**Application Security Test Certificate**

|  |  |
| --- | --- |
| **Certificate Ref. No:** | **Issue date** |
| TCG Kol/Events/Dept-IT/CERT-In/01 | 07/05/2020 |

|  |  |
| --- | --- |
| **Name of Organization** | **{{Name}}** |
| **Website Tested:** | **Events Portal – Dept of IT, Govt of WestBengal** |
| **Test Url:** | **https://events-itewb.nltr.org** |
| **Host Url:** | **https://events-itewb.nltr.org** |
| **Production URL** | **https://events-itewb.gov.in** |
| **Test/ Audit Agency:** | **TCG Digital Solutions Private Ltd.** |
| **Testing/ Audit Dates:** | **28th January to 29th January, 2020 (1st Round of Testing)**  **26th March to 31st March, 2020 (2nd Round of Testing)**  **15th April 2020 (3rd Round of Testing)**  **29 th April 2020 (Final Round of Testing)** |

**Test/ Audit Result Summary:**

|  |  |  |  |
| --- | --- | --- | --- |
| **OWASP Top Ten (2021)** | **Web Application Vulnerabilities** | **Compliance** | **Remark** |
| A1 | Injection | Satisfactory | Nil |
| A2 | Broken Authentication | Satisfactory | Nil |
| A3 | Sensitive Data Exposure | Satisfactory | Nil |
| A4 | XML External Entities (XXE) | Satisfactory | Nil |
| A5 | Broken Access Control | Satisfactory | Nil |
| A6 | Security Misconfiguration | Satisfactory | Nil |
| A7 | Cross-Site Scripting (XSS) | Satisfactory | Nil |
| A8 | Insecure Deserialization | Satisfactory | Nil |
| A9 | Using Components with Known Vulnerabilities | Satisfactory | Nil |
| A10 | Insufficient Logging & Monitoring | Satisfactory | Nil |

**Note:**

This Certificate is valid for one year from the date of issue or till any change in the application or any new vulnerability is discovered, whichever is earlier.

**Conclusion:**

The above-mentioned web application is free from OWASP Top 10, 2017 (and any other known) vulnerabilities and is Safe for Hosting.

**Recommendation:**

1. Entire application to be deployed over SSL on production server
2. The application may be hosted with Read-Only permission
3. The Write Permission should be granted only on the folder where the files are to be uploaded
4. Web server and OS level hardening need to be in place for the production server.

**A close up of a device

Description automatically generated Tested by: Analysed by: Approved by:**

**A close up of a logo

Description automatically generated **

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Varun Bansal Abir Ranjan Atarthy Indranil Banerjee**

**A CERT-In Empanelled Information Security Auditing Organization**