Application Security Assessment Report

Of

Department of

General Administration Department (GAD)

AP CODES

Dated 09/07/2019

By

Andhra Pradesh Technology Services

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

Vijayawada – 520 010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc13581628)

[1.1. Introduction 3](#_Toc13581629)

[1.2. Engagement Specific Details 3](#_Toc13581630)

[1.3. Scope Details 3](#_Toc13581631)

[1.3.1. Inclusion 3](#_Toc13581632)

[1.3.2. Exclusion 3](#_Toc13581633)

[1.4. Approach & Methodology 3](#_Toc13581634)

[1.4.1. Information Gathering 3](#_Toc13581635)

[1.4.2. Automated & Manual Scanning 4](#_Toc13581636)

[1.4.3. Analyse Results & Reporting 4](#_Toc13581637)

[1.5. Risk Categorization 4](#_Toc13581638)

[1.6. Vulnerability Summary 6](#_Toc13581639)

[1.6.1. Distribution of Observation 6](#_Toc13581640)

[2. Detailed Observation 7](#_Toc13581641)

[2.1. Web Application Security Assessment & Penetration Testing 7](#_Toc13581642)

[3. Appendix 25](#_Toc13581643)

[3.1. OWASP Checklist 25](#_Toc13581644)

[3.2. Network Reconnaissance 29](#_Toc13581645)

[4. Scanned Items 29](#_Toc13581646)

[5. Limitations 31](#_Toc13581647)

1. Executive Summary

## Introduction

This is the official portal for General Administration Department of Government of Andhra Pradesh. The Office of the Nodal Authority, General Administration Department manages this site. Though all efforts have been made to ensure the accuracy and currency of the content on this website, the same should not be construed as a statement of law or used for any legal purposes.

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

## Engagement Specific Details

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Activity** | 1. **Date** |
| 1. 1. | 1. Start date of engagement | 1. 08/07/2019 |
| 1. 3. | 1. Submission date of initial report | 1. 09/07/2019 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | APTS TEAM | Praveen Kodi | GAD |

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 09/07/2019 | V1.0 | 1. Application Security Assessment |

## Scope Details

### Inclusion

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

Application Name: AP Codes

Application URL: https://www.codes.ap.gov.in/

Environment: Production Server

Version Number [or] Latest Compilation Timestamp:

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

The web application security assessment was conducted in line with the leading security standards and guidelines for web application security such as OWASP. 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 authenticated/ Black-box 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 & 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** | 2 | 3 | 4 |
| **Total** |  |  | **9** |
|

