VAPT ATTACKS

1.SSL Certificate – Low Level In Software And Data Integrity Failure also in (system misconfiguration)

2.Broken Access Control–
IDOR–Insecure Direct Object Reference
In broken access control we have to sign up
IDOR MEANS CHANGING FROM 1 TO 3
EXAMPLE:
ACCOUNT ID 1 TO ACCOUNT ID 3 IN REPEATER and vuln level crit/high

IDOR Must probably used in banking account site

3. DIRECTORY ATTACK (RANDOM MANUAL SEARCH)
RESOURCES,PLACEHOLDERS,BOOTSTRAP,

ETC CHECK ALL THE HTTP TRAFFIC AND EXPLORE(Insecure Design)(BROKEN ACCESS CONTROL)

4.system misconfiguration
Ssl certificate http is vuln and https is not vuln.
We can also see info about login it self on the page

5.(System misconfiguration) is also when we see server name information on http page in burp level hig/crit and also in (software and data integrity failure)

We have to check that server name etc if it is outdated it is considered as high level in outdated component

User token/cookies come in cryptographic failures and also in data integrity failure (critical)whenever we see an cookie it is an medium level vuln jsessionid (Cookie information leaking)

User token (last line) is also a cryptographic failure

Also username and password if not encypted are also a vuln

6.SSRF(SERVER SIDE REQUEST FORGERY)THR MOST CRITICAL ATTACK WHERE WE USE INTERCEPTING

Ssrf is when we send the user from a to c instead of a to B

Cross site scripting xss scripts = linkedin readymade script

Secure connection failed tls protocol

outdated is also a vuln

8.security monitoring and logging is when we put incorrect passwords multiple time and it still does not block us is a vulnerable

Cryptographic failure: Cookies, username, password are not encrypted and can be seen