सी डैक
CDAC

प्रगत संगणन विकास केंद्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
(A Scientific Society of Ministry of Communications and Information Technology, Government of India)
Plot No. 6 & 7, Hardware Park, Sy No. 1/1, Srisailam Highway, Pahadi Shareef Via Keshavagiri (Post), Hyderabad – 501510
Email: cdachyd@cdac.in **Website:** www.cdac.in
Cert-In Empaneled Organization

ID # CH/ISS-CT-775/2019

AUDIT CERTIFICATE

Application Name	Jharkhand Bijli Vitran Nigam Limited Portal
Test URL	https://59.145.221.106/
Test dates	19th March 2017 to 09th July 2019
Conclusion	Website is free from OWASP vulnerabilities and any known vulnerabilities. It is safe for public hosting.
Production URL	https://jbvnl.co.in

Recommendations

1. Website may be considered safe for hosting with read only permissions. **YES**
2. Entire website should be implemented over SSL/TLS
3. The production server should have operating system and web server hardening done.
4. The Server should be physically protected from unauthorized access

Note:

- The certification is valid till no changes are done on the application's dynamic content or one year from the date of issue whichever is earlier.
- The Certificate is generated based on the enclosed closure report.

Date of Issue: 12-07-2019

Centre for Development of Advanced Computing
Hyderabad

Ch.A.S.Murty
Information Security Services
C-DAC, Hyderabad

This certificate can be verified at : https://cdac.in/verify-sth

Web Application Security Testing Closure Report of JBVNL

Testing URL: https://59.145.221.106/

Report Submission Date: 9-07-2019

Centre for Development of Advanced Computing (C-DAC),
Hyderabad.

Application Test Environment

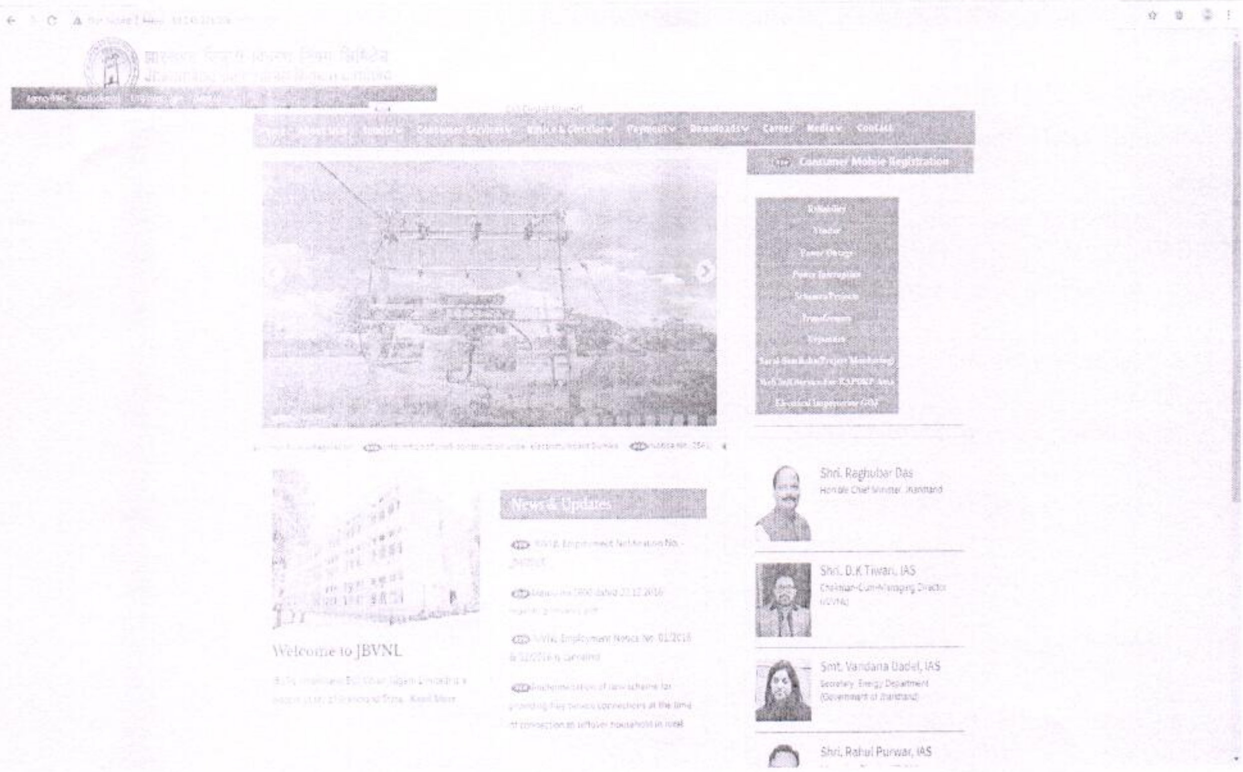
1. Name and address of client	Jharkhand Bijli Vitaran Limited(JBVNL)
2. Description & Identification of Item	https://59.145.221.106/
3. Sample Received on	19/03/2019
4. Test Completed on	9/07/2019
5. No. of items tested	One
6. Test performed at	C-DAC Hyderabad
7. Standard/ Test Procedure reference	CDAC IT Services checklist & OWASP Checklist
8. Scopes	Application Security Testing
9. Major Equipment/ Tool used	Burp Professional, Acunetix