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **Cross Site Scripting(XSS)** | **Risk Rating**: High |
| **Description** | The application is affected with this vulnerability which occurs at the client side due to the improper input validation supplied by the user. This is a code injection that includes client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. | |
| **Affected Path(s)** | <https://www.codes.ap.gov.in/code/officeinfo.aspx> | |
| **Impact** | An attacker can insert malicious JavaScript code that has access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user. | |
| **Evidence/Proof of Concept**  **Step 1:** Access the URL <https://www.codes.ap.gov.in/code/officeinfo.aspx?Officeid=AGC02G29920> and inject the xss payload in URL.    **Figure:** javascript code is seen resulting in a pop up showing xss vulnerability. | | |
| **Recommendation** | * Every User input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain * User input should be HTML-encoded at any point where it is copied into application responses. All HTML meta characters, including < > " ' and =, should be replaced with the corresponding HTML entities (&lt; &gt; etc). * Refer: https://www.owasp.org/index.php/XSS\_(Cross\_Site\_Scripting)\_Prevention\_Cheat\_Sheet https://www.checkmarx.com/2017/10/09/3-ways-prevent-xss/ | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **Hard-coded Cryptographic keys in source code** | **Risk Rating:** Medium |
| **Description** | Cryptographic keys are found in source code which will be used for data encryption mechanisms such as converting usernames and passwords into encrypted format. | |
| **Affected Path(s)** | https://www.codes.ap.gov.in/Login | |
| **Impact** | The use of hard-coded cryptographic keys significantly increases the possibility that encrypted data may be decrypted. | |
| **Evidence/Proof of Concept**  **Step1:** Go to login page and click on view page source code  **keys.png**  **Step2:** Now under function log(pass) function you can view Cryptographic keys  keys are exposed in client side source  code.png  **Step3:** By using above keys we can recover the encrypted data.  re.png | | |
| **Recommendation** | 1. It is recommended to implement asymmetric key encryption. And do not hardcoded any cryptographic keys. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **Forced Browsing/Broken Access control** | **Risk Rating**: Medium |
| **Description** | The application allows an unauthenticated user to access the pages that should be accessible to the administrator/user/Ad only. This happens due to the improper implementation of access controls set by the application. | |
| **Affected Path(s)** | https://www.codes.ap.gov.in/changepassword  <https://www.codes.ap.gov.in/home> | |
| **Impact** | Attackers acting as users or administrators, or users using privileged functions have the ability of creating, accessing, updating or deleting every record. | |
| **Evidence/Proof of Concept**  **Step1:** Access the URL https://codes.ap.gov.in /home without authentication.    **Figure:** Forced Browsing | | |
| **Recommendation** | Restrict the access of the authorized pages and maintain proper authorization schema with secure session management.  Reference links:  https://www.owasp.org/index.php/Top\_10-2017\_A5-Broken\_Access\_Control | |
| **Management Comments** |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Vulnerability Title** | **Admin Account Credentials Enumerated** | | **Risk Rating**: Medium |
| **Description** | Admin Account Credentials enumerated but the password which was in encrypted form was decrypted by using the key which disclosed in the source page. | | |
| **Affected Path(s)** | https://www.codes.ap.gov.in | | |
| **Impact** | If the attacker able to find the user credentials he can login to the page and do some malicious activity. | | |
| **Evidence/Proof of Concept**    re.png  **Figure:**  User Account credentials enumerated | | | |
| **Recommendation** | | Do not disclose the account credentials and secret key which was disclosed in page source.  Reference links-  https://cwe.mitre.org/data/definitions/319.html | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **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. Spam bot programs look for strings like myname@mydomain.com and then record any addresses found. | |
| **Affected Path(s)** | <https://www.codes.ap.gov.in/code/officeinfo.aspx> | |
| **Impact** | Email addresses of developers and other individuals may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login, and they may be used in social engineering attacks against the organization's personnel. Unnecessary or excessive disclosure of email addresses may also lead to an increase in the volume of spam email receive. | |
| **Evidence/Proof of Concept**  **C:\Users\APTSADMIN\Desktop\Untitled.png**  Figure-12.1: Email id Disclosure. | | |
| **Recommendation** | Please enclose the email address with example [at] gmail [dot] com | |
| **Management**  **Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **Technology/Version Disclosure** | **Risk Rating**: Low |
| **Description** | The HTTP responses returned by this web application include a header named Server reveals Microsoft version. This information is ignored by most people, with the exception of hackers, who use this information to launch targeted attacks against your web server and version. It is not necessary for production sites and should be disabled. | |
| 1. **Affected Path(s)** | https://www.codes.ap.gov.in | |
| 1. **Impact** | The HTTP header may disclose sensitive information. This information can be used to launch further attacks. | |
| **Evidence/Proof of Concept**  **Step1:** Below response header revealing the server banner and technology information.     1. **Figure :** POC for Microsoft version Detected | | |
| **Recommendation** | Remove these headers from the response messages by editing the web server configuration file and make sure that the technology /version number being used is not disclosed in any manner.  Reference Links:  https://www.saotn.org/remove-iis-server-version-http-response-header/ | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **Insufficient Anti-Automation** | **Risk Rating**: Low |
| **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://www.codes.ap.gov.in/login>  https://www.codes.ap.gov.in/feedback | |
| **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 is not implemented on login page and on feedback form.    **feed.png** | | |
| **Recommendation** | It is recommended to implement captcha.  http://www.captcha.net | |
| **Management Comment** |  | |

|  |  |  |
| --- | --- | --- |
| **9. Vulnerability Title** | **Vulnerable Javascript library** | **Risk rating:** Low |
| **Description** | The application is using multiple vulnerable Javascript libraries that have the known public exploits. Using these libraries may affect the application’s overall security. | |
| **Affected Path(s)** | 1. https://www.codes.ap.gov.in /headsofdepartmentsoffice | |
| **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 affecting the end users. | |
| **Evidence/Proof of Concept** | | |
| **Recommendation** | Upgrade to the latest version of the JQuery libraries 3.0 or higher. | |
| **Management Comments** |  | |

