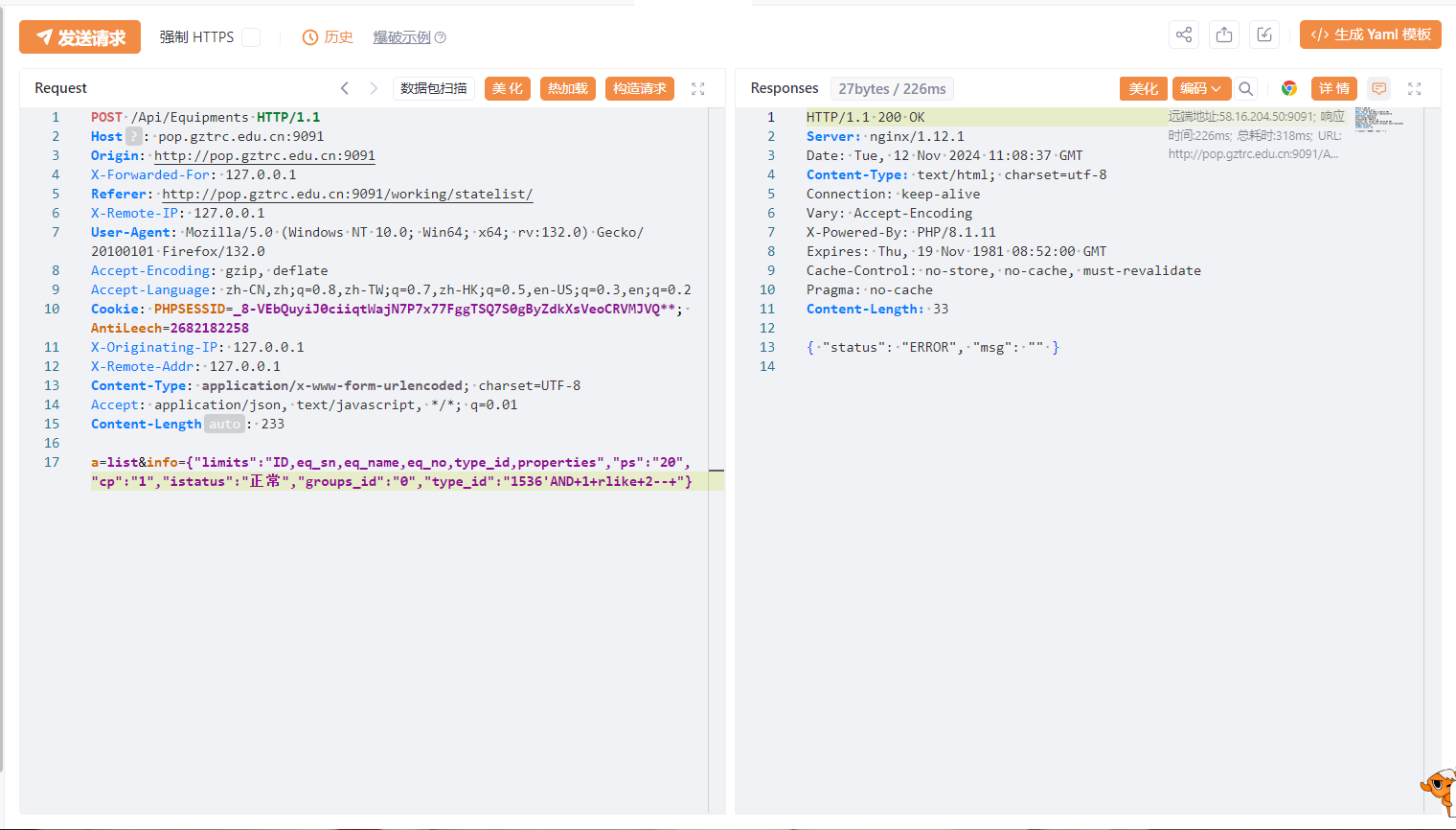
提示没有权限登录，把路径/login/login/index/删除后发现登录成功



