Honours - Cybersecurity

Module - 2

Q.1 Write a detail about OWASP TOP 10 vulnerabilities along with its mitigation?

→ • OWASP stands for Open Web Application Security project.
• OWASP Top 10 is regularly updated list of the most critical web application security vulnerabilities.
• OWASP TOP 10 serves as a valuable resource for developer, security professional & organi-zation to priotize their effort in securing web application.
• OWASP TOP 10
1) Injection
2) Broken Authenticat^n
3) Sensitive Data Exposure
4) XML External Entities (XEE)
5) Broken Access Control
6) Security Misconfigurat^n
7) Cross-site scripting (XSS)
8) Insecure Deserializat^n
9) Using Components with Known Vulnerabiliti
10) Insufficient logging & Monitoring.

① Injection:-
This attack happens when untrusted data is sent to code, interpreter thru a form input / some other data submission to a web applicat^n.

Migitat^{n}: This type of attack can be prevented by validating and sanitizing user-submitted data. Also, avoid dynamic Query & inputs directly from user.

(2) Broken Authenticat^{n}:-
Vulnerabilities in authencat^{n} (login) sys can give attacker access to user accnt and even the ability to compromise an entire system using an admin accnt.

Mitigat^{n}: Implement strong password policy, enable E2FA and MFA, limit login attempt using rate limiting, etc.

(3) Sensitive Data Exposure:-
- When sensitive data is not properly protected it can be exposed to unauthorised parties & they can sell or utilize that data for nefarious purpose.

Mitigat^{n}: Can be minimized by encrypting all sensitive data as well as disabling the caching of any sensitive information. Also Regularly review & audit data access.

(4) XML External Entities (XEE):
- This is an attack against web app that parses XML input. This input can reference an external entity, attempting to exploit vulnerability in parser. An 'external entity' in this context refer to as storage unit such as Hard Drive.

Mitigat^{n}: Disable XML external entity processing, use whitelist to validate XML inputs & update parser to the latest version that have protect^{n} against XEE attack.

5) Broken Access Control :-
- This vulnerability allows unauthorised user to bypass & perform task as though they were priveleged user such as admin.

Mitigat^{n} :-
Implement proper access control, ensure that user can only access data & functionality that are authorised for, regularly test for access control issue, use authorisat^{n} tokens.

6) Security Misconfig :-
- This occurs when security setting are not correctly configured, leaving vulnerab-ilities open to exploit.
- Mitigat^{n} :-
Continuously monitor & audit ur app's security setting and regularly update & patch software components.

7) Cross-Site Scripting (XSS) :-
- This vulnerability occurs when web app allow user to add custom code into a URL path / onto a website that will be seen by other users. Often leading to theft of session cookies & other sensi information.

- Mitigatⁿ:
  Sanitize & validate user-submitted data (I/p). & educate developers about XSS preventⁿ.

8) Insecure Deserializatⁿ:-

Threat target

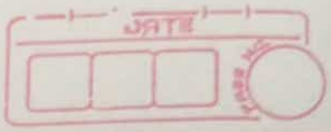
- Many web app frequently seralize & desereralize data
- Serializatⁿ → taking obj from app code & converting them into format that can be used for another propose. Deserializatⁿ → opposite.
- Vulnerability arises when an app deserialise untrusted data, allowing attacker to execute malicious code.

Mitigatⁿ:-
Avoid deserialisatⁿ of untrusted data, implement propey serializatⁿ & deserializatⁿ control.

9) Using Compo with Known Vulnerabilities:-

- Many web applicatⁿ uses 3rd party libraries & components.
- These compo are peiece of s|w that helps developer avoid redundant work & provide needed functionality. - If they have known vul → att can exploit them.

Mitigatⁿ:-
Have process in place that Quickly address known vulnerabilities, Regularly update & patch s|w compo.



10) Insufficient logging & monitoring :-

- Inadequate logging & monitoring make it diff to detect & respond to security incidents promtly.
- Mitigat^{n} :-
  Ensure logs are reviewed regularly, Set up automated alert for suspicious activity & have IR plan in place.