Cyber Security Assessment Report

of

TTD,

TTD,

Govt. of AP

01/11/2019

by

Andhra Pradesh Technology Services

3rd Floor, R&B Building, M.G. Road, Labbipet,

Vijayawada – 520 010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc23518112)

[1.1. Introduction 3](#_Toc23518113)

[1.2. Engagement Specific Details 3](#_Toc23518114)

[1.3. Scope Details 4](#_Toc23518115)

[1.3.1. Inclusion 4](#_Toc23518116)

[1.3.2. Exclusion 4](#_Toc23518117)

[1.4. Approach & Methodology 4](#_Toc23518118)

[1.4.1. Information Gathering: 4](#_Toc23518119)

[1.4.2. Automated & Manual Scanning: 4](#_Toc23518120)

[1.4.3. Analyse results and reporting: 4](#_Toc23518121)

[1.5. Risk Categorization 5](#_Toc23518122)

[1.6. Vulnerability Summary 6](#_Toc23518123)

[1.6.1. Distribution of Observation 6](#_Toc23518124)

[2. Detailed Observation 7](#_Toc23518125)

[2.1. Web Application Security Assessment & Penetration Testing 7](#_Toc23518126)

[3. Scanned Items 19](#_Toc23518127)

[4. Limitations 26](#_Toc23518128)

1. Executive Summary

## Introduction

Tirumala Tirupati Devasthanams (TTD) is an independent trust which manages the [Tirumala Venkateswara Temple](https://en.wikipedia.org/wiki/Tirumala_Venkateswara_Temple) at [Tirumala](https://en.wikipedia.org/wiki/Tirumala), [Andhra Pradesh](https://en.wikipedia.org/wiki/Andhra_Pradesh). The trust oversees the operations and finances of the second richest and the most visited religious center in the world. It is also involved in various social, religious, literary and educational activities. TTD is headquartered at Tirupati and employs about 16,000 people.

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Cyber Security Assessment of TTD Application for TTD Department to determine, if any weakness exist in the application.

## Engagement Specific Details

|  |  |  |
| --- | --- | --- |
| 1. **S. No.** | **Activity** | 1. **Date** |
| 1. 1. | 1. Start date of engagement | 1. 31/10/2019 |
| 1. 2. | 1. Submission date of initial report | 1. 01/11/2019 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | 1. APTS Team | 1. Name | 1. TTD |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 01/11/2019 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

1. **Web Application Security Assessment & Penetration Testing**

Application Name: Tirumala Tirupati Devasthanams

Application URL: https://tirumala-uat.tirumala.org

Environment: UAT

Version Number [or] Latest Compilation Timestamp: Not Provided

Type of Review: Black box

Hash of Zipped Source Code (SHA512):Not Provided

### Exclusion

1. Secure Code Review
2. Process Review
3. Secure Network Architecture Review

## Approach & Methodology

1. The web application security assessment was conducted in line with the leading security standards and guidelines for web application security such as OWASP.
2. The approach followed for the security assessment is detailed below:

### Information Gathering:

We conducted a walkthrough of the web application to assess the scope of the security assessment and obtain the following information to identify the potential attack vectors:

* 1. Functionalities available in the web application
  2. Entry points for the web application
  3. Web application is custom developed or off-the-shelf application
  4. Protocols used by the web application
  5. Back-end technology including web server, framework, and development language
  6. Conduct search engine discovery and reconnaissance
  7. Banner grabbing (finger printing) to identify the running version of web server / application server and framework
  8. Enumerate application on web server to identify other applications running on the server
  9. View source of the web application to review the comments and metadata
  10. Map functionalities and data flow to identify attack vectors

### Automated & Manual Scanning:

We performed an unauthenticated automated & Manual scanning of the web application URL using commercial and open source tools. The scanning was conducted to identify any known vulnerabilities in the subjected application.

### Analyse results and reporting:

We then analysed the results from manual inspection to identify the vulnerabilities applicable to the web application. The risk classification for each of these vulnerabilities was identified based on the likelihood of occurrence, impact, and level of access required to exploit these vulnerability as per the risk classification methodology detailed in 1.5 of the report.