1. Appendix

## OWASP Checklist

The Application Security Assessment has been evaluated as per Open Web Application Security Project Testing guide v4.0 as follows:

| **Ref. No.** | **Category** | **Test Name** | **Safe?** | **Remarks** |
| --- | --- | --- | --- | --- |
| 1.1 | **Information Gathering** | | | |
| 1.1.1 | OTG-INFO-001 | Conduct Search Engine Discovery and Reconnaissance for Information Leakage | Yes | Tested, Not vulnerable |
| 1.1.2 | OTG-INFO-002 | Fingerprint Web Server | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.1.3 | OTG-INFO-003 | Review Webserver Metafiles for Information Leakage | Yes | Tested, Not vulnerable |
| 1.1.4 | OTG-INFO-004 | Enumerate Applications on Webserver | Yes | Tested, Not vulnerable |
| 1.1.5 | OTG-INFO-005 | Review Webpage Comments and Metadata for Information Leakage | Yes | Tested, Not vulnerable |
| 1.1.6 | OTG-INFO-006 | Identify application entry points | Yes | Tested, Not vulnerable |
| 1.1.7 | OTG-INFO-007 | Map execution paths through application | NA | Not Applicable |
| 1.1.8 | OTG-INFO-008 | Fingerprint Web Application Framework | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.1.9 | OTG-INFO-009 | Fingerprint Web Application | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.1.10 | OTG-INFO-010 | Map Application Architecture | NA | Not Applicable |
| 1.2 | **Configuration and Deploy Management Testing** | | | |
| 1.2.1 | OTG-CONFIG-001 | Test Network/Infrastructure Configuration | NA | Not Applicable |
| 1.2.2 | OTG-CONFIG-002 | Test Application Platform Configuration | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.2.3 | OTG-CONFIG-003 | Test File Extensions Handling for Sensitive Information | Yes | No information found |
| 1.2.4 | OTG-CONFIG-004 | Backup and Unreferenced Files for Sensitive Information | Yes | Tested, Not vulnerable |
| 1.2.5 | OTG-CONFIG-005 | Enumerate Infrastructure and Application Admin Interfaces | NA | Not Applicable |
| 1.2.6 | OTG-CONFIG-006 | Test HTTP Methods | Yes | Tested, Not vulnerable |
| 1.2.7 | OTG-CONFIG-007 | Test HTTP Strict Transport Security | Yes | Tested, Not vulnerable |
| 1.2.8 | OTG-CONFIG-008 | Test RIA cross domain policy | NA | Not Applicable |
| 1.3 | **Identity Management Testing** | | | |
| 1.3.1 | OTG-IDENT-001 | Test Role Definitions | NA | Not Applicable |
| 1.3.2 | OTG-IDENT-002 | Test User Registration Process | NA | Not Applicable |
| 1.3.3 | OTG-IDENT-003 | Test Account Provisioning Process | NA | Not Applicable |
| 1.3.4 | OTG-IDENT-004 | Testing for Account Enumeration and DefaultUser Account | Yes | Tested unsafe refer  vulnerability in 2.1 |
| 1.3.5 | OTG-IDENT-005 | Testing for Weak or unenforced username policy | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.3.6 | OTG-IDENT-006 | Test Permissions of Guest/Training Accounts | NA | Not Applicable |
| 1.3.7 | OTG-IDENT-007 | Test Account Suspension/Resumption Process | NA | Not Applicable |
| 1.4 | **Authentication Testing** | | | |
| 1.4.1 | OTG-AUTHN-001 | Testing for Credentials Transported over an Encrypted Channel | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.4.2 | OTG-AUTHN-002 | Testing for default credentials | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.4.3 | OTG-AUTHN-003 | Testing for Weak lock out mechanism | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.4.4 | OTG-AUTHN-004 | Testing for bypassing authentication schema | Yes | Tested, Not vulnerable |
