SSRF

Tuesday, February 4, 2020 11:44 PM

1.TRY TO GET THE PARAMETER WHERE IT IT REQUESTING SOME URL.
2.TRY TO CHECK THE LOCAL ADDRESS OR YOUR CONTROLLABLE ADDRESS.

EXPLOITATION

1.Give local address and check the output.
2.check for access control. Ex=> localhost/admin
3.Try to enumerate ports and services.

ITS NOT MANDETORY THAT THE ADDRESS WILL BE LOCAL HOST SO OR URL IT MAY BE ANY OTHER IT ALSO SO FIRST LOOK CAREFULLY AT URL THEN PROCEED.

4.Many times developer applied blacklisting like you can not use local host or admin path.
a)to broke or bypass this use 127.1 for localhost and url double encoding for admin.

BLIND

1.TO CHECK BLIND BASED TRY TO USE OUT OF BAND TECHNIQUES.IF NOTHING FOUND TRY ON REFERER HEADER

2.