1. An exception based detailed report is prepared with the following:
2. Description of the vulnerability
3. Risk Rating
4. Impact & Root Cause
5. Recommendation including reference links

## Risk Categorization

The risk ratings assigned to each finding in this report are based on 3 dimensions – Likelihood, Impact, and Level of access required. These are defined below.

|  |  |  |
| --- | --- | --- |
| **Likelihood** | High | Attacker can use existing tools to exploit the vulnerability by following prescriptive instructions and without knowledge of coding/platforms. Target can be exploited directly. Finding assists with exploitation of or is linked to other high or critical risk findings. |
| Medium | Attacker must have knowledge of coding/platforms and may require customisation of tools (e.g. batch scripts, shell scripts, Metasploit module customization) to exploit the vulnerability.  Exploitation of target may require setup of additional infrastructure or processes. |
| Low | High level of skill required to exploit. Attacker must develop their own tools or processes (e.g. custom written exploit code) to successfully exploit the vulnerability.  Publicly available exploits were not identified.  Exploitation of target requires setup of additional infrastructure or processes (e.g. Spear Phishing). |
| **Impact** | Severe | Vulnerability may lead to widespread administrator access to multiple materially sensitive systems (e.g. Enterprise Administrator), or access to the internal network from the Internet. |
| Major | Vulnerability may lead to immediate access to sensitive or materially sensitive data, or highly privileged access to critical business systems, or a severe and extended disruption to critical business systems or operations, with impact to many users or sites. |
| Moderate | Vulnerability may lead to access to sensitive data, or privileged access to critical business systems, or partial disruption to critical business systems or operations, with impact to some users or sites. |
| Minor | Vulnerability may lead to:  Access to non-sensitive data, or  Access to non-critical business systems, or  Disruption to non-critical business systems or operations, with limited impact to users/sites. |
| Insignificant | Information disclosure of non-sensitive enticement information (e.g. IP addresses, hostnames, system information) with no direct impact to availability. |
| **Level of access required** | Privileged | Privileged user (e.g. administrator). |
| Non-privileged | General user (e.g. domain user). |
| Internal Anonymous | Unauthenticated user with access to the internal network. |
| External Anonymous | Unauthenticated Internet user (includes web applications that allow self-registration). |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Consequence**  **Likelihood** | **Small** | **Moderate** | **Severe** | **Catastrophic** |
| **Low** | Info | Low | Medium | Medium |
| **Moderate** | Low | Medium | Medium | High |
| **High** | Low | Medium | High | High |
| **Very High** | Medium | High | High | High |

The final risk ratings are defined as follows:

|  |  |
| --- | --- |
| High | Urgent action should be taken to address findings. |
| Medium | Action should be taken to address findings in a timely manner.  Out of cycle change and compensating controls may be required. |
| Low | No immediate action required. Remediation items can be implemented during the next scheduled change window. |
| Information | No immediate risks to the environment were identified as part of the testing. Findings are informational only. |

Note: The above matrices are intended to be used as a guide only in determining the appropriate risk rating for a particular vulnerability. Other factors may need to be considered when weighing up the final risk rating, such as the number of servers/applications affected by the vulnerability, nature of system’s affected (e.g. Production, Development, and Test), and nature of data accessed or disclosed.

## Vulnerability Summary

Below is the summary of open vulnerabilities that still exist in the application.

|  |  |  |  |
| --- | --- | --- | --- |
| **Review Area** | **Initial Review** | | |
| **High** | **Medium** | **Low** |
| **Web Application Security Assessment** | 1 | 3 | 5 |
| **Total** |  | | **9** |

