Application Security Assessment Report

Of

APCCE

Department Of Higher Education,

Govt. of AP

17/10/2019

by

Andhra Pradesh Technology Services

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

Vijayawada – 520 010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc22228335)

[1.1. Introduction 3](#_Toc22228336)

[1.2. Engagement Specific Details 3](#_Toc22228337)

[1.3. Scope Details 3](#_Toc22228338)

[1.3.1. Inclusion 3](#_Toc22228339)

[1.3.2. Exclusion 4](#_Toc22228340)

[1.4. Approach & Methodology 4](#_Toc22228341)

[1.4.1. Information Gathering: 4](#_Toc22228342)

[1.4.2. Automated & Manual Scanning: 4](#_Toc22228343)

[1.4.3. Analyse results and reporting: 4](#_Toc22228344)

[1.5. Risk Categorization 5](#_Toc22228345)

[1.6. Vulnerability Summary 6](#_Toc22228346)

[1.6.1. Distribution of Observation 6](#_Toc22228347)

[2. Detailed Observation 7](#_Toc22228348)

[2.1. Web Application Security Assessment & Penetration Testing 7](#_Toc22228349)

[3. Scanned Items 20](#_Toc22228350)

[4. Limitations 35](#_Toc22228351)

1. Executive Summary

## Introduction

In the year 1969 the State Government had introduced 10+2+3 systems of education and started number of Junior Colleges in the State to impart Intermediate Education. The number of these colleges increased immensely after formation of Directorate of Higher Education on 30.06.1975. Consequently, the administrative responsibilities of Director of Higher Education have enormously increased and the centralized management of all the colleges from the State capital had become very difficult. Thus the need was felt to decentralize the organization which has resulted in the creation of three regional offices in the State to oversee the functioning of colleges in the respective regions in the year 1981.

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Application Security Assessment of APCCE Application for APCCE 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. 11/10/2019 |
| 1. 2. | 1. Submission date of initial report | 1. 17/10/2019 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | 1. APTS TEAM | 1. Name | 1. Department of Higher Education |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 17/10/2019 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

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

Application Name: APCCE

Application URL: http://www.apcce.gov.in/

Environment: Production

Version Number [or] Latest Compilation Timestamp: Not Provided

Type of Review: Black box

Hash of Zipped Source Code (SHA512): Not Provided

### Exclusion

1. Server Vulnerability Assessment
2. Secure Code Review
3. Process Review
4. 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 a black-box automated & Manual scanning (without the knowledge of user credentials) 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 | 1 | 4 |
| **Total** |  | | 7 |

