Lab Pentest Report

Performed By
Priyanshu Patel

Start Date: 5 Sep 2023
End Date: 5 Sep 2023

Contact:
priyanshupatel2301@gmail.com

Scope:
url: https://portswigger.net/web-security/sql-injection/blind/lab-time-delays
this lab is our scope it's a simple task of forcing a delayed response

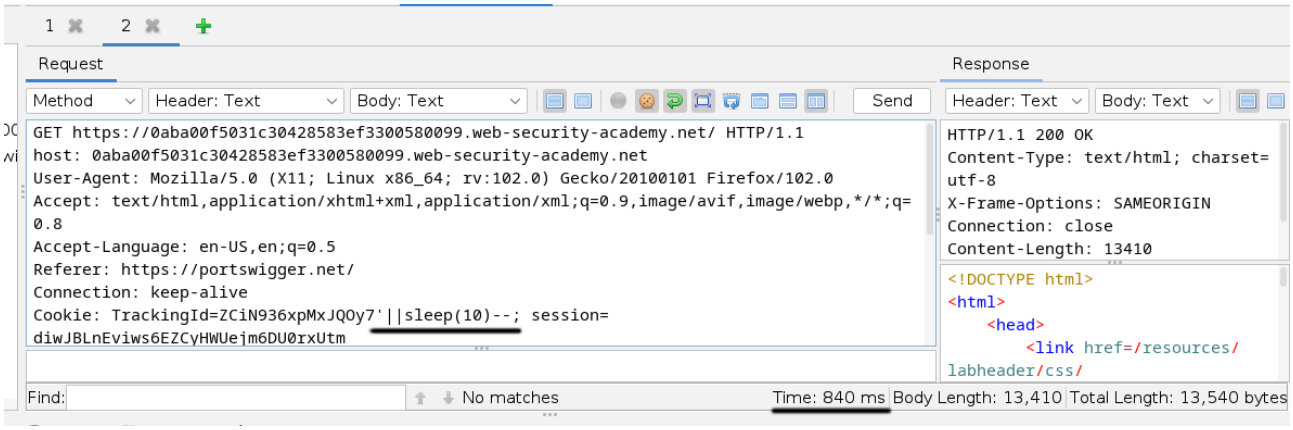
Goal Assesment:
we know that vulnerable parameter is tracking cookie.
Results of the sql query is not showed in site.
Site has the same response if the query generate error or if it doesn't.
Goal: we have to force the time delay of 10 seconds

Attack Perspective:
a side from the lab information it's black box

Attacking The Lab Environment (Attack Steps):

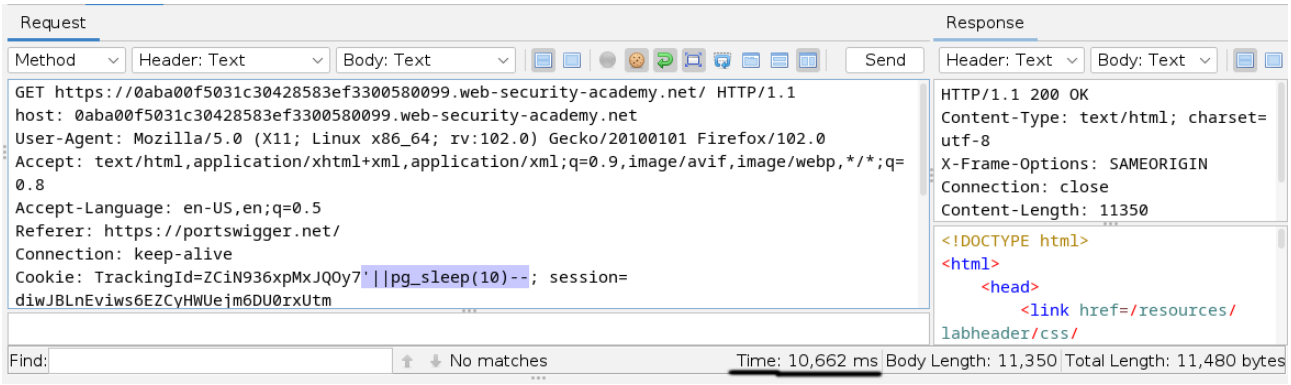
there's only 1 step here
we know what's vulnerable so
out of the 4 db platforms(mysql, postgre, oracle, microsoft)
one of them would force the time delay
so fuzz all 4 in the parameter and see which one works

1. mysql
payload: '||sleep(10)--

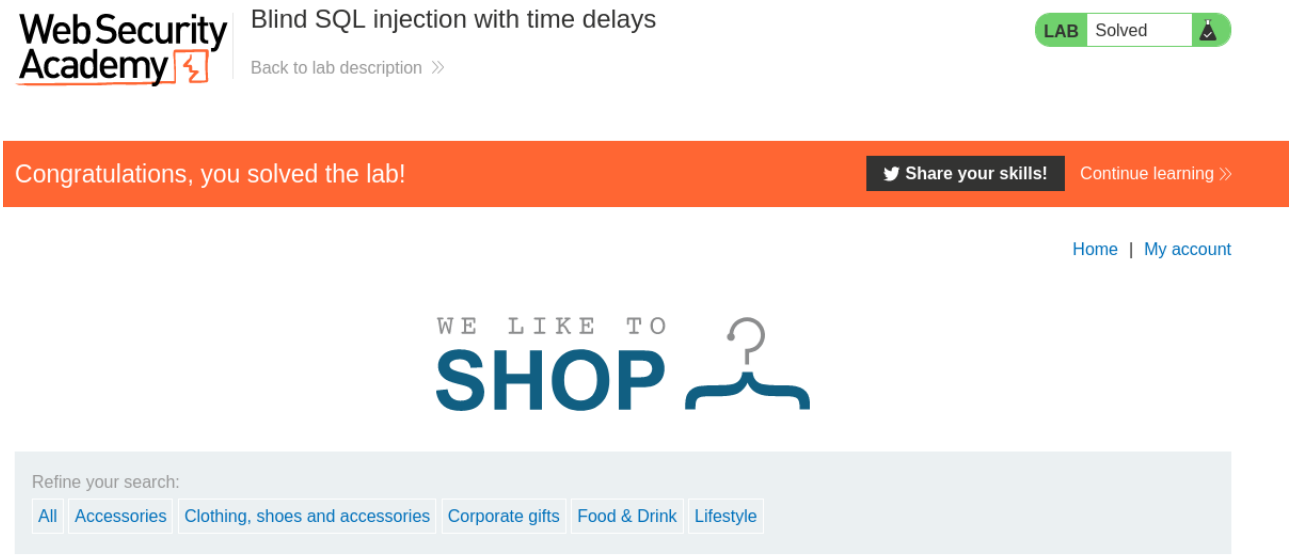


so as you can see we got the response in 840ms so this is not it.

2. postgresql
payload: '||pg_sleep(10)--



okay now we used postgre payload and you can see we get the response in 10,662ms time and we get the 10 second delay we want. Means site uses postgrey db in the backend



and we have successfully solved the lab...

--END--