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Local File Inclusion** | **Risk Rating**: High |
| **Description** | An attacker can use Local File Inclusion (LFI) to trick the web application into exposing or running files on the web server. An LFI attack may lead to information disclosure, remote code execution, or even [Cross-site Scripting (XSS)](https://www.acunetix.com/websitesecurity/cross-site-scripting/). Typically, LFI occurs when an application uses the path to a file as input. If the application treats this input as trusted, a local file may be used in the include statement. | |
| **Affected Path(s)** | https://tirumala-uat.tirumala.org/FileCS.ashx?Id=\*  https://tirumala-uat.tirumala.org/RamanujamKeertanasFileCS.ashx?Id=\*  https://tirumala-uat.tirumala.org/SaranagathiGadhyamFileCS.ashx?Id=\* | |
| **Impact** | The impacts of exploiting Local File Inclusion (LFI) vulnerability vary from information disclosure to complete compromise of the system. Even in cases where the included code is not executed, it can still give an attacker enough valuable information to be able to compromise the system. | |
| **Evidence/Proof of Concept**  **Step 1:** The Id parameter is vulnerable to LFI attacks, enabling read access to arbitrary files on the server.  lfi1.png  **Step 2:** The payload was injected in the Id parameter. The requested file was downloaded as shown in image.  lfi2.png  **Step 3:** The version of windows using is displayed in the file downloaded as shown in image.  lfi3.png | | |
| **Recommendation** | * Save the file paths in a database and assign an ID to each of them. BY doing so users can only see the ID and are not able to view or change the path. * Use a white list of files and ignore every other filename and path. * Instead of including files on the web server, store their content in databases where possible. * Instruct the server to automatically send download headers and not execute files in a specific directory such as /download/. That way you can point the user directly to the file on the server without having to write additional code for the download. An example link could look like https://example.com/downloads/brochure2.pdf | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Insufficient anti automation** | **Risk Rating**: Medium |
| **Description** | Insufficient Anti-automation is when a web site permits an attacker to automate a process that should only be performed manually. Certain web site functionalities should be protected against automated attacks. | |
| **Affected Path(s)** | https://tirumala-uat.tirumala.org/Contactus.aspx | |
| **Impact** | Attackers could repeatedly exercise web site functionality attempting to exploit or defraud the system. An automated robot could potentially execute thousands of requests a minute, causing potential loss of performance or service. | |
| **Evidence/Proof of Concept**  **Step 1:** Captcha not implemented.  insufficen anti automation.png | | |
| **Recommendation** | It is recommended to implement captcha on Contact Us page. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | 1. **Vulnerable JavaScript library** | **Risk Rating**: Medium |
| **Description** | The application is using multiple vulnerable JavaScript libraries that have the known public exploits. Using these libraries may affect the application’s security. | |
| **Affected Path(s)** | (/Web Sever) | |
| **Impact** | The vulnerabilities caused by the used vulnerable libraries could help the attacker to perform cross site scripting attacks that result in client side attacks that affect the end users. | |
| **Evidence/Proof of Concept**  **vunlerable java script .png** | | |
| **Recommendation** | Upgrade to the latest version. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Unencrypted view state** | **Risk Rating**: Medium |
| **Description** | The \_\_VIEWSTATE parameter is not encrypted. To reduce the chance of someone intercepting the information stored in the View State, it is good design to encrypt the View State. | |
| **Affected Path(s)** | (/Web Server) | |
| **Impact** | Possible Sensitive Information Disclosure | |
