AI For Web Security

Name: Nikhil Sri Harsha

Reg.No: 21BCE8711

Date:22/08/23

Task-3:

Date:25/08/2023

Top 10 OWASP VUNERABILITIES:

1. **Injection**
   CWE : CWE-20, Improper Input Validation
   Description : The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.
2. **Broken Authentication**
   CWE : CWE-287, Improper Authentication
   Description : When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.
3. **Sensitive Data Exposure**
   CWE : CWE-200, Exposure of Sensitive Information to an Unauthorized Actor
   Description : The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.
4. **XML External Entities (XXE)**
   CWE : CWE-611, Improper Restriction of XML External Entity Reference
   Description : The product processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.
5. **Broken Access control**
   CWE : CWE-284, Improper Access Control
   Description : The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.
6. **Security misconfigurations**
   CWE : CWE-264, Improper Restriction of Functionality
   Description : The product does not properly restrict the functionality that is available to users.

7. **Cross-Site Scripting (XSS)**
   CWE : CWE-79, Improper Neutralization of Input During Web Page Generation
   Description : The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.
8. **Insecure Deserialization**
   CWE : CWE-502, Deserialization of Untrusted Data
   Description : The product deserializes untrusted data without sufficiently verifying that the resulting data will be valid.
9. **Using Components with known vulnerabilities**
   CWE : CWE-937, Using Components with Known Vulnerabilities
   Description : The product is developed using an outdated version of the component, or when the component is not properly patched.
10. **Insufficient logging and monitoring.**
    CWE : CWE-778, Insufficient Logging and Monitoring
    Description : When a security-critical event occurs, the product either does not record the event or omits important details about the event when logging it.

p