1. Introduction

C-DAC has conducted three rounds of Security Audit on "JBVNL" web application which is installed in staging server and accessible at "https://59.145.221.106/" Stage 1 testing is done on 19/03/2019, and final stage on 9/07/2019. This report documents the conclusion results for further stages of Security Testing. The objective of the entire test was to find out vulnerabilities that can be seen and compromise the application by malicious users. The results indicate the status of the application during the evaluation period only.

2. Application Overview

The JBVNL application which is accessible throughhttps://59.145.221.106/, this site is web portal customized for Jharkhand Bijli Vitran Nigam Limited. This is web application provides different modules like Consumer Mobile Registration, Notice and Circular. Also there are some modules like Payment, E-tender, Employee login, Agency , Consumer Services which redirect to different domain that are not in scope of audit.



3. Scope

The Security Audit scope is restricted to testing the JBVNL website through web URL https://59.145.221.106/

4. Evaluation Methodology

Different security testing techniques (both manually and using tools) were employed to unearth application security vulnerabilities, weaknesses and concerns in the following aspects

1. Input Validation
2. Authentication and Session Management
3. Access Control
4. Error Handling
5. Data Protection
6. Denial of Service
7. File Extensions Handling
8. Web Application Finger Print
9. Insufficient Logging & Monitoring

5. Overview of findings

The following table gives of overview of the findings and their status by the end of our security audit process.

Sl no	Name of Vulnerability	Stage I	Final Stage
1	**Reflective Cross-site Scripting**	OPEN	CLOSED
2	**Directory Listing**	OPEN	CLOSED
3	**Missing Custom Error Pages**	OPEN	CLOSED
4	**Unwanted HTTP Methods**	OPEN	CLOSED
5	**Sensitive Information Leakage**	OPEN	CLOSED
6	**PhpMyAdmin Login Page Visible**	OPEN	CLOSED
7	**Arbitrary HTTP Methods**	OPEN	CLOSED
8	**Outdated Components**	OPEN	CLOSED
9	**Session ID Name Fingerprinting**	OPEN	CLOSED
10	**Web Server Version Disclosure**	OPEN	CLOSED
11	**Email Address Disclosure**	OPEN	CLOSED
12	**Missing Security Headers**	OPEN	CLOSED

Sl no	Name of Vulnerability	Stage I	Final Stage
13	Missing Anti-Automation	OPEN	CLOSED
14	Improper Invalidation	OPEN	CLOSED
15	Breach Vulnerability	OPEN	CLOSED
16	Beast Vulnerability	OPEN	CLOSED

Note*- The j-query parse click counting query error notification displayed on homepage. Client has accepted the risk and informed that it will be resolved in the production server.

The Testing Methodology and Standards followed for performing Security audit was OWASP Methods and Standards and thus this report is generated in compliance with OWASP Vulnerabilities. The following table comments on the "https://59.145.221.106/" website against OWASP top 10 – 2017 Vulnerabilities.