| **Evidence/Proof of Concept**  **Step 1:** The View state is not Encrypted as shown in Below image.  unencrypted view state'.png | | |
| **Recommendation** | Open Web.Config and add the following line under the <system.web> element:  <machine Key validation="AES"/> | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Email id disclosure** | **Risk Rating**: Low |
| **Description** | One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found. | |
| **Affected Path(s)** | https://tirumala-uat.tirumala.org/Contactus.aspx | |
| **Impact** | Email addresses posted on Web sites may attract spam. | |
| **Evidence/Proof of Concept**  **emailid disclosure.png**  Fig. Email Address disclosure | | |
| **Recommendation** | Obfuscate email address by replacing **’@‘**with [at] and **‘.’** with [dot]. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Click Jacking** | **Risk Rating**: Low |
| **Description** | Click jacking is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** | An attacker can host this domain in other evil site by using iframe and if a user fills the given field it can directly redirect as logs to attacker and after its redirect to your web server. Leading to steal user information too and use that host site as phishing of your site its CSRF and Click jacking. | |
| **Evidence/Proof of Concept**  **Step 1:** Embed the website URL in the iframe src as shown in below image.  **clickjacking code.png**  **Step 2:** The website is loaded within the frame as shown in image.  **clickjacking.png** | | |
| **Recommendation** | Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Version disclosure** | **Risk Rating**: Low |
| **Description** | The HTTP responses returned by this web application include a header named **Server**, X**-Asp Net-Version, X-Powered-By**. This value of this header includes the version of Microsoft IIS server, asp.net version. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** |  | |
| **Evidence/Proof of Concept**  **Step 1:** Application discloses the server and application framework version details in response headers.  version disclosure.png | | |
| **Recommendation** | Microsoft IIS should be configured to remove unwanted HTTP response headers from the response. Consult references links for more information.  Reference links:  https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/ | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Sub resource Integrity (SRI) not implemented** | **Risk Rating**: Low |
| **Description** | Sub resource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match. | |
| **Affected Path(s)** | https://tirumala-uat.tirumala.org/TalapakaPatakuPadhasahityam.aspx  https://tirumala-uat.tirumala.org/EDarsanCounters.aspx | |
| **Impact** | An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. | |
| **Evidence/Proof of Concept**  **sri not implemented.png**  Fig. SRI not Implemented | | |
| **Recommendation** | 1. Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Sub resource Integrity (SRI). For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match. 2. <script src="https://example.com/example-framework.js" 3. integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" 4. cross origin="anonymous"></script> | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **ASP.NET debugging is enabled** | **Risk Rating**: Low |
| **Description** | 1. ASP.NET debugging is enabled on this application. It is recommended to disable debug mode before deploying a production application. By default, debugging is disabled, and although debugging is frequently enabled to troubleshoot a problem, it is also frequently not disabled again after the problem is resolved. | |
| **Affected Path(s)** | (/Web Server) | |
| **Impact** | It may be possible that sensitive information about the web server is disclosed through the ASP.NET application. | |
| **Evidence/Proof of Concept**  **debug metod enabled.png**  Fig. ASP.NET debugging is enabled | | |
| **Recommendation** | We recommend to disable the asp.net debugging method .for more information refer to the links  Reference Links:  https://support.microsoft.com/en-in/help/815157/how-to-disable-debugging-for-asp-net-applications | |
| **Management Comments** |  | |