| 1.4.5 | OTG-AUTHN-005 | Test remember password functionality | NA | Not Applicable |
| 1.4.6 | OTG-AUTHN-006 | Testing for Browser cache weakness | Yes | Tested, Not vulnerable |
| 1.4.7 | OTG-AUTHN-007 | Testing for Weak password policy | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.4.8 | OTG-AUTHN-008 | Testing for Weak security question/answer | NA | Not Applicable |
| 1.4.9 | OTG-AUTHN-009 | Testing for weak password change or reset functionalities | NA | Not Applicable |
| 1.4.10 | OTG-AUTHN-010 | Testing for Weaker authentication in alternative channel | NA | Not Applicable |
| 1.5 | **Authorization Testing** | | | |
| 1.5.1 | OTG-AUTHZ-001 | Testing Directory traversal/file include | Yes | Tested, Not vulnerable |
| 1.5.2 | OTG-AUTHZ-002 | Testing for bypassing authorization schema | Yes | Tested unsafe refer  vulnerability in 2.1 |
| 1.5.3 | OTG-AUTHZ-003 | Testing for Privilege Escalation | NA | Not applicable |
| 1.5.4 | OTG-AUTHZ-004 | Testing for Insecure Direct Object References | Yes | Tested, Not vulnerable |
| 1.6 | **Session Management Testing** | | | |
| 1.6.1 | OTG-SESS-001 | Testing for Bypassing Session Management Schema | Yes | Tested, Not vulnerable |
| 1.6.2 | OTG-SESS-002 | Testing for Cookies attributes | NA | Not applicable |
| 1.6.3 | OTG-SESS-003 | Testing for Session Fixation | NA | Not applicable |
| 1.6.4 | OTG-SESS-004 | Testing for Exposed Session Variables | NA | Not applicable |
| 1.6.5 | OTG-SESS-005 | Testing for Cross Site Request Forgery | NA | Not applicable |
| 1.6.6 | OTG-SESS-006 | Testing for logout functionality | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.6.7 | OTG-SESS-007 | Test Session Timeout | NA | Not applicable |
| 1.6.8 | OTG-SESS-008 | Testing for Session puzzling | NA | Not Applicable |
| 1.7 | **Data Validation Testing** | | | |
| 1.7.1 | OTG-INPVAL-001 | Testing for Reflected Cross Site Scripting | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.7.2 | OTG-INPVAL-002 | Testing for Stored Cross Site Scripting | Yes | Tested, Not vulnerable |
| 1.7.3 | OTG-INPVAL-003 | Testing for HTTP Verb Tampering | Yes | Tested, Not vulnerable |
| 1.7.4 | OTG-INPVAL-004 | Testing for HTTP Parameter pollution | Yes | Tested, Not vulnerable |
| 1.7.5 | OTG-INPVAL-005 | Testing for SQL Injection | Yes | Tested, Not vulnerable |
| 1.7.5.1 |  | Oracle Testing | NA | Not Applicable |
| 1.7.5.2 |  | MySQL Testing | NA | Not Applicable |
| 1.7.5.3 |  | SQL Server Testing | NA | Not Applicable |
| 1.7.5.4 |  | Testing PostgreSQL | NA | Not Applicable |
| 1.7.5.5 |  | MS Access Testing | NA | Not Applicable |
| 1.7.5.6 |  | Testing for NoSQL injection | NA | Not Applicable |
| 1.7.6 | OTG-INPVAL-006 | Testing for LDAP Injection | NA | Not Applicable |
| 1.7.7 | OTG-INPVAL-007 | Testing for ORM Injection | NA | Not Applicable |
| 1.7.8 | OTG-INPVAL-008 | Testing for XML Injection | NA | Not Applicable |
| 1.7.9 | OTG-INPVAL-009 | Testing for SSI Injection | NA | Not Applicable |
| 1.7.10 | OTG-INPVAL-010 | Testing for XPath Injection | NA | Not Applicable |
| 1.7.11 | OTG-INPVAL-011 | IMAP/SMTP Injection | NA | Not Applicable |
| 1.7.12 | OTG-INPVAL-012 | Testing for Code Injection | Yes | Tested, Not vulnerable |
| 1.7.12.1 |  | Testing for Local File Inclusion | NA | Not Applicable |
| 1.7.12.2 |  | Testing for Remote File Inclusion | NA | Not Applicable |
| 1.7.13 | OTG-INPVAL-013 | Testing for Command Injection | Yes | Tested, Not vulnerable |
| 1.7.14 | OTG-INPVAL-014 | Testing for Buffer overflow | NA | Not Applicable |
| 1.7.14.1 |  | Testing for Heap overflow | NA | Not Applicable |
| 1.7.14.2 |  | Testing for Stack overflow | NA | Not Applicable |
| 1.7.14.3 |  | Testing for Format string | NA | Not Applicable |
| 1.7.15 | OTG-INPVAL-015 | Testing for incubated vulnerabilities | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.7.16 | OTG-INPVAL-016 | Testing for HTTP Splitting/Smuggling | Yes | Tested, Not vulnerable |
| 1.8 | **Error Handling** | | | |
| 1.8.1 | OTG-ERR-001 | Analysis of Error Codes | Yes | Tested, Not vulnerable |
| 1.8.2 | OTG-ERR-002 | Analysis of Stack Traces | NA | Not Applicable |
| 1.9 | **Cryptography** | | | |
| 1.9.1 | OTG-CRYPST-001 | Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection | NA | Not Applicable |
| 1.9.2 | OTG-CRYPST-002 | Testing for Padding Oracle | NA | Not Applicable |
| 1.9.3 | OTG-CRYPST-003 | Testing for Sensitive information sent via unencrypted channels | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.1 | **Business Logic Testing** | | | |
| 1.10.1 | OTG-BUSLOGIC-001 | Test Business Logic Data Validation | NA | Not Applicable |
| 1.10.2 | OTG-BUSLOGIC-002 | Test Ability to Forge Requests | NA | Not Applicable |
| 1.10.3 | OTG-BUSLOGIC-003 | Test Integrity Checks | NA | Not Applicable |
| 1.10.4 | OTG-BUSLOGIC-004 | Test for Process Timing | NA | Not Applicable |
| 1.10.5 | OTG-BUSLOGIC-005 | Test Number of Times a Function Can be Used Limits | NA | Not Applicable |
| 1.10.6 | OTG-BUSLOGIC-006 | Testing for the Circumvention of Work Flows | NA | Not Applicable |
| 1.10.7 | OTG-BUSLOGIC-007 | Test Defenses Against Application Mis-use | NA | Not Applicable |
| 1.10.8 | OTG-BUSLOGIC-008 | Test Upload of Unexpected File Types | NA | Not Applicable |
| 1.10.9 | OTG-BUSLOGIC-009 | Test Upload of Malicious Files | NA | Not Applicable |
| 1.11 | **Client Side Testing** | | | |
| 1.11.1 | OTG-CLIENT-001 | Testing for DOM based Cross Site Scripting | Yes | Tested, Not vulnerable |
| 1.11.2 | OTG-CLIENT-002 | Testing for JavaScript Execution | No | Tested unsafe refer  vulnerability in 2.1 |
| 1.11.3 | OTG-CLIENT-003 | Testing for HTML Injection | Yes | Tested, Not vulnerable |
| 1.11.4 | OTG-CLIENT-004 | Testing for Client Side URL Redirect | Yes | Tested, Not vulnerable |
| 1.11.5 | OTG-CLIENT-005 | Testing for CSS Injection | Yes | Tested, Not vulnerable |
| 1.11.6 | OTG-CLIENT-006 | Testing for Client Side Resource Manipulation | Yes | Tested, Not vulnerable |
| 1.11.7 | OTG-CLIENT-007 | Test Cross Origin Resource Sharing | Yes | Tested, Not vulnerable |
| 1.11.8 | OTG-CLIENT-008 | Testing for Cross Site Flashing | NA | Not Applicable |
| 1.11.9 | OTG-CLIENT-009 | Testing for Clickjacking | Yes | Tested not vulnerable |
| 1.11.10 | OTG-CLIENT-010 | Testing WebSockets | NA | Not Applicable |
| 1.11.11 | OTG-CLIENT-011 | Test Web Messaging | NA | Not Applicable |
| 1.11.12 | OTG-CLIENT-012 | Test Local Storage | Yes | Tested, Not vulnerable |

## Network Reconnaissance

PORT STATE SERVICE

80 open http

443 open https

## Scanned Items

https://www.codes.ap.gov.in/

https://www.codes.ap.gov.in/AddNewUser

https://www.codes.ap.gov.in/AOHierarchy

https://www.codes.ap.gov.in/Aooffice

https://www.codes.ap.gov.in/assetsco

https://www.codes.ap.gov.in/assetsco/bootstrap

https://www.codes.ap.gov.in/assetsco/bootstrap/css

https://www.codes.ap.gov.in/assetsco/bootstrap/css/bootstrap.min.css.map

https://www.codes.ap.gov.in/assetsco/bootstrap/js

https://www.codes.ap.gov.in/assetsco/bootstrap/js/bootstrap.bundle.min.js

https://www.codes.ap.gov.in/assetsco/bootstrap/js/bootstrap.bundle.min.js.map

https://www.codes.ap.gov.in/assetsco/font-awesome

https://www.codes.ap.gov.in/assetsco/font-awesome/fonts

https://www.codes.ap.gov.in/assetsco/jquery

https://www.codes.ap.gov.in/assetsco/jquery-easing

https://www.codes.ap.gov.in/assetsco/jquery-easing/jquery.easing.min.js

https://www.codes.ap.gov.in/assetsco/jquery/jquery.min.js

https://www.codes.ap.gov.in/autonomousorganisation

https://www.codes.ap.gov.in/aux

https://www.codes.ap.gov.in/changepassword

https://www.codes.ap.gov.in/code

https://www.codes.ap.gov.in/code/Aebasemp\_details.aspx

https://www.codes.ap.gov.in/code/codesdownload.aspx

https://www.codes.ap.gov.in/code/eofficeinfo.aspx

https://www.codes.ap.gov.in/code/ErrorPage.aspx

https://www.codes.ap.gov.in/code/fa-icons

https://www.codes.ap.gov.in/code/fa-icons/css

https://www.codes.ap.gov.in/code/officeinfo.aspx

https://www.codes.ap.gov.in/code/officeinfo.aspx?Officeid=

https://www.codes.ap.gov.in/codehome

https://www.codes.ap.gov.in/codes

https://www.codes.ap.gov.in/codes/encriptdecript

https://www.codes.ap.gov.in/codes/Login

https://www.codes.ap.gov.in/codes/Login/Loginauth

https://www.codes.ap.gov.in/codesadmin

https://www.codes.ap.gov.in/codesadmin/Login.aspx

https://www.codes.ap.gov.in/com1

https://www.codes.ap.gov.in/com2

https://www.codes.ap.gov.in/Contact

https://www.codes.ap.gov.in/copyright

https://www.codes.ap.gov.in/css2

https://www.codes.ap.gov.in/css2/datatable.js

https://www.codes.ap.gov.in/css2/jqurey31.js

https://www.codes.ap.gov.in/css2/swlalert.js

https://www.codes.ap.gov.in/cssco

https://www.codes.ap.gov.in/Distoffice

https://www.codes.ap.gov.in/districts

https://www.codes.ap.gov.in/download

https://www.codes.ap.gov.in/download/HRMSCODEBOOK.pdf

https://www.codes.ap.gov.in/errorpage

https://www.codes.ap.gov.in/feedback

https://www.codes.ap.gov.in/Gad

https://www.codes.ap.gov.in/Gad/aoDepartments

https://www.codes.ap.gov.in/Gad/edit

https://www.codes.ap.gov.in/Gad/index

https://www.codes.ap.gov.in/Gad/index/Dasbboard

https://www.codes.ap.gov.in/Gad/Levels

https://www.codes.ap.gov.in/Gad/Levels/Hierachies

https://www.codes.ap.gov.in/Gad/Levels/OfficeHeads

https://www.codes.ap.gov.in/Gad/Locations

https://www.codes.ap.gov.in/Gad/Locations/OfficeDistricts

https://www.codes.ap.gov.in/Gad/Locations/RevenueVillages

https://www.codes.ap.gov.in/Gad/office

https://www.codes.ap.gov.in/Gad/office/Aebasemp

https://www.codes.ap.gov.in/Gad/office/eofficeinfo

https://www.codes.ap.gov.in/Gad/office/officeinfo

https://www.codes.ap.gov.in/Gad/Offices

https://www.codes.ap.gov.in/Gad/Offices/districthodsuaoOffices

https://www.codes.ap.gov.in/Gad/Offices/hodsuaoOffices

https://www.codes.ap.gov.in/Gad/Organisations

