Application Security Assessment Report

Of

Telugu University,

Telugu University, Govt. of AP

Dated 11/09/2019

by

Andhra Pradesh Technology Services Ltd

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

Vijayawada – 520010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc18935487)

[1.1. Introduction 3](#_Toc18935488)

[1.2. Engagement Specific Details 3](#_Toc18935489)

[1.3. Scope Details 3](#_Toc18935490)

[1.3.1. Inclusion 3](#_Toc18935491)

[1.3.2. Exclusion 3](#_Toc18935492)

[1.4. Approach & Methodology 3](#_Toc18935493)

[1.4.1. Information Gathering: 4](#_Toc18935494)

[1.4.2. Automated & Manual Scanning: 4](#_Toc18935495)

[1.4.3. Analyse results and reporting: 4](#_Toc18935496)

[2. Detailed Observation 7](#_Toc18935497)

[2.1. Web Application Security Assessment & Penetration Testing 7](#_Toc18935498)

[3. Scanned Items 10](#_Toc18935499)

[4. Limitations 11](#_Toc18935500)

1. Executive Summary

## Introduction

Reports Application provides the details of the employees from various departments in state. It also provides the details of pending and parked files of each officer of the various departments in state.

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Application Security Assessment of Reports Application for ITE&C 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. 07/09/2019 |
| 1. 2. | 1. Submission date of initial report | 1. 11/09/2019 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 11/09/2019 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

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

Application Name: Telugu University

Application URL: [http://teluguuniversity.ac.in](http://teluguuniversity.ac.in/)

Environment: Staging Server

Version Number [or] Latest Compilation Timestamp: Not provided

Type of Review: Black box

Hash of Zipped Source Code (SHA512): Not Provided

User Accounts Tested:

### 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
   1. **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.

* 1. **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 | 4 |
| **Total** |  |  | **8** |