## Scanned Items

/

/AakatiVeLala.aspx

/AbhideyakaAbhishekam.aspx

/Abhishekam.aspx

/Aboutsrivaritemple.aspx

/Accommodation.aspx

/AccommodationAtTirumala.aspx

/AccommodationAtTirupati.aspx

/ActiveTenders.aspx

/AdivoAlladivoSriHariVasamu.aspx

/Advancebooking.aspx

/AdvanceReservationAtTirumala.aspx

/AlapaduImages.aspx

/AlaraChanchalamaina.aspx

/AlarulaKuriyagaaadenade.aspx

/AlasitiniPunyapaapamulu.aspx

/ALBUMS

/ALBUMS/bootstrap-image-gallery.js

/ALBUMS/bootstrap.min.js

/ALBUMS/jquery.blueimp-gallery.min.js

/ALBUMS/jquery.min.js

/AlwarDivyaPrabhandams.aspx

/AlwarPasurams.aspx

/AmudalavalasaImages.aspx

/Anjaneya\_TempleLegend.aspx

/Annamacharya%20project.aspx

/Annamacharya\_Keertanas\_Sravanam.aspx

/AnnamaCharyaLifeHistory.aspx

/AnnamacharyaSankeerthanas.aspx

/AnnamacharyaWebPage.aspx

/AnnualSevas.aspx

/applicationformfordonations.aspx

/Archana.aspx

/ArjithaSevas.aspx

/AshtadalaPadaPadmaradhana.aspx

/ASWA%20VAHANAM.aspx

/AutomobileClinic.aspx

/BandivallavuruImages.aspx

/BEAUTY%20OF%20GODDESS%20ON%20PALLAKI.aspx

/BelumsingavaramImages.aspx

/BirdTrust.aspx

/BrahmaKadiginaPadamu.aspx

/BrahmostavamAlbum2017Images.aspx

/BrahmostavamAlbumImages.aspx

/Bramhostavam.aspx

/BranhotsvamsEnthrall.aspx

/Cds.aspx

/CELESTIALKALYANAM.aspx

/CHAKRASNANAM.aspx

/ChandralapaduImages.aspx

/CHANDRAPRABHA%20VAHANAM.aspx

/CheruvupalliImages.aspx

/CHINNA%20SESHA%20VAHANAM.aspx

/CM%20VISIT%20TO%20TIRUMALA.aspx

/Contactus.aspx

/Copperplates.aspx

/CottageDonation.aspx

/CulturalsAlbumImages.aspx

/Current\_Booking.aspx

/DailySevas.aspx

/Dams.aspx

/DasaSahithya.aspx

/DasaSahitya.aspx

/DehradoonImages.aspx

/dewplayer-vol.swf

/DHARMIC%20SADASSU.aspx

/DigitalLibrary.aspx

/DivyaDarshan.aspx

/Documents

/Donations.aspx

/Dos\_Donot.aspx

/Downloads

/Downloads/MUSIC%20BOOKS

/Downloads/OTHER%20THAN%20SAMKIRTHANAS

/Downloads/RESERCH%20BOOKS

/Downloads/SAMKIRTHANAS

/Downloads/SAMKIRTHANAS/New-SAMKIRTHANAS

/Downloads/SAMKIRTHANAS/Old-SAMKIRTHANAS

/DressCode.aspx

/EDarsanCounters.aspx

/EducationalTrust.aspx

/EkanthaSeva.aspx

/EkkadiMaanushaJanma.aspx

/ElurupaduImages.aspx

/ErrorPage.aspx

/ErukulaPakaluImages.aspx

/EtuvantiMohamo.aspx

/FAQ.aspx

/FAVOURITE%20CARRIER.aspx

/Feedback.aspx

/Festivals.aspx

/FileCS.ashx

/FreeBusServiceAtTirumala.aspx

/FreeBusServiceTirupathi.aspx

/frmAnnaprasadamPreviousData.aspx

/GAJA%20LAKSHMI%20AVATAR.aspx

/GangavaramImages.aspx

/GaraImages.aspx

/GARUDA%20VAHANAM.aspx

/Garudavahanam.aspx

/Golagamudi.aspx

/Governors%20Who%20Had%20Darshan%20Of%20Srivaru.aspx

/GRAND%20BANGARU%20TIRUCHI%20UTSAVAM.aspx

/GumithamthandaImages.aspx

/GuntikadaPalliImages.aspx

/HAMSA%20VAHANAM.aspx

/HANUMAN%20VAHANAM.aspx

/Harikatha.aspx

/Hariyavatara.aspx

/hdpp.aspx

/Hmv.aspx

/Home.aspx

/Howtoreach\_TirupatiandTirumala.aspx

/HYDERABADISBLESS.aspx

/images

/Instrumental.aspx

/IralaImages.aspx

/JayaMangalamu.aspx

/JiyyammaValasaImages.aspx

/joint.aspx

/jquery-1.11.2.min.js