#	Vulnerabilities	Status
1	Injection	Safe
2	Broken Authentication	Safe
3	Sensitive Data Exposure	Safe
4	XML External Entities (XXE)	Safe
5	Broken Access Control	Safe
6	Security Misconfiguration	Safe
7	Cross-Site Scripting (XSS)	Safe
8	Insecure Deserialization	Safe
9	Using Components with Known Vulnerabilities	Safe
10	Insufficient Logging and Monitoring	Not Safe

6. Detailed Observations:

#	Category	Particulars	Observations	Remarks
1	Input validation	Information from user requests should be properly validated before being used by the applications.		
1.1	Script injection	Ensure that any part of the application that allows input, does not process script as a part of input	Scripts are not allowed in the application	Complied with
1.2	Blind SQL Injection	Ensure the application will not process SQL commands from the user	Blind SQL Injections are not accepted by the application by the end of audit	Complied with
1.3	OS Command Injection	Ensure the applications will not process operating system commands from the user	It is observed that the application did not have the OS command injection	Complied with
1.4	IFRAME Injection	Ensure the application should not allow the iframe injection at the client side validation	IFRAME were not allowed in the application	Complied with
1.5	Cross Site Scripting(XSS)	Ensure that the application will not store or reflect malicious script code	The application allows the malicious special characters with in the input fields	Complied with
1.6	Cross Site Request Forgery	Ensure that the application will not process Cross site	It is observed that the application did not have the CSRF Injection.	Complied with
1.7	XML injection	Ensure that XML parser should validate the data to prevent attacks like XXE	It is observed that the application did not have the XML Injection	Complied with
1.8	Insecure Deserialization	Ensure that data in application is properly sanitized during deserialization process	It is observed that the data in application is properly sanitized during deserialization process	Complied with

#	Category	Particulars	Observations	Remarks
2	Authentication and Session Management	Ensure security of the authentication credentials like, passwords, cookies, keys and other session tokens		
2.1	Secure Authentication endpoints	Ensure that users are only asked to submit details on pages that are served with SSL	The credentials are sent through the encrypted channel	Complied with
2.2	Authentication bypass	Ensure that the authentication process cannot be bypassed	Authentication mechanism is not implemented in the application.	Not Applicable
2.3	Secure Transport of Credentials	Ensure that usernames and passwords are sent over an encrypted channel	Authentication mechanism is not implemented in the application.	Not Applicable
2.4	Default Accounts	Check for default account names and passwords in use	Authentication mechanism is not implemented in the application.	Not Applicable
2.5	Password Quality	Ensure that the system enforces to use quality passwords only	Authentication mechanism is not implemented in the application..	Not Applicable
2.6	Password Reset	Ensure that the user must respond to a secret answer or secret question or other predetermined information before passwords can be reset	Authentication mechanism is not implemented in the application..	Not Applicable
2.7	Password Lockout	Ensure that the users account is locked out for a period of time when the incorrect passwords is entered more than a specific number of times (usually 5).	Authentication mechanism is not implemented in the application.	Not Applicable
2.8	Restricted characters in Password	Ensure that special meta characters (', =,-etc.)cannot be used within the password	Authentication mechanism is not implemented in the application.	Not Applicable
2.9	Blank Passwords	Ensure that blank passwords are not allowed	Authentication mechanism is not implemented in the	Not Applicable

#	Category	Particulars	Observations	Remarks
			application.	
2.10	Password Auto Complete	Ensure password auto complete should be disabled in sensitive application	Authentication mechanism is not implemented in the application.	Not Applicable
2.11	Session Token Length	Ensure that the session token is of adequate length to provide protection from guessing during an authenticated session.	Authentication mechanism is not implemented in the application.	Not Applicable
2.12	Session Timeout	Ensure that the session tokens are only valid for a predetermined period after the Last request by the user.	Authentication mechanism is not implemented in the application.	Not Applicable
2.13	Session Reuse	Ensure that session tokens are changed when the user moves from an SSL protected resource to a non- SSL protected Resource. The sessions are maintained properly.	Authentication mechanism is not implemented in the application.	Not Applicable
2.14	Session Deletion	Ensure that the session token is invalidated when the user logs Out.	Authentication mechanism is not implemented in the application.	Not Applicable
2.15	Session Token Format	Ensure that the session token is non-persistent and is never written to the browsers history or cache.	Authentication mechanism is not implemented in the application.	Not Applicable
2.16	CAPTCHA implementation	Ensure that the sensitive application needs CAPTCHA implementation to avoid automated GET/POST request in a short time	CAPTCHA is implemented	Complied with
3	Access Control	Ensure controlled access to the resources/services by the authenticated users as per the access control policy		
3.1	Parameter Analysis	Ensure that application enforces its access control model by	Application performs all parameter	Complied with