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Sql Injection** | **Risk Rating**: High |
| **Description** | SQL Injection is an attack technique used to exploit applications that construct SQL statements from user supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database. | |
| **Affected Path(s)** | http://www.apcce.gov.in/tisslogin.aspx  http://www.apcce.gov.in/JKC/mentorbudgetlogin.aspx | |
| **Impact** | A wide range of damaging attacks can be delivered via SQL injection, including reading or modifying critical application data, interfering with application logic, escalating privileges within the database and taking control of the database server. | |
| **Evidence/Proof of Concept**  **Step 1:** Access the URL and enter the SQL payloads in username and password fields as shown below.  sqlinjection1.png  **Step 2:** After successful attack the database names are retrieved as shown in image.  sqlinjection3.png | | |
| **Recommendation** | This is a critical vulnerability to have on a web application and should be addressed immediately. User controllable data should be validated before any queries are performed on the database using the data. Blacklisting is an approach which consists of checking the input data for malicious characters but a more effective approach is white listing. White listing consists of only allowing certain characters to be submitted. For example checking if data submitted is alphanumeric and rejecting the request if it is not. Many libraries exist, such as built-in libraries for programming languages and open-source libraries, which can assist you in preventing this vulnerability. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Improper Error Handling** | **Risk Rating**: Medium |
| **Description** | The application responds with stack traces that are not managed which could reveal information useful to attackers. Providing debugging information as a result of operations that generate errors is considered a bad practice due to multiple reasons. For example, it may contain information on internal workings of the application such as relative paths of the point where the application is installed or how objects are referenced internally. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** | An attacker can obtain information such as: • ASP.NET version. • Physical file path of temporary ASP.NET files. • Information about the generated exception and possibly source code, SQL queries, etc. This information might help an attacker gain more information and potentially focus on the development of further attacks for the target system | |
| **Evidence/Proof of Concept**  stack trace error.png  Fig. Stack trace enabled | | |
| **Recommendation** | It is recommended to implement a custom error page and display it to end user. | |
| **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)** | http://www.apcce.gov.in/tisslogin.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.  insufficent anti automation.png | | |
| **Recommendation** | It is recommended to implement captcha on login page. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Email Id Disclosure** | **Risk Rating**: Low |
| **Description** | During assessment, we found that a lot of email ids in the contact us page which is not a good practice suggested by the OWASP community. The mail ids displayed here are not any generic ones (ex: helpdesk@gmail.com) rather they belong to the respective individuals based on their designation. 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)** | http://www.apcce.gov.in/jkccontact.aspx  http://www.apcce.gov.in/newwebsite30122010/Contactus.aspx | |
| **Impact** | Disclosing the individual mail ids sometimes lead to social engineering attacks and often affected with the spam mails. However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login. | |
| **Evidence/Proof of Concept**  email id disclosure.png  Fig. Email Address disclosure | | |
| **Recommendation** | Obfuscate email address by replacing @ with [at] and . with [dot]. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Unencrypted View State** | **Risk Rating**: Low |
| **Description** | The \_\_VIEWSTATE parameter is not encrypted. To reduce the chance of someone intercepting the information stored in the ViewState, it is good design to encrypt the ViewState. To do this, set the machineKey validation type to AES. This instructs ASP.NET to encrypt the ViewState value using the Advanced Encryption Standard. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** | Possible sensitive information disclosure. | |
| **Evidence/Proof of Concept**  viewstate.png  Fig. Unencrypted View State | | |
| **Recommendation** | 1. Open Web.Config and add the following line under the <system.web> element:   <machineKey validation="AES"/> | |
| **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** | Sites can use X-Frame-Options to avoid click jacking attacks, by ensuring that their content is not embedded into other sites.  It is recommended to perform the following: ? Use the X-FRAME Options in response header set to DENY or Same Origin or ALLOW-FROM a specified URL ? X-Frame-Options: This header works with modern browsers and can be used to prevent framing of the page. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Technology/version Disclosure** | **Risk Rating**: Low |
| **Description** | The HTTP responses returned by this web application include a header named X-AspNet-Version. The value of this header is used by Visual Studio to determine which version of ASP.NET is in use. It is not necessary for production sites and should be disabled. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** | The HTTP header may disclose sensitive information. This information can be used to launch further attacks. | |
| **Evidence/Proof of Concept**  **Step 1:** Application discloses the server and application framework version details in response headers.  version disclosure.png | | |
| **Recommendation** | Apply the following changes to the web.config file to prevent ASP.NET version disclosure: <System.Web><httpRuntime enableVersionHeader="false" /></System.Web> | |
| **Management Comments** |  | |

