Cyber Security Assessment Report

of

AP Codes,

General Administration Department (GAD),

Govt. of AP

Dated 22/10/2018

by

Andhra Pradesh Technology Services

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

Vijayawada – 520 010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc528001006)

[1.1. Introduction 3](#_Toc528001007)

[1.2. Engagement Specific Details 3](#_Toc528001008)

[1.3. Scope Details 4](#_Toc528001009)

[1.3.1. Inclusion 4](#_Toc528001010)

[1.3.2. Exclusion 4](#_Toc528001011)

[1.4. Approach & Methodology 5](#_Toc528001012)

[1.4.1. Information Gathering: 5](#_Toc528001013)

[1.4.2. Automated & Manual Scanning: 5](#_Toc528001014)

[1.4.3. Analyse results and reporting: 5](#_Toc528001015)

[1.5. Risk Categorization 6](#_Toc528001016)

[1.6. Vulnerability Summary 7](#_Toc528001017)

[1.6.1. Distribution of Observation 7](#_Toc528001018)

[2. Detailed Observation 8](#_Toc528001019)

[2.1. Web Application Security Assessment & Penetration Testing 8](#_Toc528001020)

[2.2. Server Vulnerability Summary 24](#_Toc528001021)

[3. Appendix 26](#_Toc528001022)

[3.1. OWASP Checklist 26](#_Toc528001023)

[3.2. Network Reconnaissance 32](#_Toc528001024)

[4. SSL Test 32](#_Toc528001025)

[5. Scanned Items 34](#_Toc528001026)

[6. Limitations 38](#_Toc528001027)

1. Executive Summary

## Introduction

The General Administration Department (GAD) deals with the entire gamut of personnel management in the Government- recruitment, training, performance evaluation, promotion, discipline, placement, service conditions and so on.

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Cyber Security Assessment of AP Codes Application for General Administration 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. 09/10/2018 |
| 1. 2. | 1. Submission date of initial report | 1. 11/10/2018 |
| 1. 3. | 1. Submission date of confirmatory review | 1. 22/10/2018 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | 1. Ch. Sai Suresh | 1. Praveen Kodi | 1. General Administration Department |
| 1. 2. | 1. Server Vulnerability Assessment | 1. Ch. Sai Suresh | 1. Praveen Kodi | 1. General Administration Department |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 11/10/2018 | 1. v1.0 | 1. Initial Review |
| 1. 2 | 1. 22/10/2018 | 1. v1.1 | 1. Confirmatory review |

## Scope Details

### Inclusion

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

Application Name: AP Codes

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

Environment: Production

Version Number [or] Latest Compilation Timestamp: Not provided

Type of Review: Blackbox

Hash of Zipped Source Code (SHA512): Not provided

1. **Server Vulnerability Assessment**

Type of Review: Black box

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **IP Address** | **OEM** | **Version No.** | **Server Type** |
| 1. | 125.18.110.41 | Microsoft Windows Server | 2012 R2 | Web Server |
| 2. | Microsoft-IIS | 8.5 |
| 3 | 10.252.115.151 | SQL Server | 2012 – 11.0.2 | DB Server |

### Exclusion

1. Secure Code Review
2. Process Review
3. Secure Network Architecture Review
4. Our review was not done to full length due to the security devices at the production server that have not white listed our ip address.

## 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/ 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** | | | **Confirmatory Review** | | |
| **High** | **Medium** | **Low** | **High** | **Medium** | **Low** |
| **Web Application Security Assessment** | 2 | 2 | 7 | **00**0 | 0 | 0 |
| **Server Vulnerability Assessment** | 0 | 2 | 0 | 0 | 0 | 0 |
| **Total** | **2** | **4** | **7** | **0** | **0** | **0** |
|  |  |  | **13** |  |  | **0** |