#	Category	Particulars	Observations	Remarks
		ensuring that any parameters available to an attacker would not afford additional service.	analysis and does not allow tampering	
3.2	Authorization	Ensure that resources that require authorization perform adequate authorization checks before being sent to a user	No Authorization mechanism is implemented	Not Applicable
3.3	Authorization Parameter Manipulation	Ensure that once a valid user has logged in, it is not possible to change the session ID's parameter to reflect another user account	No Authorization mechanism is implemented	Not Applicable
3.4	Authorization Pages/functions	Check if it is possible to access pages or functions that require logon but can be bypassed	Authorization bypass is not possible	Not Applicable
3.5	Application Workflow	Ensure that where the application requires the user to perform actions in a specific sequence, the sequence is enforced	Application workflow is maintained	Complied with
4	Error Handling	Ensure proper error handling by the application to avoid information leakage		
4.1	Application Error Messages	Application does not present application error messages to an attacker that could be used in an attack	Application error messages were not revealing any type of server information.	Complied with
4.2	User Error Messages	Ensure that application does not present user error messages to an attacker that could be used in an attack	User error messages were not found	Complied with
5	Data Protection	Ensure implementation of strong cryptography to avoid compromise of sensitive user authentication information during storage, use or transmission		
5.1	Sensitive Data in HTML	Ensure that there is no sensitive data in the HTML (cached in the browser history) that could lead an attacker to mount a focused attack.	No sensitive data found in HTML	Complied with
5.2	Sensitive Data in HTML	Ensure that supported SSL versions do not have cryptographic weakness	TLS 1.2	Complied with

#	Category	Particulars	Observations	Remarks
5.3	SSL Key Exchange Methods	Ensure that the web server does not allow anonymous key exchange methods	SHA 256	Complied with
5.4	SSL Algorithms	Ensure that weak algorithms are not available	RSA	Complied with
5.5	SSL Key Lengths	Ensure the website uses an appropriate length key.	2048	Complied with
5.6	Digital Certificate Validity	Ensure the application uses valid digital certificates	1/11/2018 to 29/10/2028	Complied with
6	Denial of Service	Ensure that the applications are equipped to handle different denial of service attacks		
6.1	Application Flooding	Ensure that the application function correctly when presented with large volumes of requests, transactions, and/or network traffic	For all the input fields boundaries were mentioned in the server side	Complied with
6.2	Application lockout	Ensure that the application does not allow an attacker to reset or lockout users account	Login mechanism is not implemented.	Not Applicable
7	File Extension Handling	Should not allow to upload .exe, .vbs files in the application	File Upload Functionality is not present.	Not Applicable
8	Web application finger print	Ensure that application server information should not reveal	Application server information is not revealed.	Complied with
9	Logging & Monitoring	Ensure that logs (application & server) are properly maintained.		
9.1	Sensitive information in logs	Ensure that the logs should not store any sensitive information such PII, credentials, passwords, transaction details etc.	The application is not saving any sensitive information about the JBVNL application in logs	Complied with
9.2	Log Location	Ensure that the logs are stored in separate location & not in the web server itself	It is observed that logs are stored in the application server only.	Not Complied With
9.3	Log consumption	Ensure that log usage does not generate denial of service condition.	It is observed that logs are having minimum information not	Complied With

#	Category	Particulars	Observations	Remarks
			causing denial of service	
9.4	Log rotation	Ensure that logs are kept for the sufficient time and are rotated properly.	It is observed that the logs are rotated for every 6 months.	Complied With
9.5	Log Access Control	Ensure that proper log access control mechanism is implemented	It is observed that log access control is provide to restricted user	Complied With
9.6	Log review	Ensure that log support/meeting the needs for future analysis in case of an unwanted event, like 404,500,503 etc.,	It is observed that Error logs are maintained.	Complied With

7. Recommendations for Deployment Server:

1. The web application component may be considered safe for hosting with read only permissions.
2. Hosted server should be configured with for transmitting the data over SSL/TLS
3. The production server should have operating system and web server hardening done.
4. The Server should be physically protected from unauthorized access.
5. Sanitized Logging and regular monitoring of the logs is recommended. Logs should be maintained for a period of 1 year or more where ever deployed.

8. Conclusions

Site may be considered safe for hosting and is secured for deployment **YES**

Verified and reviewed by

Signature: K.Indr

Name : K.Indraveni

Date: 12/07/19

Centre for Development of Advanced Computing
Hyderabad

Approved by

Signature:

Name: Ch.A.S.Murty

Date: 12.07.19