## Scanned Items

/

/1035235

/2012-13\_CollegeDetails

/2012-13\_CollegeDetails/jkc\_budget\_details/Budget.aspx

/2013\_jkcregistrations

/2013\_jkcregistrations/jkcstudentregloginbi.aspx

/2013\_jkcregistrations/jkcstudentregloginbii.aspx

/2013\_jkcregistrations/jkcstudentreglogint.aspx

/2013\_JLPromotions

/2013\_transfers

/2013\_transfers/Vacancy\_pos.aspx

/7thPRC.aspx

/aboutus.aspx

/airjkc.aspx

/anacollegesabstract.aspx

/anacollegeslist.aspx

/anaworkload.aspx

/anaworkloadfront.aspx

/AntiRagging

/AntiRagging/Default.aspx

/AntiRagging/js

/API

/APPSCProc

/Articals

/Aut\_Transfers.aspx

/Auto\_trans.aspx

/bulats2013.aspx

/bulatsactionplan2.aspx

/business

/capacity.aspx

/ccecircularnew3.aspx

/ccephotogallery.aspx

/ccephotogallery2.aspx

/ccephotogallery4.aspx

/ccephotogallerymenu.aspx

/ccephotogalllery3.aspx

/cceproceedings.aspx

/cceproceedings1.aspx

/CIPS

/cipsevl.aspx

/circularitm10.aspx

/circularitm19.aspx

/circularitm2.aspx

/circularitm21\_1.aspx

/circularitm22.aspx

/circularitm23.aspx

/circularitm4.aspx

/circularitm6.aspx

/circularitm9.aspx

/Circulars

/cityjfdrreddysphotos.aspx

/clockh.js

/clockp.js

/COE

/coe.aspx

/COE/slider.html

/COE/sliderengine

/COE/sliderengine/amazingslider.js

/COE/sliderengine/initslider-1.js

/COE/sliderengine/jquery.js

/collegewebsites.aspx

/contentmag.aspx

/coordinatorslist.aspx

/courses2.aspx

/culture

/default.aspx

/digitallibrary.aspx

/doc

/doc/Gos

/doc/job fairs

/Documentation

/Documentation/2014-2015

/Documentation/April2013

/Documentation/April2014

/Documentation/April2015

/Documentation/April2018

/Documentation/Aug2013

/Documentation/Aug2015

/Documentation/August2014

/Documentation/Dec2015

/Documentation/December2013

/Documentation/DR2012

/Documentation/Feb2013

/Documentation/Feb2015

/Documentation/Jan2013

/Documentation/Jan2015

/Documentation/Jan2016

/Documentation/July2013

/Documentation/July2014

/Documentation/July2015

/Documentation/july2016

/Documentation/June2013

/Documentation/June2015

/Documentation/June2016

/Documentation/Mar2013

/Documentation/March2015

/Documentation/March2018

/Documentation/MAY2013

/Documentation/May2014

/Documentation/Nov2015

/Documentation/November

/Documentation/October2015

/Documentation/Seminars

/Documentation/Sep2015

/Documentation/Sept2014

/Documentation/Sept2014/Transfers

/Documentation/September2013

/Documentation/transferproc2012

/Documentation/ugc

/Dr2012.aspx

/ebcmatter.aspx

/elearningnew.aspx

/ELF

/elf2014.aspx

/ell.aspx

/ELL201516

/ELL201516/ell24abstract.aspx

/ELL201516/ell316abstract.aspx

/ELL201516/ell3abstract.aspx

/ELL201516/ell42abstract.aspx

/ELL201516/ellnote.aspx

/ELL201516/ellproducts.aspx

/ELL201516/js

/entertainment

/environment

/eresdesirstruct.aspx

/eresejourn.aspx

/eresinflilist.aspx

/eresintro.aspx

/ereslib.aspx

/Evoluations

/Excel

/fadeslideshow.js

/feedback

/feedbackform.aspx