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Broken authentication and Improper Session Management** | **Risk Rating**: High | **Compliance status: C**losed & Complied |
| **Description** | The application allows an authenticated user to access the pages that should be accessible to the administrator only. This happens due to the improper implementation of access controls by the application. The AddUser page is accessible to any unauthenticated user by visiting the URL | |
| **Affected Path(s)** | /AddNewUser  /ChangePassword | |
| **Impact** | An unauthenticated user, who has access to the application, can make any changes to the application’s data with the admin privileges. | |
| **Evidence/Proof of Concept** | | |
| **Recommendation** | 1. Ensure that the authentication and session management is implemented with proper access controls. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Unrestricted File upload** | **Risk Rating**: High | **Compliance status: C**losed & Complied |
| **Description** | The application allows the user to upload files without any restrictions. In this case, the application accepted the given file anydesk.exe which is an executable file. | |
| **Affected Path(s)** | /ca\_sectdep   1. /ca\_officeheads 2. /ca\_HeadsofDep 3. /ca\_StateUnits 4. /ca\_AUOrganisations   /ca\_hodoffices | |
| **Impact** | If the uploaded file contains the ***VIRUS*** in it, it may harm the server very badly and the users. | |
| **Evidence/Proof of Concept** | | |
| **Recommendation** | 1. 1. Never accept a filename and its extension directly without having a white-list filter. 2. 2. If there is no need to have Unicode characters, it is highly recommended to only accept alpha-numeric characters and only one dot as an input for the file name and the extension. 3. 3. Don't rely on client-side validation only.   4. Uploaded directory should not have any "execute" permission.  Reference:   1. https://www.owasp.org/index.php/Unrestricted\_File\_Upload | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **No account lockout policy implemented** | **Risk Rating**: Medium | **Compliance status : C**losed & Complied |
| **Description** | The application does not implement account lockout policy for the multiple invalid login attempts made by the user. This allows an attacker to guess for the correct combination of credentials by trying in a random manner. | |
| **Affected Path(s)** | /Login  /codesadmin/Login.aspx | |
| **Impact** | The attacker can perform the countless login attempts to find the right set of login credentials which should not happen. | |
| **Evidence/Proof of Concept**  F:\security res\Audit\AP Codes\UNSAFE SCREENSHOTS\account lockout.PNG | | |
| **Recommendation** | It is recommended to perform the following:   * Implement the tools such as the reCAPTCHA to prevent automated submissions. * Also use the lockout method to block after the certain number of requests made by the user. * Block the requests from that IP address for sometime if you find multiple requests are made from it. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Technology / Version Disclosure** | **Risk Rating : Medium** | **Compliance status : C**losed & Complied |
| **Description** | The application includes the headers Server and X-Powered-By in the response that reveals the server and the application version details. | |
| **Affected Path(s)** | / (web server) | |
| **Impact** | An attacker makes use of this information to launch focused attacks based on the public exploits available for these versions. | |
| **Evidence/Proof of Concept**  F:\security res\Audit\AP Codes\UNSAFE SCREENSHOTS\Version disclosure.PNG | | |
| **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. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **HTTP vulnerable method enabled** | **Risk Rating**: Low | **Compliance status : C**losed & Complied |
| **Description** | Vulnerable HTTP method is enabled on this web server. The OPTIONS method provides a list of the methods that are supported by the web server, it represents a request for information about the communication options available on the request/response chain identified by the Request-URI  TRACE is method which can be used for debugging purposes should be disabled. | |
| **Affected Path(s)** | /(web server) | |
| **Impact** | The TRACE method repeats the content of a request, and an attacker could steal credentials by using a client-side attack. | |
| **Evidence/Proof of Concept**  F:\security res\Audit\AP Codes\UNSAFE SCREENSHOTS\Options enabled.PNG | | |
| **Recommendation** | It's recommended to disable TRACE Method on the web server from the config file. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Stack Trace enabled** | **Risk Rating**: Low | **Compliance status : C**losed & Complied |
| **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** | 1. 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**  F:\security res\Audit\AP Codes\UNSAFE SCREENSHOTS\Stack trace #1.PNG | | |
| **Recommendation** | 1. Apply following changes on your web.config file to prevent information leakage by applying custom error pages. 2. <System.Web> 3. <customErrors mode="On" defaultRedirect="~/error/GeneralError.aspx"> 4. <error statusCode="403" redirect="~/error/Forbidden.aspx" /> 5. <error statusCode="404" redirect="~/error/PageNotFound.aspx" /> 6. <error statusCode="500" redirect="~/error/InternalError.aspx" /> 7. </customErrors>   </System.Web> | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Internal path disclosure through improper handling of error messages.** | **Risk Rating**: Low | **Compliance status : C**losed & Complied |
| **Description** | The application software generates an error message that includes sensitive information about its environment. In this case, the server discloses the unnecessary information like the source file path. | |
| **Affected Path(s)** | / (web server) | |
| **Impact** | The information might help an attacker gain more information and potentially focus on the development of further attacks for the target system such as the file location on the server. | |
| **Evidence/Proof of Concept**  F:\security res\Audit\AP Codes\UNSAFE SCREENSHOTS\Error #1.PNG | | |
| **Recommendation** | 1. Apply following changes on your web.config file to prevent information leakage by applying custom error pages. 2. <System.Web> 3. <customErrors mode="On" defaultRedirect="~/error/GeneralError.aspx"> 4. <error statusCode="403" redirect="~/error/Forbidden.aspx" /> 5. <error statusCode="404" redirect="~/error/PageNotFound.aspx" /> 6. <error statusCode="500" redirect="~/error/InternalError.aspx" /> 7. </customErrors>   </System.Web> | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Click jacking Attack** | **Risk Rating**: Low | **Compliance status : C**losed & Complied |
| **Description** | 1. Clickjacking 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. The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. | |
| **Affected Path(s)** | / (webserver) | |
| **Impact** | An attacker may trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons. When the user clicks on the buttons he is redirected to the attacker’s malicious websites. | |
| **Evidence/Proof of Concept**  F:\security res\Audit\AP Codes\UNSAFE SCREENSHOTS\Clickjackin.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.   Refer to respective CWE and relevant guidelines for more information:  https://cwe.mitre.org/data/definitions/1021.html | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Strict-Transport-Security Header Not Set** | **Risk Rating**: Low | **Compliance status : C**losed & Complied |
| **Description** | The server is not configured with the HTTP strict transport security header (HSTS) in the response header. HTTP Strict Transport Security (HSTS) is a method for web applications to ensure they only use TLS to support secure transport. It protects users against passive eavesdropper and active man-in-the-middle (MITM) attacks. | |
| **Affected Path(s)** | / (web server) | |
| **Impact** | Failing to implement HSTS can lead to potential man in the middle attack and eavesdropping the connections due to plain text transfer of data. | |
| **Evidence/Proof of Concept**  F:\security res\Audit\AP Codes\UNSAFE SCREENSHOTS\HSTS.PNG | | |
| **Recommendation** | 1. Configure the server with the following options:  * **Strict-Transport-Security: max-age=31536000**  1. The HSTS policy is applied only to the domain of HSTS host issuing it and remains in effect for one year.  * **Strict-Transport-Security: max-age=31536000; includeSubDomains**  1. The HSTS policy is applied to the domain of the issuing host as well as its subdomains and remains in effect for one year. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Password type input with auto-complete enabled** | **Risk Rating**: Low | **Compliance status : C**losed & Complied |
| **Description** | The application allows the passwords to be saved when the form is submitted by the user. These credentials are stored in the browser cache for later use by the user. | |
| **Affected Path(s)** | / Login | |
| **Impact** | An attacker with local access could obtain the clear text password from the browser cache that result in the sensitive information disclosure. | |
| **Evidence/Proof of Concept**  C:\Users\APTSADMIN\Pictures\Screenshots\Screenshot (31).png | | |
| **Recommendation** | 1. The password auto-complete should be disabled in sensitive applications. 2. To disable auto-complete, you may use a code similar to: 3. <INPUT TYPE="password" AUTOCOMPLETE="off" | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerable Javascript library** | **Risk rating: Low** | **Compliance status : C**losed & Complied |
| **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. /AOHierarchy 2. /Aooffice 3. /Contact 4. /HOHierachy 5. /Levels 6. /Levelscodingsystem 7. /SUHierarchy 8. /autonomousorganisation 9. /code/officeinfo.aspx 10. /districts 11. /feedback 12. /headsofdepartments 13. /headsofdepartmentsoffice 14. /officeheadcategories 15. /organisation 16. /organisationcodingsystem   /stateunits | |
| **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** |  | |

## Server Vulnerability Summary

| **S. No** | **Vulnerability Name** | **Risk Rating** | **Affected Devices** | **Description** | **Impact** | **Recommendation** | **Management Comments** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | SMB Signing not required | Medium | 125.18.110.41  TCP/445 | An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | Signing is not required on the remote SMB server. | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the links for further details.   1. https://support.microsoft.com/en-us/kb/887429 2. http://technet.microsoft.com/en-us/library/cc731957.aspx   http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html |  |
| 2 | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) | Medium | 125.18.110.41  TCP/445 | 1. The remote Windows host supports Server Message Block Protocol version 1 (SMBv1). Microsoft recommends that users discontinue the use of SMBv1 due to the lack of security features that were included in later SMB versions. Additionally, the Shadow Brokers group reportedly has an exploit that affects SMB; however, it is unknown if the exploit affects SMBv1 or another version. In response to this, US-CERT recommends that users disable SMBv1 per SMB best practices to mitigate these potential issues. 2. TCP/445   The remote host supports SMBv1. | The remote Windows host supports the SMBv1 protocol. | 1. Disable SMBv1 according to the vendor instructions in Microsoft KB2696547. 2. Additionally, block SMB directly by blocking TCP port 445 on all network boundary devices. 3. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices. 4. See also: 5. https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/   https://support.microsoft.com/en-us/kb/2696547 |  |

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 | No considerable information found |
| 1.1.2 | OTG-INFO-002 | Fingerprint Web Server | No | Microsoft-IIS/8.5  AspNet-Version: 4.0.30319 |
| 1.1.3 | OTG-INFO-003 | Review Webserver Metafiles for Information Leakage | Yes | No data found |
| 1.1.4 | OTG-INFO-004 | Enumerate Applications on Webserver | Yes | Codes.ap.gov.in |
| 1.1.5 | OTG-INFO-005 | Review Webpage Comments and Metadata for Information Leakage | Yes | No information found |
| 1.1.6 | OTG-INFO-006 | Identify application entry points | Yes | /Login |
| 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 | Microsoft-IIS/8.5  ASP.NET |
| 1.1.9 | OTG-INFO-009 | Fingerprint Web Application | No | Asp.Net 4.0.30319 |
| 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 | Microsoft-IIS/8.5  ASP.NET |
| 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 | No | /AddNewUser  /codesadmin/Login.aspx |
| 1.2.5 | OTG-CONFIG-005 | Enumerate Infrastructure and Application Admin Interfaces | No | /codesadmin/Login.aspx |
| 1.2.6 | OTG-CONFIG-006 | Test HTTP Methods | No | Tested. Observation reported |
| 1.2.7 | OTG-CONFIG-007 | Test HTTP Strict Transport Security | No | Tested. Observation reported |
| 1.2.8 | OTG-CONFIG-008 | Test RIA cross domain policy | No | Cross domain policy not implemented |
| 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 found |
| 1.3.3 | OTG-IDENT-003 | Test Account Provisioning Process | NA | Not applicable |
| 1.3.4 | OTG-IDENT-004 | Testing for Account Enumeration and Guessable User Account | Yes | Not found |
| 1.3.5 | OTG-IDENT-005 | Testing for Weak or unenforced username policy | Yes | Not vulnerable |
| 1.3.6 | OTG-IDENT-006 | Test Permissions of Guest/Training Accounts | NA | Not found |
| 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 | Yes | Appilcation using HTTPS |
| 1.4.2 | OTG-AUTHN-002 | Testing for default credentials | Yes | Not found |
| 1.4.3 | OTG-AUTHN-003 | Testing for Weak lock out mechanism | No | Tested. Observation reported |
| 1.4.4 | OTG-AUTHN-004 | Testing for bypassing authentication schema | No | Tested. Observation reported |
| 1.4.5 | OTG-AUTHN-005 | Test remember password functionality | No | Tested. Observation reported |
| 1.4.6 | OTG-AUTHN-006 | Testing for Browser cache weakness | Yes | Cache-Control: private  Cache-Control: no-cache  Pragma: no-cache |
| 1.4.7 | OTG-AUTHN-007 | Testing for Weak password policy | NA | Not applicable |
| 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 | Not vulnerable |
| 1.5.2 | OTG-AUTHZ-002 | Testing for bypassing authorization schema | No | Tested. Observation Reported |
| 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 | Not vulnerable |
| 1.6 | **Session Management Testing** | | | |
| 1.6.1 | OTG-SESS-001 | Testing for Bypassing Session Management Schema | No | Tested. Observation Reported |
| 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 | NA | Not applicable |
| 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 | Yes | Not vulnerable |
| 1.7.2 | OTG-INPVAL-002 | Testing for Stored Cross Site Scripting | Yes | Not vulnerable |
| 1.7.3 | OTG-INPVAL-003 | Testing for HTTP Verb Tampering | No | Tested. Observation reported |
| 1.7.4 | OTG-INPVAL-004 | Testing for HTTP Parameter pollution | Yes | Not vulnerable |
| 1.7.5 | OTG-INPVAL-005 | Testing for SQL Injection | Yes | Not vulnerable |
| 1.7.5.1 |  | Oracle Testing | Yes | Not vulnerable |
| 1.7.5.2 |  | MySQL Testing | Yes | Not vulnerable |
| 1.7.5.3 |  | SQL Server Testing | Yes | Not vulnerable |
| 1.7.5.4 |  | Testing PostgreSQL | Yes | Not vulnerable |
| 1.7.5.5 |  | MS Access Testing | Yes | Not vulnerable |
| 1.7.5.6 |  | Testing for NoSQL injection | Yes | Not vulnerable |
| 1.7.6 | OTG-INPVAL-006 | Testing for LDAP Injection | NA | Technology not in use |
| 1.7.7 | OTG-INPVAL-007 | Testing for ORM Injection | Yes | Not vulnerable |
| 1.7.8 | OTG-INPVAL-008 | Testing for XML Injection | NA | No XML pages used. |
| 1.7.9 | OTG-INPVAL-009 | Testing for SSI Injection | NA | No .SHTML pages found |
| 1.7.10 | OTG-INPVAL-010 | Testing for XPath Injection | NA | No XML pages used. |
| 1.7.11 | OTG-INPVAL-011 | IMAP/SMTP Injection | NA | Technology not in use |
| 1.7.12 | OTG-INPVAL-012 | Testing for Code Injection | Yes | Not vulnerable |
| 1.7.12.1 |  | Testing for Local File Inclusion | Yes | Not vulnerable |
| 1.7.12.2 |  | Testing for Remote File Inclusion | Yes | Not vulnerable |
| 1.7.13 | OTG-INPVAL-013 | Testing for Command Injection | Yes | Not vulnerable |
| 1.7.14 | OTG-INPVAL-014 | Testing for Buffer overflow | Yes | Not vulnerable |
| 1.7.14.1 |  | Testing for Heap overflow | Yes | Not vulnerable |
| 1.7.14.2 |  | Testing for Stack overflow | Yes | Not vulnerable |
| 1.7.14.3 |  | Testing for Format string | Yes | Not vulnerable |
| 1.7.15 | OTG-INPVAL-015 | Testing for incubated vulnerabilities | No | Tested. Observation reported as multiple vulnerabilities |
| 1.7.16 | OTG-INPVAL-016 | Testing for HTTP Splitting/Smuggling | Yes | Not vulnerable |
| 1.8 | **Error Handling** | | | |
| 1.8.1 | OTG-ERR-001 | Analysis of Error Codes | No | Tested. Observation reported |
| 1.8.2 | OTG-ERR-002 | Analysis of Stack Traces | No | Tested. Observation reported |
| 1.9 | **Cryptography** | | | |
| 1.9.1 | OTG-CRYPST-001 | Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection | No | Server Using RC4 weak cipher suites |
| 1.9.2 | OTG-CRYPST-002 | Testing for Padding Oracle | Yes | Tested. Not vulnerable |
| 1.9.3 | OTG-CRYPST-003 | Testing for Sensitive information sent via unencrypted channels | Yes | Application using HTTPS |
| 1.1 | **Business Logic Testing** | | | |
| 1.10.1 | OTG-BUSLOGIC-001 | Test Business Logic Data Validation | Yes | Not vulnerable |
| 1.10.2 | OTG-BUSLOGIC-002 | Test Ability to Forge Requests | Yes | Not vulnerable |
| 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 | No | Tested. Observation reported |
| 1.10.9 | OTG-BUSLOGIC-009 | Test Upload of Malicious Files | No | Tested. Observation reported |
| 1.11 | **Client Side Testing** | | | |
| 1.11.1 | OTG-CLIENT-001 | Testing for DOM based Cross Site Scripting | Yes | Not vulnerable |
| 1.11.2 | OTG-CLIENT-002 | Testing for JavaScript Execution | Yes | Not vulnerable |
| 1.11.3 | OTG-CLIENT-003 | Testing for HTML Injection | Yes | Not vulnerable |
| 1.11.4 | OTG-CLIENT-004 | Testing for Client Side URL Redirect | Yes | Not vulnerable |
| 1.11.5 | OTG-CLIENT-005 | Testing for CSS Injection | Yes | Not vulnerable |
| 1.11.6 | OTG-CLIENT-006 | Testing for Client Side Resource Manipulation | Yes | Not vulnerable |
| 1.11.7 | OTG-CLIENT-007 | Test Cross Origin Resource Sharing | Yes | Not vulnerable |
| 1.11.8 | OTG-CLIENT-008 | Testing for Cross Site Flashing | NA | Not applicable. No flash content in the application |
| 1.11.9 | OTG-CLIENT-009 | Testing for Clickjacking | No | Tested. Observation reported |
| 1.11.10 | OTG-CLIENT-010 | Testing WebSockets | NA | Technology not in use |
| 1.11.11 | OTG-CLIENT-011 | Test Web Messaging | NA | Technology not in use |
| 1.11.12 | OTG-CLIENT-012 | Test Local Storage | Yes | Cache-Control: private  Cache-Control: no-cache  Pragma: no-cache |

## Network Reconnaissance

PORT STATE SERVICE VERSION

80/tcp open http Microsoft IIS httpd 8.5

113/tcp closed ident

8008/tcp open http Fortinet FortiGuard block page

8010/tcp closed xmpp

Service Info: OS: Windows; Device: security-misc; CPE: cpe:/o:microsoft:windows

## SSL Test

SSL/TLS Connection Test: Successful

Offer SSLv2: No

Offer SSLv3: No

Offer TLS1.0: No

Offer TLS1.1: No

Offer TLS1.2: Yes

Available ciphers:

NULL Cipher (no encryption): No

ANON Cipher (no authentication): No

EXP Cipher (without ADH+NULL): No

LOW Cipher (64 Bit + DES Encryption): No

WEAK Cipher (SEED, IDEA, RC2, RC4): No

3DES Cipher (Medium): No

HIGH Cipher (AES+Camellia, no AEAD): Yes (OK)

STRONG Cipher (AEAD Ciphers): No (not OK)

Heartbleed: Not vulnerable

CCS Injection: Not vulnerable

TLS\_FALLBACK\_SCSV Support: No

POODLE (SSLv3): Not vulnerable

Sweet32: Not vulnerable

DROWN: Not vulnerable

FREAK: Not vulnerable

LUCKY13: Potentially vulnerable

CRIME (TLS): Not vulnerable

BREACH: Not vulnerable

BEAST: Not vulnerable

LOGJAM (Export): Not vulnerable

LOGJAM (Common Prime): Not vulnerable

Finished scanning

Summary

Supported ciphers (by Protocol)

TLSv1.2

AES256-SHA256: LUCKY13

AES256-SHA: LUCKY13

ECDHE-RSA-AES256-SHA: LUCKY13

ECDHE-RSA-AES128-SHA256: LUCKY13

ECDHE-RSA-AES128-SHA: LUCKY13

AES128-SHA256: LUCKY13

AES128-SHA: LUCKY13

Supported ciphers (by Vulnerability)

LUCKY13

AES128-SHA (TLSv1.2)

AES128-SHA256 (TLSv1.2)

AES256-SHA (TLSv1.2)

AES256-SHA256 (TLSv1.2)

ECDHE-RSA-AES128-SHA (TLSv1.2)

ECDHE-RSA-AES128-SHA256 (TLSv1.2)

ECDHE-RSA-AES256-SHA (TLSv1.2)

Issues found

[Low] LUCKY13

[Information] Supported Cipher Suites

## Scanned Items

[/](https://www.codes.ap.gov.in/)

[/accountactivity](https://www.codes.ap.gov.in/accountactivity)

[/AddNewUser](https://www.codes.ap.gov.in/AddNewUser)

[/AOHierarchy](https://www.codes.ap.gov.in/AOHierarchy)

[/Aooffice](https://www.codes.ap.gov.in/Aooffice)

[/assetsco](https://www.codes.ap.gov.in/assetsco)

/assetsco/bootstrap

/assetsco/bootstrap/css

/assetsco/bootstrap/css/bootstrap.min.css

/assetsco/bootstrap/js

/assetsco/bootstrap/js/bootstrap.bundle.min.js

/assetsco/font-awesome

/assetsco/font-awesome/css

/assetsco/font-awesome/css/font-awesome.min.css

/assetsco/font-awesome/fonts

/assetsco/font-awesome/fonts/fontawesome-webfont.woff2

[/assetsco/jquery](https://www.codes.ap.gov.in/assetsco/jquery)

/assetsco/jquery-easing

/assetsco/jquery-easing/jquery.easing.min.js

/assetsco/jquery/jquery.min.js

/autonomousorganisation

[/ca\_aooffice](https://www.codes.ap.gov.in/ca_aooffice)

[/ca\_AUOrganisations](https://www.codes.ap.gov.in/ca_AUOrganisations)

[/ca\_districts](https://www.codes.ap.gov.in/ca_districts)

[/ca\_HeadsofDep](https://www.codes.ap.gov.in/ca_HeadsofDep)

[/ca\_hodoffices](https://www.codes.ap.gov.in/ca_hodoffices)

[/ca\_mandals](https://www.codes.ap.gov.in/ca_mandals)

/ca\_municipalareas

[/ca\_municipalwards](https://www.codes.ap.gov.in/ca_municipalwards)

/ca\_officeheads

[/ca\_officeheads.aspx](https://www.codes.ap.gov.in/ca_officeheads.aspx)

/ca\_panchayats

/ca\_panchayatshabitation

/ca\_postcategorycodes

/ca\_revenuehabitation

[/ca\_revenuevillages](https://www.codes.ap.gov.in/ca_revenuevillages)

[/ca\_sectdep](https://www.codes.ap.gov.in/ca_sectdep)

[/ca\_servicecodes](https://www.codes.ap.gov.in/ca_servicecodes)

[/ca\_StateUnits](https://www.codes.ap.gov.in/ca_StateUnits)

[/ca\_suoffices](https://www.codes.ap.gov.in/ca_suoffices)

[/ChangePassword](https://www.codes.ap.gov.in/ChangePassword)

[/co](https://www.codes.ap.gov.in/co)

[/co/officeinfo.aspx](https://www.codes.ap.gov.in/co/officeinfo.aspx)

[/code](https://www.codes.ap.gov.in/code)

[/code/fa-icons](https://www.codes.ap.gov.in/code/fa-icons)

[/code/fa-icons/css](https://www.codes.ap.gov.in/code/fa-icons/css)

/code/fa-icons/css/fontawesome-all.min.css

/codesadmin

/codesadmin/accountactivity

/codesadmin/AddNewUser

/codesadmin/ca\_aooffice

/codesadmin/ca\_AUOrganisations

/codesadmin/ca\_districts

/codesadmin/ca\_HeadsofDep

/codesadmin/ca\_hodoffices

/codesadmin/ca\_hodoffices.aspx

/codesadmin/ca\_mandals

/codesadmin/ca\_municipalareas

/codesadmin/ca\_municipalwards

/codesadmin/ca\_officeheads

/codesadmin/ca\_officeheads.aspx

/codesadmin/ca\_panchayats

/codesadmin/ca\_panchayatshabitation

/codesadmin/ca\_postcategorycodes

/codesadmin/ca\_revenuehabitation

/codesadmin/ca\_revenuevillages

[/codesadmin/ca\_sectdep](https://www.codes.ap.gov.in/codesadmin/ca_sectdep)

/codesadmin/ca\_servicecodes

/codesadmin/ca\_StateUnits

/codesadmin/ca\_suoffices

/codesadmin/ChangePassword

/codesadmin/home

/codesadmin/index

/codesadmin/Login.aspx

/codesadmin/Profile

[/codesadmin/UserRights](https://www.codes.ap.gov.in/codesadmin/UserRights)

[/Contact](https://www.codes.ap.gov.in/Contact)

[/copyright](https://www.codes.ap.gov.in/copyright)

[/css2](https://www.codes.ap.gov.in/css2)

/css2/bootstrap-select.min.css

/css2/bootstrap.min.css

/css2/customstyle.css

[/css2/datatable.css](https://www.codes.ap.gov.in/css2/datatable.css)

[/css2/datatable.js](https://www.codes.ap.gov.in/css2/datatable.js)

[/css2/frstyle.css](https://www.codes.ap.gov.in/css2/frstyle.css)

[/css2/jqurey31.js](https://www.codes.ap.gov.in/css2/jqurey31.js)

[/css2/style.css](https://www.codes.ap.gov.in/css2/style.css)

[/css2/swlalert.js](https://www.codes.ap.gov.in/css2/swlalert.js)

[/cssco](https://www.codes.ap.gov.in/cssco)

/cssco/customstyle.css

[/cssco/frstyle.css](https://www.codes.ap.gov.in/cssco/frstyle.css)

[/Default](https://www.codes.ap.gov.in/Default)

[/districts](https://www.codes.ap.gov.in/districts)

[/download](https://www.codes.ap.gov.in/download)

[/feedback](https://www.codes.ap.gov.in/feedback)

[/fonts](https://www.codes.ap.gov.in/fonts)

/fonts/glyphicons-halflings-regular.woff2

[/Gad](https://www.codes.ap.gov.in/Gad)

/Gad/aoDepartments

/Gad/aoDepartments/aoDepartments

[/Gad/edit](https://www.codes.ap.gov.in/Gad/edit)

[/Gad/index](https://www.codes.ap.gov.in/Gad/index)

[/Gad/index/Dasbboard](https://www.codes.ap.gov.in/Gad/index/Dasbboard)

/Gad/Levels

/Gad/Levels/OfficeHeads

/Gad/Locations

/Gad/Locations/Districts

/Gad/Locations/Habitations

/Gad/Locations/Mandal

/Gad/Locations/OfficeDistricts

/Gad/Locations/officeMandal

/Gad/Locations/Panchayats

/Gad/Locations/RevenueVillages

/Gad/Offices

/Gad/Offices/hodsuaoOffices

/Gad/Organisations

/Gad/Organisations/OrganisationsDepartments

/Gad/Services

/Gad/Services/PostCategoryCodes

/Gad/Services/ServiceCodes

/Gad/suOrganisations

/Gad/suOrganisations/suDepartments /Gad/suOrganisations/suOrganisationsDepartments

/headsofdepartments /headsofdepartmentsoffice

[/HOHierachy](https://www.codes.ap.gov.in/HOHierachy)

[/home](https://www.codes.ap.gov.in/home)

[/home.aspx](https://www.codes.ap.gov.in/home.aspx)

[/hyperlinking](https://www.codes.ap.gov.in/hyperlinking)

/images

[/imagesco](https://www.codes.ap.gov.in/imagesco)

/index

[/js](https://www.codes.ap.gov.in/js)

[/js/fr-admin.min.js](https://www.codes.ap.gov.in/js/fr-admin.min.js)

/js1

[/js1/aes.js](https://www.codes.ap.gov.in/js1/aes.js)

/js1/bootstrap-select.min.js

/js1/bootstrap.min.js

[/js1/custom.js](https://www.codes.ap.gov.in/js1/custom.js)

/js1/edit.css /js1/JS\_Aadhar\_Verifivation.JS

/js1/ser.js

[/Levels](https://www.codes.ap.gov.in/Levels)

/Levelscodingsystem

[/locationscodingsystem](https://www.codes.ap.gov.in/locationscodingsystem)

/Login

[/mandals](https://www.codes.ap.gov.in/mandals)

/municipalareas

/municipalwards

/officeheadcategories

/officescodingsystem

/organisation

/organisationcodingsystem

[/panchayats](https://www.codes.ap.gov.in/panchayats)

/panchayatshabiti

/postcategorycodes

[/privacypolicy](https://www.codes.ap.gov.in/privacypolicy)

[/Profile](https://www.codes.ap.gov.in/Profile)

/revenuevillages

/revenuevillageshabi

/ScriptResource.axd

/servicecodes

/servicescodingsystem

[/stateunits](https://www.codes.ap.gov.in/stateunits)

[/SUHierarchy](https://www.codes.ap.gov.in/SUHierarchy)

[/suoffice](https://www.codes.ap.gov.in/suoffice)

/tags\_code=value

/termsandconditions

/UserRights

/WebResource.axd

/www.lgdirectory.gov.in

## Limitations

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