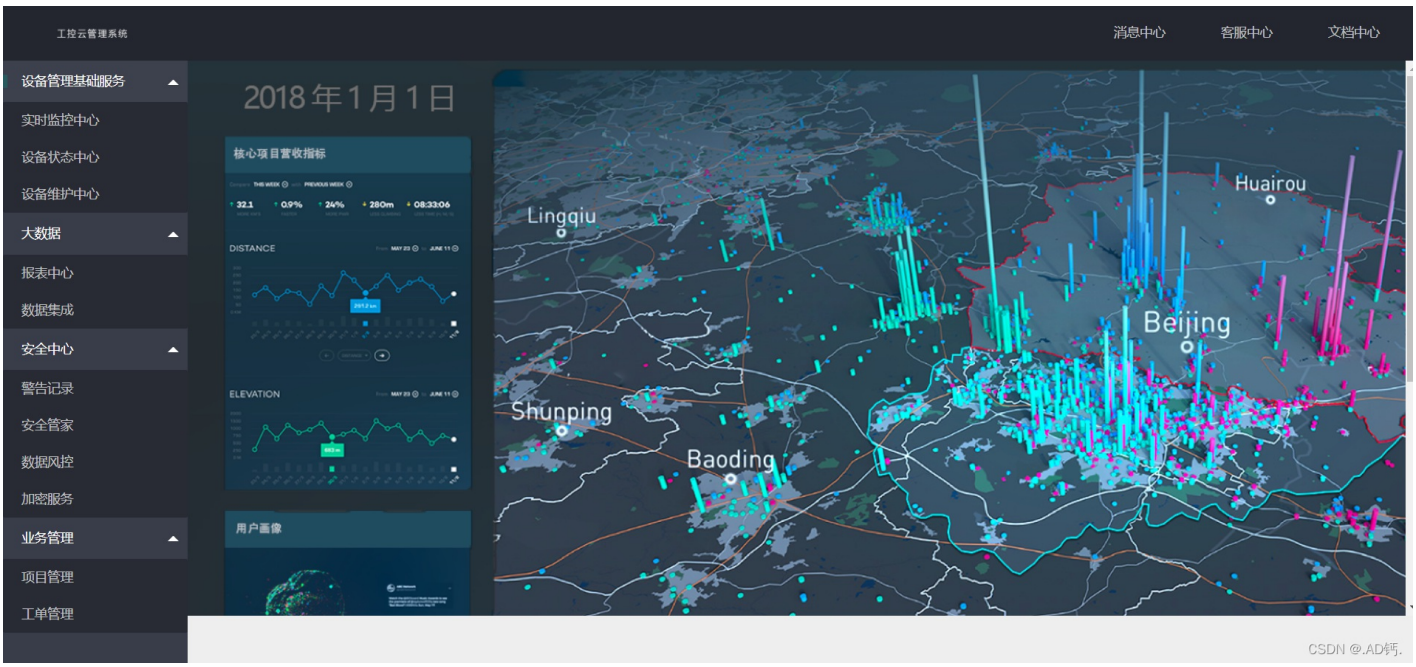
XCTF-WEB-ics-06

原创

.AD钙. 于 2022-03-10 16:06:44 发布 5317 收藏
分类专栏： WP 文章标签： web安全 安全

这道题有那么一丢丢实战的意思了，至少它是个正常的网页页面了。



能点的地方都点一点，发现报表中心能进去。

列表

日期范围 -

确认

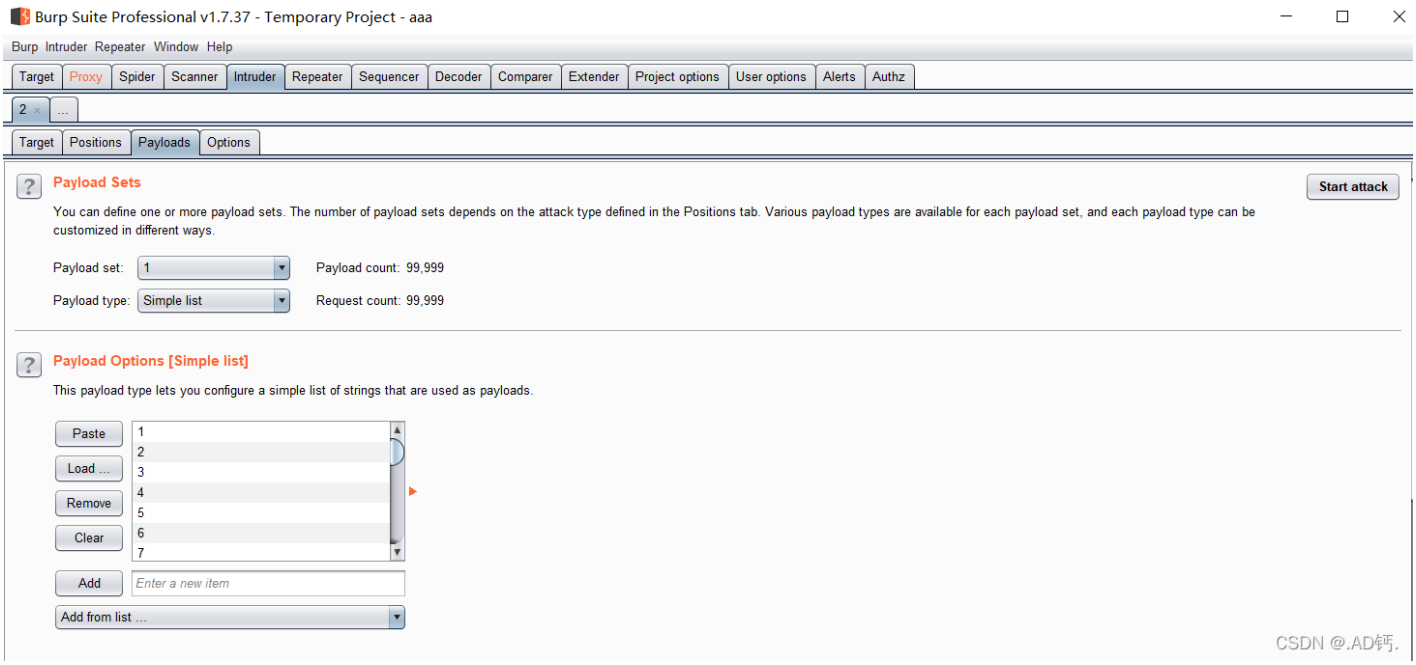
送分题

进来之后看到一个“送分题”。

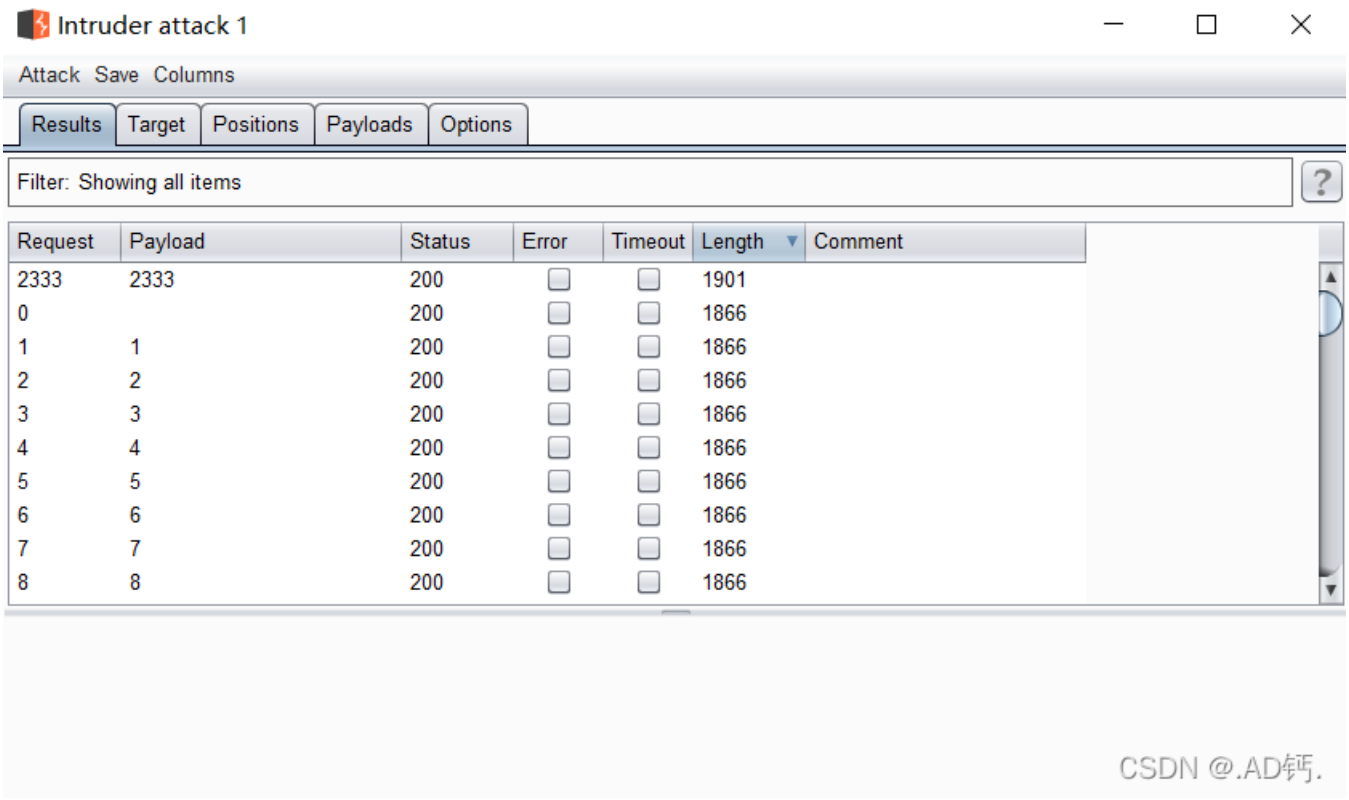
日期范围随便点一点也没发现啥，f12也啥都没有。

这个时候注意到url有一个?id=1，但是双引号啊单引号啥的发现没啥用，不是sql注入。

看题目描述说有一页留下了痕迹，这个id=1应该是页数的意思，所以我们打开burpsuite爆破。



自己用python生成一个1到很大的数的字典，然后load到burp的字典里，点右上角start attack



点一个下Length这个按钮，让它按返回字节长度的倒序显示，发现2333返回了1901的长度，跟其他的都不一样，所以说明2333这个页面有别的东西。

得到flag。