/feedbackformmain.aspx

/feedbackforms.aspx

/feedbackformsfirst.aspx

/feedbackprint.aspx

/filesinccefrom1.2.11

/formnew.aspx

/fortnitephotogallery.aspx

/fortniteregionalwisewinners.aspx

/forum.aspx

/freshcontractlect2011-12.aspx

/genpact.html

/GORPS.aspx

/Gos

/guntur.html

/health

/home

/hyderabad1.html

/infosys2009guidelines.aspx

/infosyspress21may.aspx

/infosysprojectgenesis.aspx

/infosysselectedstudent.aspx

/infrastructure

/infrastructure/infralogin.aspx

/infrastructure/js

/ingvysyaongole.aspx

/introductioncontinue.aspx

/ipg2009.aspx

/ipg2009a.aspx

/JDGDCNaidupet.aspx

/JKC

/jkc.aspx

/jkc.htm

/JKC/accordion

/JKC/accordion/jquery.ui.accordion.js

/JKC/accordion/jquery.ui.core.js

/JKC/accordion/jquery.ui.widget.js

/JKC/collegewiseplacements.aspx

/JKC/functions.js

/JKC/functions.js?ver=20140319

/JKC/global.js

/JKC/jobdrives

/JKC/jobdrives/JKCJOBDRIVES2015-2016.aspx

/JKC/jobdrives/js

/JKC/jobdrives/js/commissionerate.js

/JKC/jquery-1.11.0.min.js

/JKC/jquery-migrate.min.js

/JKC/jquery.flexslider.js

/JKC/jquery.js

/JKC/jquery.js?ver=1.11.0

/JKC/light-orange-pin.svg

/JKC/Material

/JKC/mentorbudgetlogin.aspx

/JKC/placements.aspx

/JKC/respond.js

/JKC/scripts-ck.js

/JKC/studentwiseplacement.aspx

/jkc2010monthwisejobfair.aspx

/JKC2015

/JKC2015/ActivityReports

/JKC2015/ActivityReports/EGodavari

/JKC2015/ChiefVisits

/JKC2015/Districtwise2017-18

/JKC2015/JKC

/JKC2015/JKC2015

/JKC2015/JKCActivities.aspx

/JKC2015/JKCDrivereports2015.aspx

/JKC2015/JKCE-Learning.aspx

/JKC2015/JKCJobfair2016-17.aspx

/JKC2015/JKCLabPictures.aspx

/JKC2015/JKCPlacement2017.aspx

/JKC2015/NASSCOM

/JKC2015/Scripts

/JKC2015/Scripts/nanoGALLERY-5.6.0

/JKC2015/Scripts/nanoGALLERY-5.6.0/jquery.nanogallery.js

/JKC2015/Scripts/nanoGALLERY-5.6.0/jquery.nanogallerydemo.js

/JKC2015/skype2015

/jkcaboutusguidelines.aspx

/jkcactionplan.aspx

/jkcactionplan2011to2012

/jkcactionplan2012to2013.aspx

/jkcactionplan2013to2014.aspx

/jkcactionplan2014to2015.aspx

/jkcactivities.aspx

/jkcbooksdistribution.aspx

/jkccips.aspx

/jkccircular8.aspx

/jkccircular9.aspx

/JKCCirculars.aspx

/JKCCirculars2012to2013.aspx

/JKCCirculars2013to2014.aspx

/JKCCirculars2014to2015.aspx

/jkccontact.aspx

/jkccuriculam.aspx

/jkccuriculam201516.aspx

/JKCCurriculam.aspx

/jkcdefault.aspx

/JKCE-Classes.aspx

/jkcforum.aspx

/JKCGallery.aspx

/jkcguidelinescirculars.aspx

/jkchcljfdrivephotos.aspx

/jkcintroduction.aspx

/JKCJobDriveReport.aspx

/JKCJOBDRIVES2012-13.aspx

/JKCJOBDRIVES2013-2014.aspx

/jkcjobfair2014.aspx

/jkcl2013.aspx

/jkcll2013.aspx

/jkcllab.aspx

/jkclogin.aspx

/jkcmc.aspx

/jkcmcell.aspx

/JKCMCPORTAL

/JKCMCPORTAL/AboutJKC.aspx

/JKCMCPORTAL/Default.aspx

/JKCMCPORTAL/Scripts

/JKCMCPORTAL/Scripts/jquery-2.1.1.js

/JKCMCPORTAL/Scripts/jquery-advanced-news-ticker-master

/JKCMCPORTAL/Scripts/smartmenus-0.9.7

/JKCMCPORTAL/Scripts/smartmenus-0.9.7/jquery.smartmenus.js