**Distribution of Observation**

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Word Press Admin Console Available to End user** | **Risk Rating**: High |
| **Description** | The application discloses Word Press admin console to end-user and Word Press doesn’t limit the number of login attempts, so brute force attacks can be very effective. | |
| **Affected Path(s)** | http://aparchmuseums.nic.in/wp-login.php | |
| **Impact** | Brute force attacks can be possible on the login page which may lead to the complete takeover of the website and can also change the design and layout of the website. | |
| **Evidence/Proof of Concept**  **Step1:** By Accessing the URL http://aparchmuseums.nic.in/wp-login.php,the word press login page can be accessed as shown in the image.  Annotation 2019-09-11 115213.png | | |
| **Recommendation** | The best defence against this vulnerability is installing a plug-in that will limit the number of allowed login attempts, such as iThemes Security Pro. You can also use a password manager to generate random passwords that are much less likely to be guessed. Stay away from passwords that seem obvious — don’t use anything like 123456, password, or anything related to you. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Word Press XML-RPC authentication brute force** | **Risk Rating**: Medium |
| **Description** | Word Press provides an XML-RPC interface via the xmlrpc.php script. XML-RPC is remote procedure calling using HTTP as the transport and XML as the encoding. An attacker can abuse this interface to brute force authentication credentials using API calls such as **wp.getUsersBlogs**. | |
| **Affected Path(s)** | http://aparchmuseums.nic.in/xmlrpc.php | |
| **Impact** | By using the xmlrpc file the attacker can perform the attacks like bruteforce attacks and XSPA or simply port scanning etc. | |
| **Evidence/Proof of Concept**  **Step 1:** By accessing the URLhttp://aparchmuseums.nic.in/xmlrpc.php we can access the xmlrpc file  xmlrpc.png | | |
| **Recommendation** | It is possible to disable the XML-RPC script if you do not want to use it. Consult references for a Word Press plug-in that does that. If you don't want to disable XML-RPC you can monitor for XML-RPC authentication failures with a Web Application Firewall like ModSecurity.  Reference link:  https://wordpress.org/plugins/prevent-xmlrpc/  https://isc.sans.edu/diary/+WordPress+brute+force+attack+via+wp.getUsersBlogs/18427 | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **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 URL(s)** | http://teluguuniversity.ac.in/contact/ | |
| **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:** By accessing the URL http://teluguuniversity.ac.in/contact/ it is observed that the captcha is not implemented as shown in image  **insufficent anti automation.png** | | |
| **Recommendation** | It is recommended to implement captcha.  Reference Links:  http://www.captcha.net | |
|  |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Email id Disclosure** | **Risk Rating**: Medium |
| **Description** | During assessment, we found the email ids in web page which is not a good practice suggested by the OWASP community. The spam-bots (also known as email harvesters and email extractors) are programs that source the internet looking for email addresses on any website they come across. Spam bot programs look for strings like myname@mydomain.com and then record any addresses found. | |
| **Affected URL(s)** | http://teluguuniversity.ac.in/contact/ | |
| **Impact** | Disclosing 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**  **Step 1:** E-mail address disclosure in the web application.  email.png | | |
| **Recommendation** | Obfuscate email address or Spell out email addresses(Please enclose the email address with example [at] gmail [dot] com)  Refer:  https://stackoverflow.com/questions/748780/best-way-to-obfuscate-an-e-mail-address-on-a-website  https://stackoverflow.com/questions/11563283/why-write-at-and-dot-in-email-rather-than-and  https://academia.stackexchange.com/questions/55612/why-do-people-in-academia-tend-to-write-their-email-address-with-dot-at  https://stackoverflow.com/questions/483212/effective-method-to-hide-email-from-spam-bots | |
|  |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Technology/Version Disclosure** | **Risk Rating**: Low |
| **Description** | Application discloses version details of server in response headers. | |
| **Affected URL(s)** | /(Web Server) | |
| **Impact** | 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**  **Step 1:** the response is displaying the the server version as shown in image  version disclosure.png | | |
| **Recommendation** | It is recommended to apply changes on your web.config file to prevent information leakage by applying custom error pages.  Remove unwanted HTTP Headers  Reference Link:  https://www.owasp.org/index.php/Fingerprint\_Web\_Server\_(OTG-INFO-002)  https://www.owasp.org/index.php/Fingerprint\_Web\_Application\_Framework\_(OTG-INFO-008)  https://www.owasp.org/index.php/Fingerprint\_Web\_Application\_(OTG-INFO-009) | |
|  |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Outdated Java script Library** | **Risk Rating**: LOW |
| **Description** | The web application is using one or more JavaScript libraries which contain a known vulnerability. Attackers could exploit the vulnerabilities in the JavaScript libraries. The exact ability to exploit and impact depends on the component(s) and usage of the vulnerable libraries by the web application. | |
| **Affected Path(s)** | http://teluguuniversity.ac.in/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 | |
| **Impact** | Attackers could exploit the vulnerable java script libraries and perform further attacks such as XSS,SQLi etc. | |
| **Evidence/Proof of Concept**  **Step 1:** It is observed that theapplication is using the outdated jquery version.  **jquery version.png** | | |
| **Recommendation** | Recommended to upgrade jQuery to latest version.  Reference Links:  https://cwe.mitre.org/data/definitions/16.html  https://blog.jquery.com/2009/02/20/jquery-1-3-2-released/ | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **Click jacking** | **Risk Rating**: Low |
| **Description** | Click jacking can be performed by framing the target site. An attack can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons. Upon executing the html file, we can see the entire website is been framed. | |
| **Affected URL(s)** | [/(Web Server)](http://teluguuniversity.ac.in/) | |
| **Impact** | Tricking the user to click on the link by framing the original page and showing a layer on top of it with dummy buttons which leads to Phishing. | |
| **Evidence/Proof of Concept**  **Step 1:** append the url in the clickjacking iframe test code as shown in the image  **Annotation 2019-09-11 141838.png**  **Step2 :**It is observed that the web site is loaded in the iframe as shown in below image  **clickjacking .png** | | |
| **Recommendation** | The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid Click jacking attacks, by ensuring that their content is not embedded into other sites. Set the X-Frame-Options header for all responses containing HTML content. The possible values are "DENY", "SAMEORIGIN", or "ALLOW-FROM Uri"  Reference Link:  https://www.owasp.org/index.php/Testing\_for\_Clickjacking\_(OTG-CLIENT-009) | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **PHPinfo page found** | **Risk Rating**: Low |
| **Description** | This script is using phpinfo() function. This function outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License. | |
| **Affected URL(s)** | http://teluguuniversity.ac.in/info.php | |
| **Impact** | 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**  **Step 1:** the application is configured to access the php info page by accessing the URL http://teluguuniversity.ac.in/info.php as shown in image:  **Annotation 2019-09-11 122036.png** | | |
| **Recommendation** | Modify the access permission of php info file in the server configuration file  References Links:  https://www.php.net/manual/en/function.phpinfo.php | |
| **Management Comments** |  | |