/JupudiBunglowImages.aspx

/KALPAVRUKSHA%20VAHANAM.aspx

/Kalyanam050719.aspx

/Kalyanam060719.aspx

/Kalyanam070719.aspx

/Kalyanam080719.aspx

/Kantulella.aspx

/KAPILESWARA%20SWAMY%20TEMPLE.aspx

/KARTHEEKA%20DEEPOTSAVAM.aspx

/KayyuruImages.aspx

/KeertanasFileCS.ashx

/KodandaramaSwamyTemple.aspx

/KoilAlwarThirumanjanam.aspx

/KomarikaImages.aspx

/KonauppalapaduImages.aspx

/KothapalligudemImages.aspx

/KushalNagarImages.aspx

/LAKSHMI%20HARAM%20SHOBHA.aspx

/LathavaramImages.aspx

/ListenSuprabhatam.aspx

/MaddiralaImages.aspx

/MalavandlapalliImages.aspx

/MANA%20AMARAVATHI%20CAMPAIGN.aspx

/MANA%20MATTI%20AND%20MANA%20NEERU.aspx

/MantralayamImages.aspx

/ManujudaiPutti.aspx

/marriagehallcotteges.aspx

/MatlampattiImages.aspx

/MedicalFacilities.aspx

/MOHINI%20VAHANAM.aspx

/MoreLinks.aspx

/MorePages\_DEL.aspx

/MorePagesNEW.aspx

/MoreTemples.aspx

/music

/music.aspx

/music/bhavamu.rm

/music/khsheerabdhi.rm

/music/srimanna.rm

/music/tiruveedhi.rm

/Musicacl\_books.aspx

/MusicandBooks.aspx

/MuthukurImages.aspx

/MUTYAPU%20PANDIRI%20VAHANAM.aspx

/NadellavaripalemImages.aspx

/NandigamaImages.aspx

/NatureAlbumImages.aspx

/NAVAHNIKA%20KARTHIKA%20BRAHMOTSAVAMS.aspx

/NavaNaarasimha.aspx

/New%20Photo%20Gallery.aspx

/New.aspx

/NewImages

/newsankeertanas.aspx

/NigamaNigamantha.aspx

/Old%20-%20CM.aspx

/oldsankeertanas.aspx

/other\_composition.aspx

/others.aspx

/OtherSankeertans.aspx

/OthersUnique.aspx

/Pacha%20Beralu.aspx

/Package\_Tours.aspx

/PackageTours.aspx

/PadmavathiParinayam.aspx

/PalasadeeviImages.aspx

/PalavenkatapuramImages.aspx

/pallaprolluImages.aspx

/PANCHAMI%20THEERTHAM.aspx

/Parishkartha.aspx

/PastTenders.aspx

/PatAtThiruchanoorSevas.aspx

/PatAtThiruchanoorTempleLegend.aspx

/PATBranmhotsvams.aspx

/PathikondaImages.aspx

/Pavithrotsavam.aspx

/PEARLY%20CARRIER%20REJUVINATES.aspx

/PEDDA%20SESHA%20VAHANAM.aspx

/PeddaguaravaluruImages.aspx

/PedduruImages.aspx

/PentapaduImages.aspx

/PhotoGallery1.aspx

/PiligrimsAlbumImages.aspx

/Places%20to%20see%20around%20Tirumala.aspx

/PlacesatTirupati.aspx

/PM%20SRI%20NARENDRA%20MODI%20VISIT.aspx

/PoolangiSeva.aspx

/PothanapalliImages.aspx

/PravachanamsandChantings.aspx

/Presidents%20Who%20Had%20Darshan%20Of%20Sri%20Varu.aspx

/Prime%20Ministers%20Who%20Had%20Darshan%20Of%20Srivaru.aspx

/Privileges.aspx

/PROTECTIONOFGOMATA.aspx

/PUSHPAKA%20VIMANAM.aspx

/PushpaPallaki.aspx

/PUSHPAYAGAM%20PERFORMED%202015.aspx

/PushpaYagam.aspx

/PuttaparthiImages.aspx

/PuttipaduImages.aspx

/RAAlwarDivyaPrabandhaProject.aspx

/RAAnnamacharyaProject.aspx

/RADasaSahityaProject.aspx

/RailwayBookingOffice.aspx

/RajampetaImages.aspx

/Ramanujam\_Keertanas\_Sravanam.aspx

/Ramanujam\_Pasuralu\_Sravanam.aspx

/RamanujamKeertanasFileCS.ashx

/RamanujamWebpage.aspx

/RASrimanVeturiPrabhakaraSastryVangmayaPeetam.aspx

/RATarigondaVengamambaProject.aspx

/RAVedaRecordingProject.aspx

/RAVenkateswaraRecordingProject.aspx

/RecordingProject.aspx

/ReligiousActivities.aspx

/REPUBLICDAY.aspx