/JKCMCPORTAL/Scripts/unslider.min.js

/jkcmentorhono.aspx

/jkcmonthwisephotogallery.aspx

/jkcmoutiss.aspx

/JKCOnline

/JKCOnline/capacity.aspx

/JKCOnline/JKCJobDriveReport.aspx

/JKCOnline/jkctimetable.aspx

/JKCOnline/jkplacements2013.aspx

/JKCOnline/jobfair2014.aspx

/JKCOnline/newjkccontact1.aspx

/JKCOnline/newjkcphotogalleryyear1.aspx

/JKCOnline/newjkcpressrelyr1.aspx

/JKCOnline/newjkcservices.aspx

/JKCOnline/Scripts

/JKCOnline/Scripts/jquery-1.11.1.js

/JKCOnline/Scripts/jquery-ui.js

/JKCOnline/skypeactivity.aspx

/JKCOnline/studymaterials.aspx

/JKCOnline/Styles

/JKCOnline/Styles/jquery-ui-themes-1.11.0

/JKCOnline/Styles/jquery-ui-themes-1.11.0/themes

/JKCOnline/~

/JKCOnline/~/Default.aspx

/jkconlinetimetable.aspx

/jkcpaperclipping.aspx

/JKCPlacementAbstract.aspx

/jkcplacements2013-14.aspx

/JKCPlacementStatus

/jkcpressreleases.aspx

/jkcproceedingsofmc.aspx

/jkcpvtaidedunaidedinvitation.aspx

/jkcsactionpla.aspx

/jkcsjobdrivereport.aspx

/jkcskypealbum.aspx

/jkcsplacementabstract.aspx

/jkcstsp.aspx

/jkcstudymaterials.aspx

/jkcteam.aspx

/jkctiss.aspx

/jkctot.aspx

/jkctrainingstatus.aspx

/jkctrainingstatuslogin.aspx

/jkctsp.aspx

/jkcvijayawadajfphotos.aspx

/jkcvizagjfphotos.aspx

/jkplacements2013.aspx

/jobfair.aspx

/jobfair2010anantapur.aspx

/jobfair2010guntur.aspx

/jobfair2010Hyderabad.aspx

/jobfair2010jan.aspx

/jobfair2010vizag.aspx

/jobfair2013.aspx

/jobfair2014.aspx

/jobfair2015.aspx

/jobfaircompanyeslist.aspx

/jobfairphotoanatapur1.aspx

/jobfairphotoshyd1.aspx

/jobfairpressrelease2010.aspx

/jobmelalogin.aspx

/jobplacements.aspx

/js

/js/commissionerate.js

/js/function.js

/js/jquery.js

/kakinadajkclab.aspx

/karimnagar.html

/KM

/KM/2013\_jkcregistrations

/KM/csrsummit.aspx

/KM/elf2015t.aspx

/KM/JKC

/KM/JKC2015

/KM/jkctissbatchI.aspx

/KM/js

/KM/KM

/knowlmang.aspx

/KPI

/KPI/default.aspx

/KPI/js

/KPI/kpilogin.aspx

/KPI/kpireport.aspx

/kurnoolkvr.aspx

/kurnoolsjjkclab.aspx

/labs.aspx

/lastarticles

/learnmang.aspx

/lifestyle

/listofjkc.aspx

/listofvacancieson51209.aspx

/ManaTV

/manatv1new.aspx

/MANATVFeedback

/MANATVFeedback/Default.aspx

/MANATVFeedback/ManatvLiveRecFeed.aspx

/MANATVFeedback/SpecialLive.aspx

/manatvlive.aspx

/manatvnew.aspx

/material.aspx

/mentorprovisionallist.aspx

/Mentors\_Recruitment\_2011

/mentorslist.aspx

/Mentorsselectionlist.aspx

/mentorsshortlistedcandidates.aspx

/mentorwaitinglist.aspx

/mm\_menu.js

/msca2.aspx

/msca2\_1.aspx

/msca2\_3.aspx

/msoffice.aspx

/new.aspx

/newccecontactus.aspx

/newchild1.aspx

/newchild2.aspx

/newchild3.aspx

/newchild4.aspx

/newchild5.aspx

/Newinfra.aspx

/objective.aspx

/orgstruct.aspx

/otherrelatedlinks.aspx

/palakollujkclab.aspx

/PensionProposals

/performance2.aspx

/photogallery.aspx

/photogalleryyear.aspx

/placements.aspx

/placements2009.aspx

/prefarticles

/press1.aspx

/pressa1.aspx

/pressa2.aspx

/pressjobfair2010month.aspx

/pressjobfair2011.aspx