2.抓包测试，发现存在sql注入

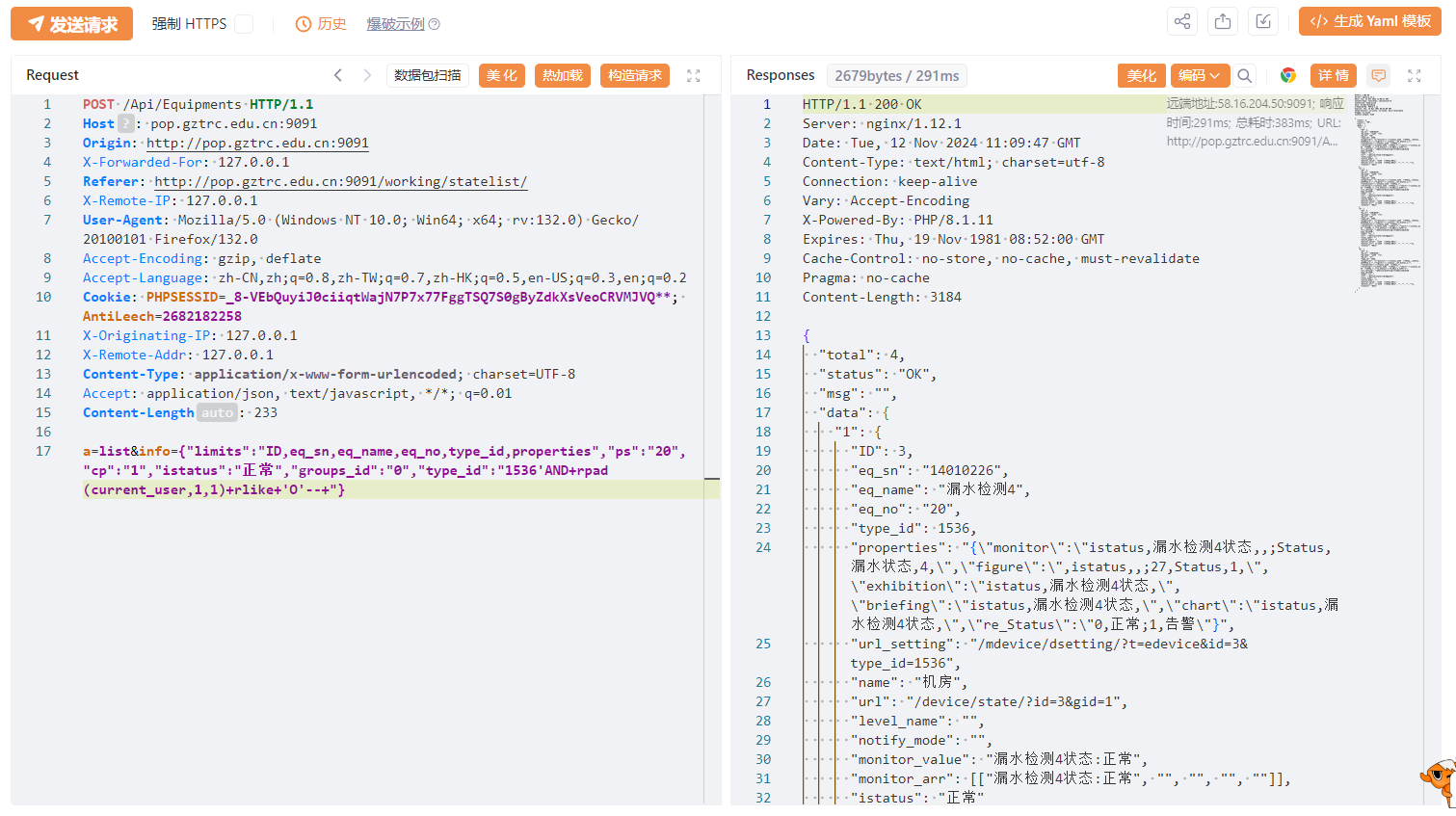
接口：/Api/EquipmentsType



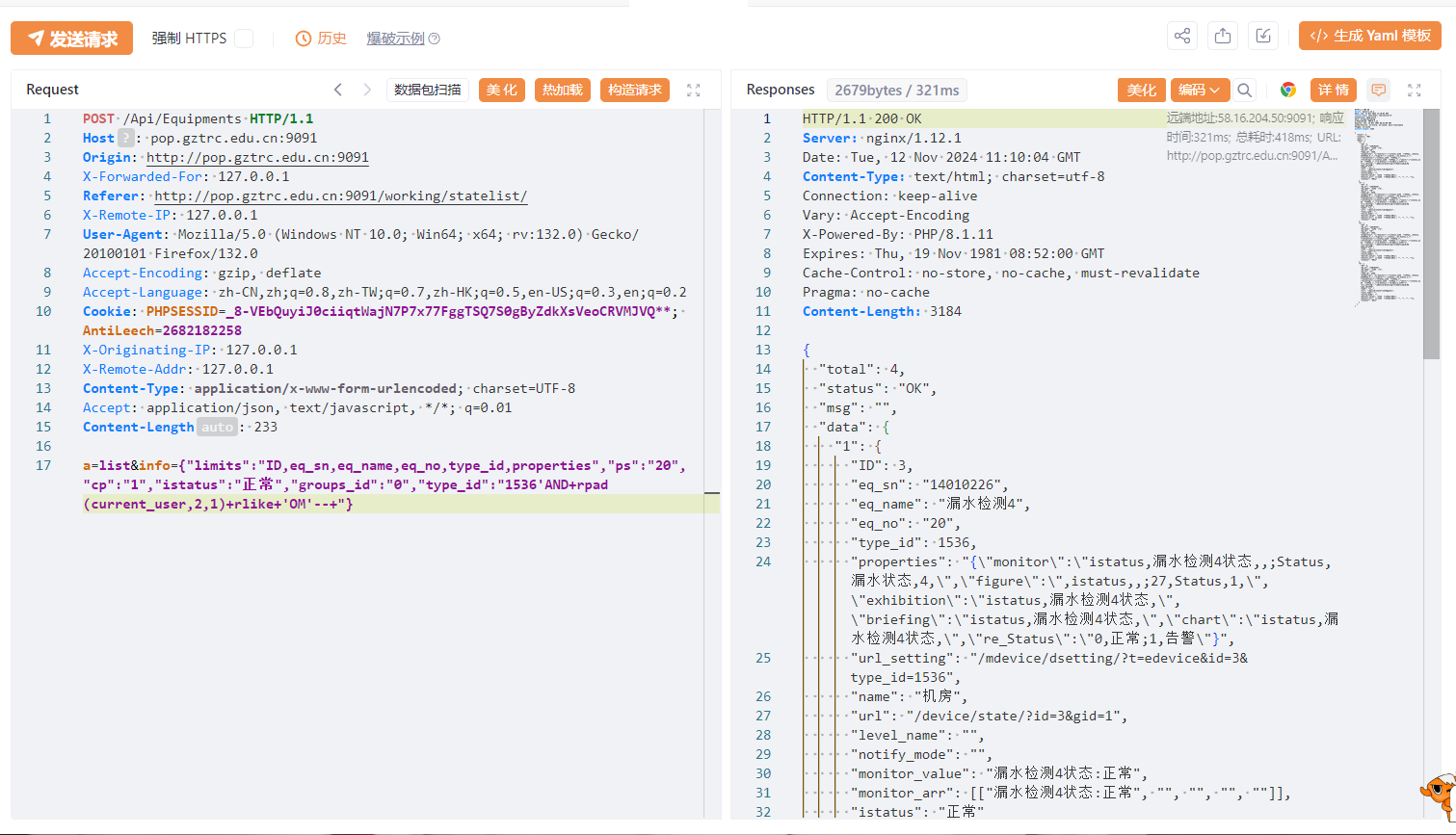


布尔盲注

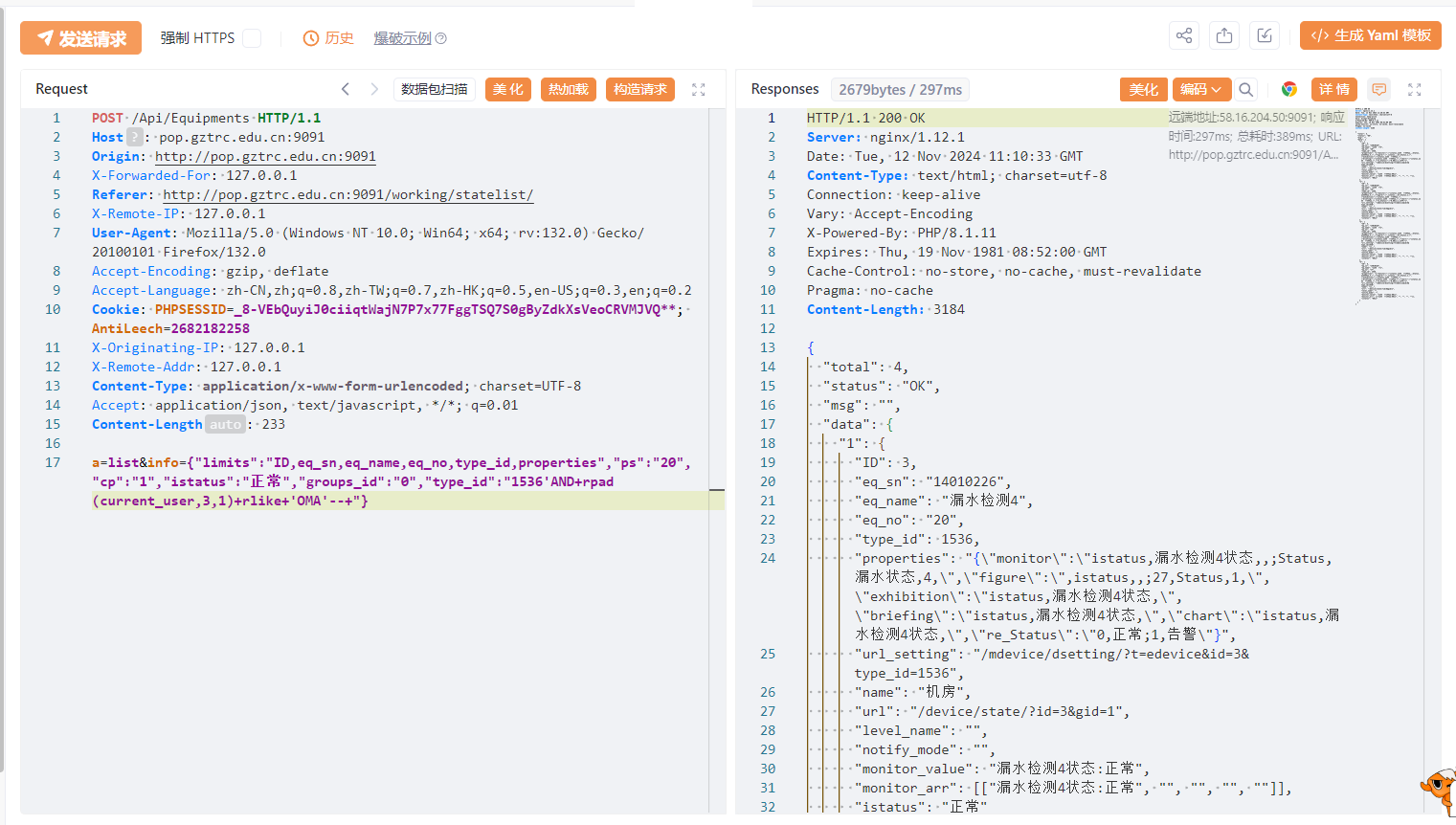
第一位为O



第二位为M



第三位为A



当前用户名为：OMARA\_CM@LOCALHOST

payload:

a=list&info={"limits":"ID,eq\_sn,eq\_name,eq\_no,type\_id,properties","ps":"20","cp":"1","istatus":"正常","groups\_id":"0","type\_id":"1536'AND+rpad(current\_user,1,1)+rlike+'O'--+"}

附件2

贵州省教育行业网络安全事件（漏洞）整改反馈单

|  |  |  |  |
| --- | --- | --- | --- |
| 漏洞通知单位 | 贵州省教育管理信息中心 | | |
| 漏洞通报单位 |  | | |
| 信息系统名称 |  | | |
| 网站URL |  | | |
| IP地址 |  | | |
| 整改情况 | （反馈内容应包括事件原因、影响范围、处置过程、处置结果及下一步工作计划等，应国家保密办要求，注明涉事服务器是否涉及处理国家秘密和工作秘密。） | | |
| 其他问题 |  | | |
| 单位联系人 |  | 联系电话（手机） |  |
| 单位或部门印章  年 月 日 | | | |