|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Yes** | **No** | **N/A** | **Comments/Evidence/Rationale** |
| **Authentication** | | | | |
| 1. Does each Web request validate authentication? |  |  | x | There is no authentication mechanism. |
| 2. Are credentials presented securely (i.e., using SSL, not the GET method?) |  |  | x | Please see response for question 1. |
| 3. Are passwords stored in an encrypted or hashed format? |  |  | x | Please see response for question 1. |
| 4. Is password complexity enforced, including minimum length, nonguessable words, special characters, and numbers? |  |  | x | Please see response for question 1. |
| 5. Do user credentials expire after a period of time? |  |  | x | Please see response for question 1. |
|  | **Yes** | **No** | **N/A** | **Comments/Evidence/Rationale** |
| 6. Are standards used for authentication and identity management (i.e., SAML, WS-Security, LDAP, NTLM, Kerberos)? |  |  | x | Please see response for question 1. |
| 7. Are user accounts locked after a certain number of failed authentication attempts? |  |  | x | Please see response for question 1. |
| **Authorization** | | | | |
| 8. Are permissions defined to create fine-grained administrator access? |  |  | x | There are no authorization mechanisms in place. |
| 9. Are permissions defined for fine-grained, administrator access. |  |  | x | Please see response for question 8. |
| 10. Are permissions enforced consistently in the application? |  |  | x | Please see response for question 8. |
| 11. Can permissions be grouped or organized to user roles for simplified access management? |  |  | x | Please see response for question 8. |
| 12. Are roles and permissions consistent with the standards or other applications in the enterprise? |  |  | x | Please see response for question 8. |
| **Data Validation** | | | | |
| 13. Are all user inputs validated? | x |  |  |  |
| 14. Does validation check data length? | x |  |  |  |
| 15. Does validation filter or escape special characters? | x |  |  |  |
|  | **Yes** | **No** | **N/A** | **Comments/Evidence/Rationale** |
| 16. Does validation of Web input remove tags before displaying it back to the user? |  |  | x |  |
| 17. Does the application validate the data type of user input before operating on it? |  | x |  |  |
| 18. Is XML received from outside of the application validated? |  |  | x |  |
| 19. Is the integrity of the files sent and received by the application validated? | x |  |  |  |
| **Session Management** | | | | |
| 20. Is session data excluded from the URL using the GET method? |  |  | x | No web requests are integrated. |
| 21. Does data in the browser cookie contain only the session ID and exclude other session information? |  |  | x | Please see question 20. |
| 22. Are session IDs hashed to prevent attackers from guessing valid sessions IDs? |  |  | x | Please see question 20. |
| 23. Are session IDs guaranteed to be unique? |  |  | x | Please see question 20. |
| 24. Are sessions validate on each page request? |  |  | x | Please see question 20. |
| 25. Do sessions expire after a period of inactivity? |  |  | x | Please see question 20. |
| 26. Are expired sessions deleted on the server? |  |  | x | Please see question 20. |
|  | **Yes** | **No** | **N/A** | **Comments/Evidence/Rationale** |
| **Logging** | | | | |
| 27. Are security-related events logged consistently? |  | x |  | There is no logging repository. |
| 28. Is sensitive information, such as passwords, kept from logs? |  | x |  | Please see question 27. |
| 29. Are security events stored in a secure location and not mixed with common application logging? |  | x |  | Please see question 27. |
| 30. Are events logged in a format and location that is compatible with security monitoring./event correlation software? |  | x |  | Please see question 27. |
| **Error Handling** | | | | |
| 31. Are exception handling mechanisms used consistently? | x |  |  |  |
| 32. Does the application fail securely? If so, how? | x |  |  | There is an error handling function integrated. |
| 33. Are open transactions processed appropriately if an error is encountered during processing? |  | x |  |  |
| 34. Are error messages displayed to the users informative without revealing information about system internals or other sensitive data? | x |  |  |  |
| 35. For function-based error, are return values of functions tested? |  | x |  |  |
|  | **Yes** | **No** | **N/A** | **Comments/Evidence/Rationale** |
| 36. For exception-based error handling, are specific exceptions caught rather than broad exception handlers (i.e., throwable in Java)? | x |  |  |  |
| 37. Are exceptions that are caught managed and logged (i.e., no empty catch() blocks?) |  | x |  | There is no logging repository. |
| **Cryptography** | | | | |
| 38. What is the sensitivity of the data being processed by the application? |  |  | x | Public. License.txt is hardcoded into the server application and this is public information. |
| 39. Is encryption required for the data? If so, in transit, at rest, or both? | x |  |  | Technically, for this level of confidentiality encryption would not be required. For this project, encryption was added. |
| 40. Does the application comply with your organization’s standards regarding encryption? | x |  |  | Yes, this is what Dr. Anand required. |
| 41. Are standard, accepted encryption protocols being used, rather than homegrown algorithms? | x |  |  | AES |
| 42. Are passwords encrypted in transit and at rest? |  |  | x | No passwords are being stored or sent. |
| 43. Are keys used with encryption protocols managed securely in the application? |  | x |  | No, they are hardcoded key, lol. |
| **Performance** | | | | |
| 44. Is the application thread-safe? |  |  |  |  |
|  | **Yes** | **No** | **N/A** | **Comments/Evidence/Rationale** |
| 45. Are variables encapsulated to limit their scope and prevent sharing between processes? |  | x |  |  |
| 46. Are efficient algorithms used? | x |  |  |  |
| 47. Are database transactions clearly defined and not subject to deadlocks? |  |  | x | No databases are being called. |
| 48. Are database tables indexed appropriately? |  |  | x | Please see question 47. |
| 49. Are files handles and connections to external systems explicitly closed? |  |  | x | Please see question 47. |
| 50. Are all variables that are initialized actually used? |  |  | x | Please see question 47. |