/Research\_books.aspx

/RestHousesInTirumala.aspx

/ReturnJourneyFromTirumala.aspx

/S.V.%20Museum.aspx

/S.V.VaibhavotsavamsImages.aspx

/S\_Kalyanam020819.aspx

/S\_Kalyanam030819.aspx

/S\_Kalyanam040819.aspx

/S\_Kalyanam050819.aspx

/S\_Kalyanam060819.aspx

/S\_Kalyanam070819.aspx

/S\_Kalyanam080819.aspx

/S\_Kalyanam160819.aspx

/S\_Kalyanam170819.aspx

/S\_Kalyanam180819.aspx

/S\_Kalyanam190819.aspx

/SABIRRD.aspx

/SACentralLibraryResearchCenter.aspx

/SAHarithaProject.aspx

/SahasraKalasabhishekam.aspx

/SankeerthaLakshnalu.aspx

/SAPublications.aspx

/Saranagathi\_Gadhyam.aspx

/SaranagathiGadhyamFileCS.ashx

/Sarangapani.aspx

/SARVABHOOPALA%20VAHANAM.aspx

/Sarvadarshanam.aspx

/SARVAJAGDRAKSHAKI%20TAKES%20SARVABHOOPALA%20VAHANAM.aspx

/SaSkVBugga.aspx

/SAVenkateswaraBalaMandir.aspx

/SAVenkateswaraPoorHome.aspx

/SAVenkateswaraSchoolDeaf.aspx

/SAVenkateswaraTrainingCentreforHandicapped.aspx

/scheme\_venkateswaraheritagepreservationtrust.aspx

/Script.js

/ScriptResource.axd

/scripts

/scripts/jquery-1.11.1.min.js

/scripts/typeintelugu.min.js

/Scrolltotop

/Scrolltotop/jquery-scrollToTop.js

/search\_result.aspx

/Sevas.aspx

/SEVEN%20TYPES%20OF%20GARLANDS.aspx

/SEVEN-HOODED%20SERPENT%20VEHICLE.aspx

/SGT.aspx

/SIMHA%20VAHANAM.aspx

/SitaramapuramImages.aspx

/Sitemap.aspx

/Skt.aspx

/Sliding

/Sliding/jquery-2.1.1.min.js

/Sliding/jquery.easing.1.3.js

/Sliding/jquery.skitter.min.js

/SNAPANA%20TIRUMANJANAM.aspx

/SobhanameSobhaname.aspx

/SocialActivities.aspx

/SocialServices.aspx

/somedharmicprograms.aspx

/spattiruchanuru.aspx

/Special%20Illuminations.aspx

/SpecialDarshanForPhysicallyDisabledAndAged.aspx

/SpecialEntryDarshan.aspx

/SPREADDHARMAPRACHARA.aspx

/SriBalajiArogryavaraprasadiniScheme.aspx

/SrikakulamImages.aspx

/SrikurmamImages.aspx

/Srinivasa\_Kalyanam030619.aspx

/Srinivasa\_Kalyanam040619.aspx

/Srinivasa\_Kalyanam050619.aspx

/Srinivasa\_Kalyanam110219.aspx

/Srinivasa\_Kalyanam240119.aspx

/SrinivasaKalyanam.aspx

/SrinivasaKalyanam121218.aspx

/SrinivasaKalyanam131218.aspx

/SrinivasaKalyanam141218.aspx

/SrinivasaKalyanamImages.aspx

/SriPadmavathiGuestHouse.aspx

/SriSrinivasaSanakaraNethralayaTrust.aspx

/SriVenkateshwaraBalaMandirTrust.aspx

/srivenkateshwararecordingproject.aspx

/SRIVENKATESWARAANNAPRASADAMTRUST.aspx

/SriVenkateswaraGosamrakshanaTrust.aspx

/SriVenkateswaraGuestHouse.aspx

/SriVenkateswaraPranadanaTrust.aspx

/SRIVENKATESWARAVEDAPARIRAKSHANATRUST.aspx

/SriVenkateswaraVidyadana.aspx

/srk1.aspx

/srk10.aspx

/srk11.aspx

/srk12.aspx

/srk13.aspx

/srk14.aspx

/srk15.aspx

/srk16.aspx

/srk17.aspx

/srk2.aspx

/srk3.aspx

/srk4.aspx

/srk5.aspx

/srk6.aspx

/srk7.aspx

/srk8.aspx

/srk9.aspx

/Sudharshanaragada.aspx

/SUN%20CARRIER.aspx

/SunkesalaImages.aspx

/Suprabhatam.aspx

/SurveyForm.aspx

/SURYAPRABHA%20VAHANAM.aspx

/Sv\_Amaravathi.aspx

/SVETA.aspx

/SVISTA.aspx

/SVphoto\_gallery.aspx

/SWARNA%20RATHAM.aspx

/TakellapaduImages.aspx

/TalagadadeeviImages.aspx

