SECURITY AUDIT REPORT

for

Transplant Authority of Tamil Nadu

CONFIDENTIAL

DISCLAIMER

All information contained in this document is confidential and proprietary to the Cyber Security Architecture of Tamil Nadu (CSA-TN) project. Use of any information contained in this document by photographic, electronic or any other means, in whole or part, for any reason other than for the purpose of operations /network security enhancement of the **Transplant Authority of Tamil Nadu** is strictly prohibited without written consent.

CSA-TN shall assume no liability for any changes, omissions, or errors in this document. All the recommendations are provided on as is basis and are void of any warranty expressed or implied. CSA-TN shall not be liable for any damages financial or otherwise arising out of use/misuse of this report by any current employee of CSA-TN or any member of the general public.

The complete scanning has been carried out as an outside entity without login credentials of Server.

1.0 Introduction

This document describes the proceedings and findings of Security Assessment conducted on various public servers in the **Transplant Authority of Tamil Nadu** to assess the security of the service/resource implemented.

2.0 Scope of Audit

Department Name	Transplant Authority of Tamil Nadu
Organisation Name	Health and Family Welfare Department
Type of Audit	Audit without credentials
Number of Applications scanned	2
Overall Scan Rating	~~Satisfactory~~ ~~Needs Review~~ Needs Immediate Attention
Conclusion	**The application servers will be more secure with the given recommendations and identified issues fixed.**

3.0 Audit Objective

Identification of the below issues -

- ➢ Known Operating System holes/ vulnerability.
- ➢ Unintentional Services running behind.
- ➢ Missing security patches/updates.
- ➢ Vulnerabilities that could allow unauthorised control or access to sensitive data on a system.
- ➢ Misconfiguration.

3.1 Audit Observations:

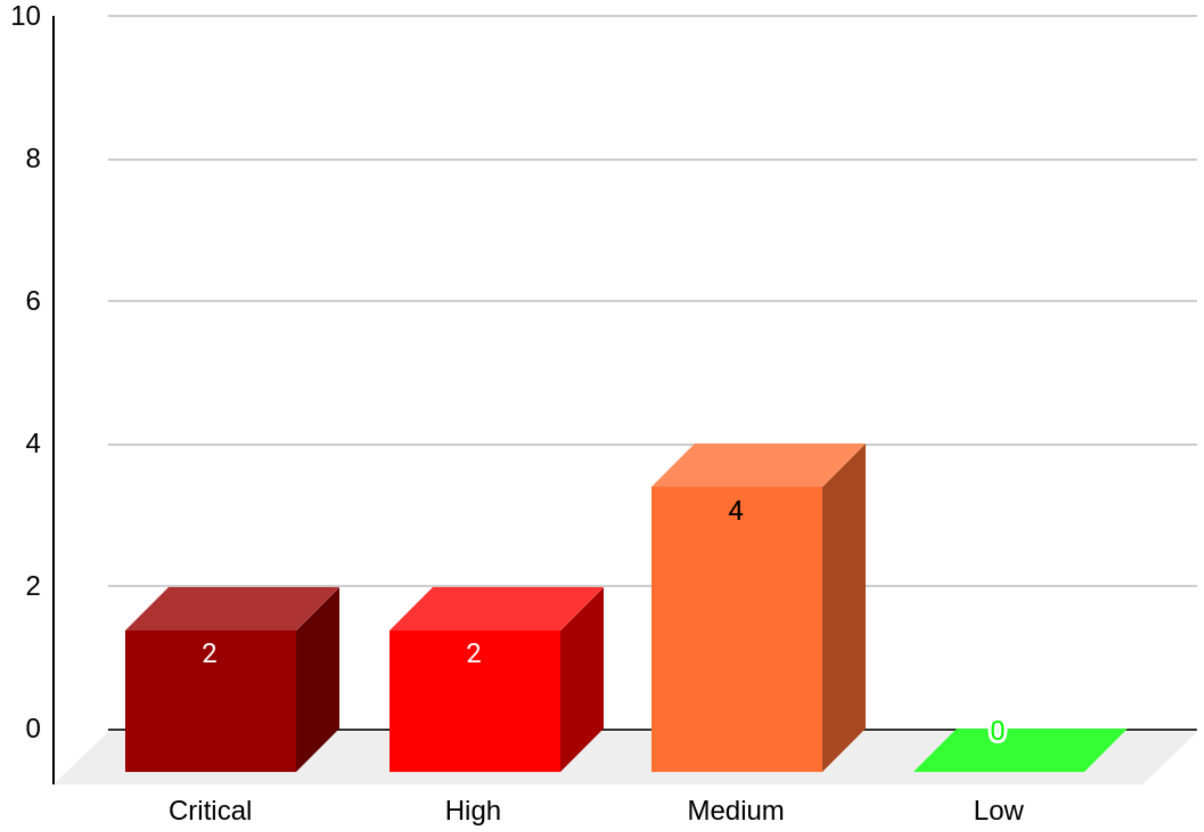
This Document enlists the

- List of URL(S) Scanned.
- Server Vulnerabilities identified on the Scanned URL(S)
- SSL Certificate Status for the Scanned URL(S).
- Overall recommendation.

