【XCTF高手进阶区】web6_ics-06 writeup

原创

Mitch311 于 2021-02-13 20:51:21 发布 92 收藏 1
分类专栏： CTF

web6_ics-06

原题链接

key:burpsuite爆破id

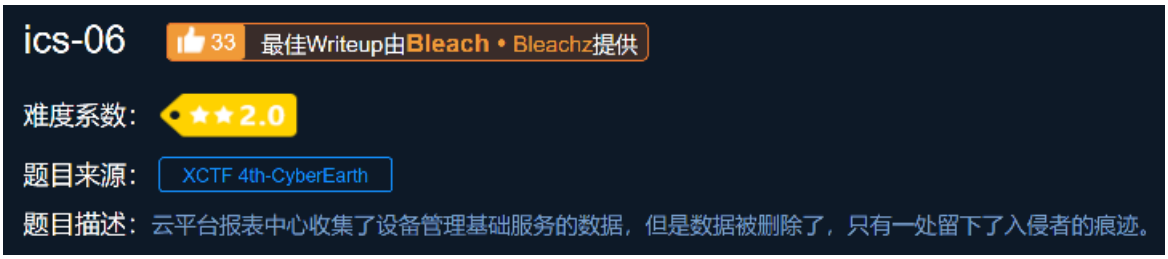
①环境打开后是这样的

我把左侧导航栏里的链接试了个遍，只有“报表中心”可以进入

②这时发现地址栏多出了id=1

我把id=1换成了id=2,3,4,5,6,7,8,9后，页面没有变化

再结合题干信息

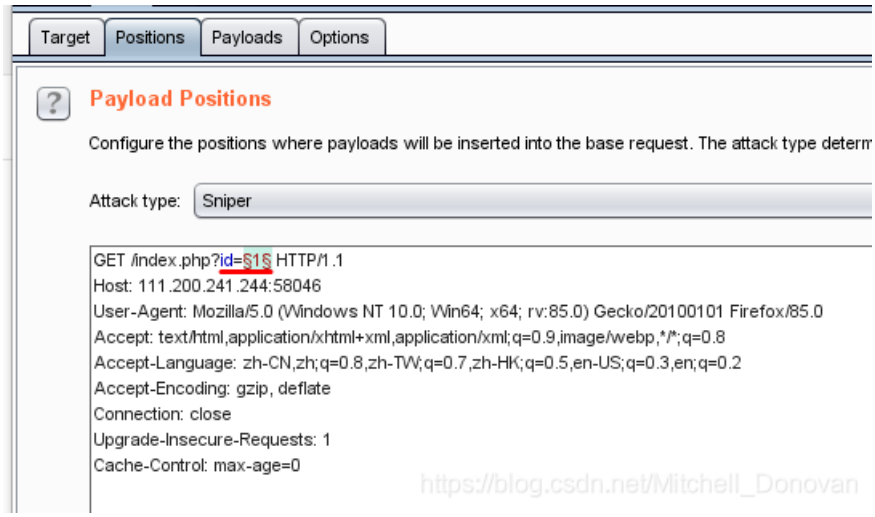


猜测入侵者可能是想通过id来给自己创造一个后门，类似于一种密钥吧

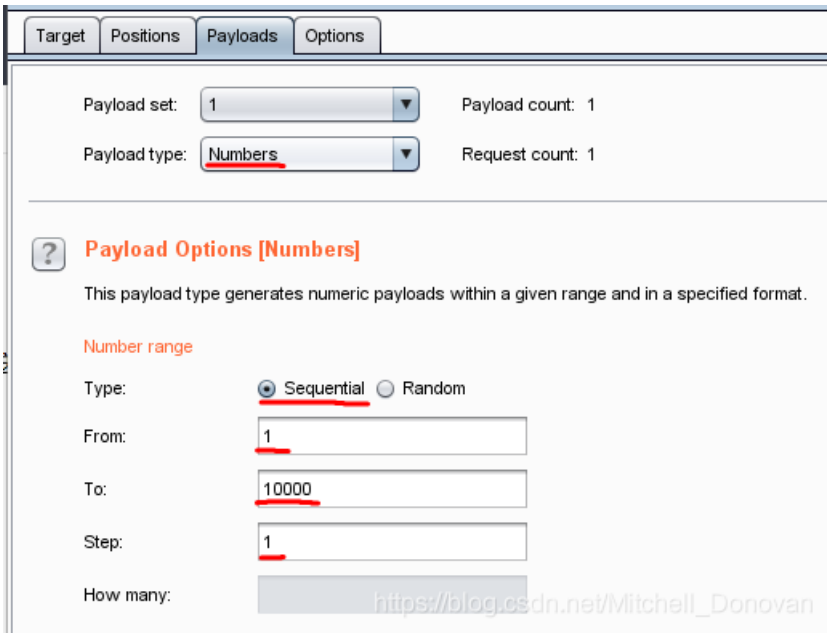
我们的任务就是爆破出id

③burpsuite抓包，右键发送到Intruder爆破

首先确定爆破位置



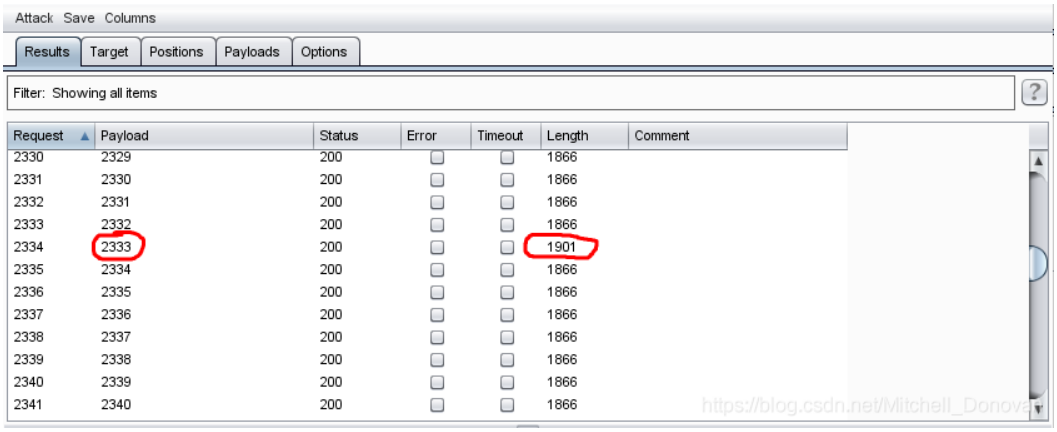
随后进行payload设置



payload类型设置为数字类型，数字类型设置为具体，范围设置为1到10000，步长设置为1

点击开始爆破□

④爆破结果□



返回报文长度不同的id是id=2333

直接去浏览器访问id=2333，得到flag□

cyberpeace{0e6aab5da4c9ecfb8d5589e041a18238}