/TalapakaPatakuPadhasahityam.aspx

/TellaguntaImages.aspx

/TempleAlbumImages.aspx

/TempleLegend.aspx

/TemplesAtTiruchanoor.aspx

/TemplesAtTirupathi.aspx

/TenderDepartmentDetails.aspx

/Teppotsavam.aspx

/Thadakaluru%20.aspx

/Tharigonda.aspx

/THEMATIC%20FLORAL%20DIORAMAS.aspx

/ThomalaSeva.aspx

/TirumalaMap.aspx

/TirumalaORGService.asmx

/TirumalaORGService.asmx/

/TirumalaORGService.asmx/getAllAddress

/TirumalaORGService.asmx/jsdebug

/TirumalatoTirupathiOnFoot.aspx

/TirupatitoTirumalaByRoad.aspx

/TiruppavadaSeva.aspx

/ToReachTirupati.aspx

/tpsattiruchanuru.aspx

/TraditionalBajans.aspx

/TravellingfromTirupatitoTirumala.aspx

/TsunduruImages.aspx

/TTD%20Trust%20Board.aspx

/TTDBoard.aspx

/TTDBoardResolutions.aspx

/ttdklmps.aspx

/TTDs\_Publications.aspx

/TTDTempleHistory.aspx

/UdayagiriImages.aspx

/UniqueAlbum.aspx

/UniqueAlbumImages.aspx

/UrlaobanapalliImages.aspx

/Uyyalawada.aspx

/VairagyaVachanamulu.aspx

/VamidiparthiImages.aspx

/Varaha\_TempleLegend.aspx

/VarahaswamiGuestHouse.aspx

/Vasanthotsavam.aspx

/VavilruImages.aspx

/VenkatapuramImages.aspx

/Videocassettes.aspx

/ViseshaPuja.aspx

/voluntaryservices.aspx

/WebResource.axd

/WeeklySevas.aspx

/YalamarruImages.aspx

/YallavathulaImages.aspx

/YemokoChigurutadharamuna.aspx

## Limitations

1. The report has been prepared based on the information given by TTD and is accordingly, given for the specific purpose of internal use by the TTD. Our conclusions are based on the completeness and accuracy of the stated facts and assumptions; which if not entirely complete or accurate, should be communicated to us immediately, as the inaccuracy or incompleteness could have a material impact on our conclusions.
2. This report has been prepared solely for TTD, being the express addressee to this document. TTD does not accept or assume any liability, responsibility or duty of care for any use of or reliance on this report by anyone, other than (i) TTD, to the extent agreed in the relevant contract for the matter to which this report relates (if any), or (ii) as expressly agreed by TTD in writing in advance.
3. Without prior permission of TTD, the contents of this report may not be quoted in whole or in part or otherwise referred to in any documents. The report is for the sole information of TTD and APTS accepts no responsibility to any other party.
4. This report (and any extract from it) may not be copied, paraphrased, reproduced, or distributed in any manner or form, whether by photocopying, electronically, by internet, within another document or otherwise, without the prior written permission of TTD. Further, any quotation, citation or attribution of this report, or any extract from it, is strictly prohibited without TTD’s prior written permission.
5. This report makes recommendations based on the initial information. However, corrective action must be taken by the respective owners by performing a root cause analysis for each of the observations highlighted as part of this report.