|  |  |  |  |
| --- | --- | --- | --- |
| Design Area | Requirement | Pass | Fail |
| Data flow | Are user inputs used to directly reference a business logic? |  |  |
| Design flow | Is there a potential for data binding flaws? |  |  |
| Design flow | Is the execution flow correct in failure cases? |  |  |
| Authentication & Authorization | Does the design implement access control for all resources? |  |  |
| Authentication & Authorization | Are sessions handled correctly? |  |  |
| Authentication & Authorization | Can any functionality be accessed without authentication? |  |  |
| Existing security control | Are there any known weaknesses in third-part security controls |  |  |
| Existing security controls | Is the placements of security controls correct? |  |  |
| Architecture | Are connections to external servers secure? |  |  |
| Architecture | Are inputs from external sources validated? |  |  |
| Configuration file & data storage | Is there any sensitive data in configuration files? |  |  |
| Configuration files & data storage | Can unauthorized user access configuration or data files? |  |  |
| Data flow | Does application use centralized input validation? |  |  |
| Data flow | Does application rely on a client-side validation? |  |  |
| Data flow | Does application validate for type, range, format and range ? |  |  |
| Authentication | Does application support password expiration periods ? |  |  |
| Authentication | Does application use secure communication channels ? |  |  |
| Authorization | Does application support privileges granularity? |  |  |
| Configuration | Are credentials hard-coded in the source code? |  |  |
| Secure communication channel | Is transport of sensitive data over the wire encrypted? |  |  |
| Cryptography | Does application use proven and tested cryptography algorithms? |  |  |
| Cryptography | Does application use right encryption algorithms and key sizes? |  |  |
| Cryptography | Are encryption keys stored in a restricted location? |  |  |
| Exception handling | Does application use a structure exception handling? |  |  |
| Exception handling | Do application’s exceptions reveal implementation details? |  |  |
| Exception handling | Are passwords logged by the application? |  |  |
| Exception handling | Does application use centralized exception management framework? |  |  |

Reference: Design Guidelines for Secure Web Application, <https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648647(v=pandp.10)?redirectedfrom=MSDN>