## Scanned Items

/

/events-2/locations

/info.php

/5343-2/embed

/5343-2

/about-us

/about-us-cde

/about-us/

/academic

/academic-calendar

/academic-calendar/embed

/academic/

/accredited-by-naac/

/administrators

/alumni

/audio-visual-studio

/audio-visual-studio/embed

/auditorium

/auditorium-booking/

/auditorium/embed

/author

/awards-and-purascars/

/awards/awards/

/awards

/awards/un\_awards

/calendar/apr

/calendar/aug

/calendar/jan

/calendar/nov/

/campuses/0/

/campuses/departments/embed

/campuses

/campuses/wings

/campuses/wings/computer-cell

/campuses/wings/computer-cell/embed

/campuses/wings/publications

/central-library

/centre-for-distance-education

/circulars

/circulars-cde

/circulars/

/comparative

/computer-cell

/computer-lab

/computer-lab/embed

/contact

/contact-classes-details-cde

/contact/

/contact/embed

/copy-of-index

/copy-of-index/museum

/course

/course-syllabus

/course/

/courses-offered-by-cde

/cssmenupro

/departments

/directory-2

/distance/

/downloads/

/DTD

/embed

/embed/

/encyclopedia

/events

/events-2

/exam-results

/examination-branch

/extension-service-division

/facilities

/facilities/

/faculty-details

/?attachment\_id=1511

/fine-arts

/fine-arts/

/folklore

/folklore/

/foreign-affiliations

/foreign-affiliations/

/grievance-cell

/grievance-cell/

/guidelines-cde

/guidelines-cde/

/hall-tickets-download-page

/hall-tickets-download-page/

/history/

/hostels/

/hyderabad-campus-old/

/index

/index-2/museum/

/index-3/index-3

/index-4/pages/

/index/

/iqac

/iqac/

/iqac/pstu\_chekback

/iqac/pstu\_chekback/

/itc

fac

/itc/itc

/kuchipudi

/kuchipudi/index-3

/kuchipudi/index-3/pages

/kuchipudi/index-3/pages/dsc\_0753

/language

/language/semi\_lib

/library

/locations

/locations/potti-sreeramulu-telugu-university

/mission

/museum/embed

/music-colleges

/naac-ssr-2018

/naac-ssr-2018/embed

/net-

/net-coaching

/newdownloads

/nss/

/office-gmail

/oldversion

/page-builder

/page-builder/

/pages/aboutus/

/pg-courses-time-table

/pg-courses-time-table/time-table

/previous-question-papers-cde/

/pstu-youtube-channel/

/pstu\_chekback

/publications

/publications-division

/publications-division/embed

/publications/

/publications/publications

/regular-pg-courses-entrance-examination-results

/research

/research-output

/research-output/embed

/research-output/

/research/emeritus

/research/major

/research/major/aboutus.html

/research/major/

/research/research/

/research/women

/robots.txt

/sample-page-2/

/sc-st-cell

/school-of-telugu-literature/

/search/gdl-course

/search/gdl-course/

/search/gdl-course/rss2/

/search/our/

/search/our/page/10

/search/our/page/12/

/search/our/page/15

/search/our/page/16/

/search/our/page/6/

/search/our/page/9

/search/our/page

/search/our/page/rss2

/search/Type%2byour%2bkeywords...

/site-map

/site-map/embed

/staff-login

/staff-login/embed

/statutory-bodies

/student-login

/student-login/book\_auditorium

/student-login/studentlogin

/student-welfare

/students-login

/students-login/book\_auditorium/

/students-login/studentlogin/

/studio-booking/

/telugu-calendar/embed

/telugu-calendar

/telugu-vaani/

/teluguvani/

/teluguvani/telugu\_vaani/

/ugc-cell/

/unique-nature/

/university-administration

/university-administration/embed

/university-at-a-glance

/university-profile

/university-profile/embed

/vc-desk

/vc-desk/embed

/wp-admin

/wp-admin/post.php?post=5205&action=edit

/wp-comments-post.php

/wp-content/

/wp-includes/js/jquery/jquery.js

/wp-includes/js/jquery/ui/draggable.min.js

/wp-json

/wp-json/

/wp-json/oembed

/wp-json/oembed/1.0

/wp-json/oembed/1.0/embed

/wp-login.php

/xmlrpc.php

## Limitations

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