/pressrelease13mayinfosys.aspx

/pressrelease2012.aspx

/pressrelease2013.aspx

/pressrelease2014.aspx

/pressreleaseatvizag.aspx

/pressreleaseinfosyschittoor.aspx

/pressreleasemonthwise.aspx

/pressreleaseyearwise.aspx

/principalslist.aspx

/projectgenesis1.aspx

/projectgenesis2.aspx

/projectgenesis3.aspx

/projectgenesis3a.aspx

/pvtaided.aspx

/rajahjkclab.aspx

/rajahmundry.html

/restructeredcourseorderson23.aspx

/ResultAnalysis-2018-19

/ResultAnalysis-2018-19/ra201819login.aspx

/ResultAnalysis-2018-19/reports.aspx

/reviewmeetings.aspx

/rti2.aspx

/rtiitems.aspx

/Rusa.aspx

/SCBookBank

/SCBookBank/js

/SCBookBank/scbookbank.aspx

/schedulejobfairforae.aspx

/ScriptResource.axd

/Scripts

/Scripts/colorbox-master

/Scripts/colorbox-master/jquery.colorbox.js

/Scripts/Demo.js

/Scripts/jquery-1.4.1.min.js

/Scripts/jquery-ui.js

/SCSP

/SCSP/login.aspx

/search

/Seminar

/seminar2015.aspx

/Skype

/skypeactivity.aspx

/society

/sports

/srikakulamjkclab.aspx

/stakeholders.aspx

/stateawards2019.aspx

/stateteacherawards.aspx

/statistic.aspx

/STBOOKBANK

/STBOOKBANK/js

/STBOOKBANK/st\_beneferies.aspx

/studymaterials.aspx

/TBSS.html

/third.party

/third.party/velocity

/timetableprint.aspx

/TISS

/tisslogin.aspx

/tissreport.aspx

/topics

/topics/Celebrations

/topics/Celebrations/easter

/topics/current

/topics/Movies

/topics/Sports

/transferpostings.aspx

/transfers2009-10.aspx

/transfers2010.aspx

/transfers2015

/transfers2015/alecworking.aspx

/transfers2016

/Transfersppl2011

/Transfersppl2011/webpromotionsforppl.aspx

/transferszones.aspx

/travel

/ugc2006.aspx

/UGC7PRC

/users

/users/top

/veldata

/vgdcwjkclab.aspx

/Videos

/vishakapatnam.html

/vskjkclab.aspx

/WebResource.axd

/whatiselearn.aspx

/whyjkcs.aspx

/wiprorajahmundry.aspx

/workload.aspx

/workload2.aspx

/yuvatarangam.aspx

## Limitations

1. The report has been prepared based on the information given by Department of Higher Education and is accordingly, given for the specific purpose of internal use by the Department of Higher Education. 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 Department of Higher Education, being the express addressee to this document. Department of Higher Education 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) Department of Higher Education, to the extent agreed in the relevant contract for the matter to which this report relates (if any), or (ii) as expressly agreed by Department of Higher Education in writing in advance.
3. Without prior permission of Department of Higher Education, 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 Department of Higher Education 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 Department of Higher Education. Further, any quotation, citation or attribution of this report, or any extract from it, is strictly prohibited without Department of Higher Education’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.