3.1.1. List of URL(S) Scanned

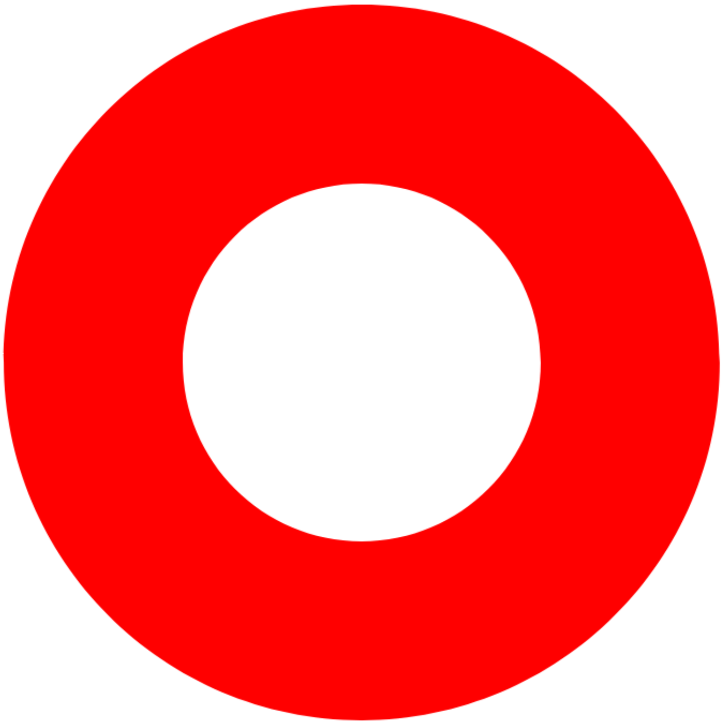
S. No	Application Name	URL	Scan Outcome	Recommendations, if any, for the URLs are found at the below sections
1	transtanregistry	https://registry.transtan.tn.gov.in	Satisfactory	NIL
2	transtan	http://transtan.tn.gov.in	Needs Immediate Attention	3.1.4.1, 3.1.4.2, 3.1.4.3, 3.1.4.4, 3.1.4.5, 3.1.4.6, 3.1.4.7, 3.1.4.8

3.1.2 Server Vulnerabilities identified on the Scanned URL(S)



Towards making the departmental application more secure it is recommended to fix the major findings to prevent attacks.

3.1.3 SSL Certificate Status for Scanned URL(S):



S.No	Application Name	URL	SSL Support
1	transtanregistry	https://registry.transtan.tn.gov.in	NO
2	transtan	http://transtan.tn.gov.in	NO

3.1.4. Overall Recommendation

section	Issues Identified	Solution
1	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability. **Technical Notes** The version of PHP running on the remote web server is prior to 7.1.33, 7.2.x prior to 7.2.24, or 7.3.x prior to 7.3.11. It is, therefore, affected by a remote code execution vulnerability due to insufficient validation of user input. An unauthenticated, remote attacker can exploit this, by sending a specially crafted request, to cause the execution of arbitrary code by breaking the fastcgi_split_path_info directive.	Upgrade to PHP version 7.3.11 or later.
2	PHP Unsupported Version Detection **Technical Notes** The remote host contains an unsupported version of a web application scripting language. According to its version, the installation of PHP on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the	Upgrade to a version of PHP that is currently supported.

	vendor. As a result, it is likely to contain security vulnerabilities.	
3	PHP < 7.3.24 Multiple Vulnerabilities **Technical Notes** The version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities	Upgrade to PHP version 7.3.24 or later.
4	SSL Medium Strength Cipher Suites Supported (SWEET32) **Technical Notes** The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.	Reconfigure the affected application if possible to avoid use of medium strength ciphers**.**
5	HSTS Missing From HTTPS Server (RFC 6797) **Technical Notes** The remote web server is not enforcing HSTS. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections	Configure the remote web server to use HSTS (HTTP Strict Transport Security).
6	Browsable Web Directories **Technical Notes** Multiple plugins identified directories on the web server that are browsable.	Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

7	PHP < 7.3.28 Email Header Injection **Technical Notes** The version of PHP running on the remote web server is prior to 7.3.28. It is, therefore, affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content.	Upgrade to PHP version 7.3.28 or later.
8	Web Application Potentially Vulnerable to Clickjacking **Technical Notes** The remote web server may fail to mitigate a class of web application vulnerabilities.	Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

General instructions :

1. One should review the above recommendation to ensure that the firewall configuration settings meet your organisation’s requirements.
2. Deploy and quickly update antivirus and antimalware software across all systems and monitor for attempts to remove or disable it.
3. Monitor sensitive objects for modification attempts and OS for events that may indicate attempted compromise.
4. Protect and monitor accounts for users who have access to sensitive data.
5. Recommended to have IT policy for the department.
6. Unnecessary ports should be blocked which are not required for the systems as they pose a serious security threat.