**DAY 31**

**PART 1**

1. Web application vulnerability assessment and penetration testing.

2. Bug hunting

Vulnerability assessment:

🡪The authorised process of identifying the weaknesses inside a software or hardware is called vulnerability assessment.

Penetration testing:

🡪The authorised process of exploitation of vulnerabilities is called penetration testing.

🡪Pentesting is performed by pentesters/ethical hackers.

🡪Pentesting is performed to analyse the risk factor/impact of the vulnerability against data.

Haveibeenzucked.com => 2019 facebook data breach checking

Bounty:

1. Money

2. Swag (coupons, T-shirts, Mugs etc.)

3. Hall of Fame

Bug bounty platforms:

1. hackerone

2. bugcrowd

3. internetbugbounty

4. synack

Intigriti.com

Yeswehack.com

Nciipc.gov.in

Burpsuite:

Burpsuite is an vulnerability assessment tool with burp proxy.

“Open in browser” option is available in burpsuite

**Part 2**

Burpsuite:

Proxy🡪options

127.0.0.1:8080

Configure in browser

Settings🡪proxy

Manual proxy

HTTP proxy: 127.0.0.1 port:8080 and check also use this proxy for FTP

New tab:

<http://burp/>

click CA certificate🡪save

Browser setting🡪certificates

View certificates

Import

Choose cacert file

Enable 2 check boxes

SQL scope (SQL injection vulnerability)

1. Bypassing authentication

2. Exposing sensitive data

3. We can compromise the data integrity

4. Erasing the database

5. Remote code execution

Client server architecture: