(158)

Govt. of Jharkhand

Department of Information Technology & e-Gov.

Jharkhand Mantralaya, Dhurwa, Ranchi-834004.

Letter No- WAMIS-99/2016 - 1094 Ranchi, Dated...17/04/18

From,

U. P. Sah,
Director.

To,

Raj Kumar Gupta,
OSD, JAPIT

Subject: Regarding migration of WAMIS from JAPIT Data Center to State Data Center

Dear Sir,

In reference to the above mentioned subject this is to inform that the security audit of WAMIS (Works And Accounts Management Information System) has been completed successfully. So, in this regard it is necessary to migrate the WAMIS application from the JAPIT Data Center to State Data Center.

Please find enclosed Security Clearance Certificate provided by the agency and inform the relevant authority to complete the formalities for this migration.

Yours Faithfully,

Umesh

(U.P. Sah)
Director

Memo No: 1094 Dated: 17/04/18

Copy to: Sri Rajesh Sinha, Project Coordinator, JAPIT/ Sri Mahavir Tirkey, Sr. Tech. Officer, CDAC for necessary information and action.

Umesh

(U.P. Sah)
Director

Business With Wisdom
...Growth With Assurance

DIGITAL AGE STRATEGIES PVT. LTD.

IT Security Solution Providers & IS Auditors
Corporate Office # 28, "Om Arcade", 2nd & 3rd Floors, Thimmappa Reddy Layout,
Hulimavu, Bannerghatta Road, Bangalore 560 076, India
Ph : 91-080-26485148, 26484636, 41503825, 49568066, 41218560
Mobile : 9448088666 / 9448055711, CIN : U74140KA2004PTC033526
Email : audit@digitalage.co.in / dinesh.shastri@digitalage.co.in

Security Clearance Certificate forDepartment of Information Technology & e-Gov., Jharkhand

Site Name: Department of Information Technology & e-Gov., Jharkhand

Hosting URL:http://112.133.209.134:9090/wamis/login.do

Audit URL:http://112.133.209.134:9090/wamis/login.do

http://112.133.209.134:9090/security/login.do

AuditPerformed by: Ms. Uma Choudhary

Issuing Date:12th March, 2018

Testing Dates:19th February, 2018to12th March, 2018

Conclusion: Site is free from OWASPand other known vulnerabilities and is safe for hosting.

Recommendation:

1. Web server should go through VA/PT on regular intervals as server side vulnerability can be used to exploit the web applications.
2. Any change in the source code of the audited web application requires a VA/PT.
3. SSL for all the web applications is recommended.
4. Web server and OS level hardening need to be in place for the production server.
5. Entire website may be hosted with Read and Script Execution permission.
6. Entire website may be deployed over TLS 1.1 or TLS 1.2 or higher.

Our opinion is valid for the period during which the changes are not made in the source of the application thus changing the system requiring re-audit and is based on the information and the website contents provided for audit. Projection of any conclusions based on our findings for future periods and application versions is subject to the risk that the validity of such conclusions may be altered because of changes made to the application or system or the failure to make the changes to the system when required.

Note: As per the Audit Policy of NIC/SDC, it is essential to refer the website for re-audit on addition of any new Dynamic content.

Dinesh S Shastri (CISA - 230592)
CISA, CISM, CEH, CHFI
IS Auditor
Digital Age Strategies Pvt. Ltd.
Date:12th March, 2018
Place: Bangalore