https://www.codes.ap.gov.in/Gad/Organisations/OrganisationsDepartments

https://www.codes.ap.gov.in/Gad/Organisations/selectOrganisationsDepartments

https://www.codes.ap.gov.in/Gad/Services

https://www.codes.ap.gov.in/Gad/Services/ServiceCodes

https://www.codes.ap.gov.in/Gad/suOrganisations

https://www.codes.ap.gov.in/headsofdepartments

https://www.codes.ap.gov.in/headsofdepartmentsoffice

https://www.codes.ap.gov.in/HOHierachy

https://www.codes.ap.gov.in/home

https://www.codes.ap.gov.in/hyperlinking

https://www.codes.ap.gov.in/images

https://www.codes.ap.gov.in/images/hierarchical-structure.svg

https://www.codes.ap.gov.in/js

https://www.codes.ap.gov.in/js/fr-admin.min.js

https://www.codes.ap.gov.in/js1

https://www.codes.ap.gov.in/js1/aes.js

https://www.codes.ap.gov.in/js1/bootstrap-select.min.js

https://www.codes.ap.gov.in/js1/bootstrap.min.js

https://www.codes.ap.gov.in/js1/brow.js

https://www.codes.ap.gov.in/js1/client\_captcha.js

https://www.codes.ap.gov.in/js1/custom.js

https://www.codes.ap.gov.in/js1/JS\_Aadhar\_Verifivation.JS

https://www.codes.ap.gov.in/js1/ser.js

https://www.codes.ap.gov.in/Levels

https://www.codes.ap.gov.in/Levelscodingsystem

https://www.codes.ap.gov.in/locationscodingsystem

https://www.codes.ap.gov.in/Login

https://www.codes.ap.gov.in/mandals

https://www.codes.ap.gov.in/municipalareas

https://www.codes.ap.gov.in/municipalwards

https://www.codes.ap.gov.in/officeheadcategories

https://www.codes.ap.gov.in/officescodingsystem

https://www.codes.ap.gov.in/organisation

https://www.codes.ap.gov.in/organisationcodingsystem

https://www.codes.ap.gov.in/panchayats

https://www.codes.ap.gov.in/panchayatshabiti

https://www.codes.ap.gov.in/postcategorycodes

https://www.codes.ap.gov.in/privacypolicy

https://www.codes.ap.gov.in/revenuevillages

https://www.codes.ap.gov.in/revenuevillageshabi

https://www.codes.ap.gov.in/servicecodes

https://www.codes.ap.gov.in/servicescodingsystem

https://www.codes.ap.gov.in/stateunits

https://www.codes.ap.gov.in/SUHierarchy

https://www.codes.ap.gov.in/suoffice

https://www.codes.ap.gov.in/termsandconditions

## Limitations

1. The report has been prepared based on the information given by Department of General Administration, Govt of Andhra Pradesh and is accordingly, given for the specific purpose of internal use by the Department of General Administration, Govt of Andhra Pradesh. 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 General Administration, Govt of Andhra Pradesh, being the express address to this document. Department of General Administration, Govt of Andhra Pradesh 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 General Administration, Govt of Andhra Pradesh, 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 General Administration, Govt of Andhra Pradesh in writing in advance.
3. Without prior permission of Department of General Administration, Govt of Andhra Pradesh, 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 Department of General Administration, Govt of Andhra Pradesh 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 General Administration, Govt of Andhra Pradesh. Further, any quotation, citation or attribution of this report, or any extract from it, is strictly prohibited without Department of General Administration, Govt of Andhra Pradesh 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.