|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sl no** | **Vulnerability Category** | **Vulnerabilities/Test Cases** | **Severity** | **Status** |
| 1 | Broken Access Control | Horizontal Privilege Escalation | High | Passed |
| Vertical Privilege Escalation | High | Passed |
| Failure to Restrict URL Access | High | Passed |
| IDOR- Insecure Direct Object Reference | High | Passed |
| Password Reset by Manipulating UID | High | Passed |
| Unauthorized Access | High | Passed |
| Context-Dependent Privilege Escalation | High | Passed |
|  |  |  |  |  |
| 2 | Cryptographic failure/Sensitive data exposure | Weak cryptographic algorithms | Medium | Passed |
| Sensitive data transmitted in clear text | High | Failed |
|  |
| Server side configuration file, webservice,WSDLs,backup files are accessible | Medium | Passed |
| Database and server information present over internet | High | Passed |
| Default crypto keys in use, weak crypto keys generated  and can be re-used | Medium | Passed |
| Username,Password,Banking data , Secret PIN, Health records disclosure | High | Passed |
|  |
|  |
| Username Travelling in Cookie | Medium | Passed |
| Cacheable HTTPS response | Low | Passed |
| Source code disclosure | High | Passed |
| Robot.txt file is accessible | Info | Passed |
| Internal path disclosure | Low | Passed |
|  |  |  |  |  |
| 3 | Injection | Reflected Cross site scripting | Medium |  |
| Passed |
|  |
| Stored Cross site scripting | High | Passed |
| DOM Cross site scripting | Low | Passed |
| SQL Injection | High | Passed |
| CSV Injection | Medium | Passed |
|  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |
| HTML Injection | Low | Passed |
| Code Injection | High | Passed |
| LDAP Injection | High | Passed |
| Command Injection | High | Passed |
|  |  |  |  |  |
| 4 | Insecure design | Missing or ineffective control design | Medium | Failed |
|  |  |  |  |  |
| 5 | Security Misconfiguration | Brute Force Attack on Login Page | Medium | Passed |
| XXE | High | Passed |
| Missing Password/PIN strength validation on the server side | High | Passed |
| PIN Expiration Date Bypass on Server Side | High | Passed |
| Cross-Site Request Forgery (CSRF) | Medium | Passed |
| Improper Cache Control/Back Button Enabled | Medium | Passed |
| Unwanted File/Path Disclosure (Database Error Message Disclosure) | Medium | Passed |
| Password Reset Link Is Not Expiring | Medium | Passed |
| Weak Password | Medium | Passed |
| Activation Code Working for Multiple User Registration | High | Passed |
| Password/PIN History not maintained | Medium | Passed |
| Rate Limiting on Login Page/ Lockout policy not implemented | Low | Passed |
| Information Disclosure / Server Banner Disclosure | Low | Passed |
| HTTP Methods are enabled | Low | Passed |
| Insecure CORS configuration | Medium | Passed |
| Buffer overflow | High | Passed |
| Clickjacking | Low | Passed |
| No Logout Functionality | Low | Passed |
| Email Content Spoofing | Low | Passed |
| Out of Band Resource Loading | Medium | Passed |
| Content Manipulation | Low | Passed |
| All Tabs Don’t Logout Automatically | Low | Passed |
| API key not Expiring | Medium | Passed |
| Flash and Silverlight Cross Domain Policy | Low | Passed |
| Integer Overflow  | Restrict the Size of Strings | Medium | Passed |
| Directory Listing | Medium | Passed |
| Improper implementation of forgot password functionality | Medium | Passed |
| Incorrect permissions | Low | Passed |
| Cloud misconfiguration | Low | Passed |
|  |  |  |  |  |
| 6 | Vulnerable and Outdated Components | Using component with known vulnerability | Low |  |
| Failed |
|  |
| Older versions of components(both client-side and server-side) | Low | Failed |
|  |  |  |  |  |
| 7 | Identification and Authentication Failures | Default credentials | High | Passed |
| Authentication Bypass | High | Passed |
| Improper session management | High | Passed |
| Session identifier in the URL | High | Passed |
| Reuse session identifier after successful login | High | Passed |
| persistent cookie | High | Passed |
| Session is not expiring immediately after logging out/after limited period of user inactivity | Medium | Passed |
| Session Replay Attack | High | Passed |
| Improper Session Timeout | High | Passed |
| User Session Token Not Expire After logout(JWT Token) | High | Passed |
| Improper Session Termination on Password Change | High | Passed |
| Session Cookie Not Expire After Logout | Medium | Passed |
| Authenticated Page Loaded in unauthenticated Session | Medium | Passed |
| Secure cookie attributes are not implemented properly | Low | Passed |
| Session fixation | Medium | Passed |
| Session Ids are not validated at server side | High | Passed |
| Second factor authentication is not properly implemented in critical application/ modules | Medium | Passed |
|  |  |  |  |  |
| 8 | Software and Data Integrity Failures | Insecure Deserialization | High | Passed |
| Use of critical data or apps without verification | Medium | Passed |
| Application relies upon plugins, libraries, or modules from untrusted sources, repositories |  |  |

...