Application Security Assessment Report

of

CSIP,

Department of Health, Medical & Family Welfare,

Govt. of AP

22/10/2019

by

Andhra Pradesh Technology Services

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

Vijayawada – 520 010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc527051578)

[1.1. Introduction 3](#_Toc527051579)

[1.2. Engagement Specific Details 3](#_Toc527051580)

[1.3. Scope Details 4](#_Toc527051581)

[1.3.1. Inclusion 4](#_Toc527051582)

[1.3.2. Exclusion 4](#_Toc527051583)

[1.4. Approach & Methodology 5](#_Toc527051584)

[1.4.1. Information Gathering: 5](#_Toc527051585)

[1.4.2. Automated & Manual Scanning: 5](#_Toc527051586)

[1.4.3. Analyse results and reporting: 5](#_Toc527051587)

[1.5. Risk Categorization 6](#_Toc527051588)

[1.6. Vulnerability Summary 7](#_Toc527051589)

[1.6.1. Distribution of Observation 7](#_Toc527051590)

[2. Detailed Observation 8](#_Toc527051591)

[2.1. Web Application Security Assessment & Penetration Testing 8](#_Toc527051592)

[2.2. Vulnerability Summary 8](#_Toc527051593)

[3. Appendix 9](#_Toc527051594)

[3.1. OWASP Checklist 9](#_Toc527051595)

[3.2. Network Reconnaissance 12](#_Toc527051596)

[4. SSL Test 12](#_Toc527051597)

[5. Scanned Items 13](#_Toc527051598)

[6. Limitations 13](#_Toc527051599)

1. Executive Summary

## Introduction

Health care should be within the reach of every citizen. For providing basic health facilities to all citizens, government has introduced and implemented various health schemes and programmes. This section provides information pertaining to health programmes, policies, schemes, forms etc. for specific beneficiaries including women, children, senior citizen, etc. The Department of Health, Medical and Family Welfare provides health care facilities to the people of Andhra Pradesh. Health care should be within the reach of every citizen.

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Application Security Assessment of CSIP Application for Department of Health,Medical & Family Welfare 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. 22/10/2019 |
| 1. 2. | 1. Submission date of initial report | 1. 23/10/2019 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | 1. APTS TEAM | 1. Name | Health, Medical ,family Welfare Department |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 22/10/2019 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

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

Application Name: CSIP

Application URL: http://hmfw.ap.gov.in/csip\_test(S(rbk1ygt52wfzoigxj1nnyg1))

Environment: UAT

Version Number [or] Latest Compilation Timestamp: Not Provided

Type of Review: Greybox

Hash of Zipped Source Code (SHA512):Not Provided

### Exclusion

[If any]

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 an automated & Manual scanning (with the knowledge of user credentials) of the web application URL using commercial and open source tools. The scanning was conducted to identify any known vulnerabilities in the subjected application.

### Analyse results and reporting:

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

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

## Risk Categorization

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

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

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

The final risk ratings are defined as follows:

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

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

## Vulnerability Summary

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Review Area** | **Initial Review** | | |
| **High** | **Medium** | **Low** |
| **Web Application Security Assessment** | 0 | 2 | 8 |
| **Total** |  | |  |

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Insufficient Anti Automation** | **Risk Rating**: Medium |
| **Description** | Insufficient Anti-automation is when a web site permits an attacker to automate a process that should only be performed manually. Certain web site functionalities should be protected against automated attacks. | |
| **Affected Path(s)** | http://hmfw.ap.gov.in/csip\_test/(S(rbk1ygt52wfzoigxj1nnyg1d))/csilogin.aspx  http://hmfw.ap.gov.in/csip\_test/(S(rbk1ygt52wfzoigxj1nnyg1d))/CSIIndianRegPersonal.aspx  http://hmfw.ap.gov.in/csip\_test/(S(rbk1ygt52wfzoigxj1nnyg1d))/CSIAttachmentLoader.aspx | |
| **Impact** | Attackers could repeatedly exercise web site functionality attempting to exploit or defraud the system. An automated robot could potentially execute thousands of requests a minute, causing potential loss of performance or service. | |
| **Evidence/Proof of Concept**  **Step 1:** CAPTCHA is not enabled in the login page and also in form submission pages before login.  captcha.JPG  cap1.JPG | | |
| **Recommendation** | It is recommended to implement captcha. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Sensitive information disclosure** | **Risk Rating**: Medium |
| **Description** | Sensitive data exposure can occur when an application does not adequately protect sensitive information from being disclosed to attackers. Sensitive information such as bank account numbers, Aadhar card numbers and pan card numbers. | |
| **Affected Path(s)** | http://hmfw.ap.gov.in/csip\_test/(S(ncmwicdu123i3dlssrvgarl3))/ViewAttachments. | |
| **Impact** | Possible sensitive information disclosure. | |
| **Evidence/Proof of Concept**  **Step-1:** Access the URL= http://hmfw.ap.gov.in/csip\_test/(S(ncmwicdu123i3dlssrvgarl3))/ViewAttachments.aspx after login. Aadhar numbers and Certificates numbers are being displayed in plaintext as shown below.  senstive information.png  **senstive information 1.png** | | |
| **Recommendation** | Mask all the sensitive information and only display last four digits.  Encrypt the data when storing in servers.  Reference Links:  https://cwe.mitre.org/data/definitions/200.html | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Improper Error Handling** | **Risk Rating**: Low |
| **Description** | 1. 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**  **error.JPG**  Fig. Stack trace enabled | | |
| **Recommendation** | 1. Disable the trace in the web.config file. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Weak password policy** | **Risk Rating:** Medium |
| **Description** | 1. The password policy implemented by the application is not as per the standard security practices recommended by the NIST. As per the NIST rules, the password must contain at least 10 characters wherein the application recommends for only minimum 5 characters. | |
| **Affected Path(s)** | http://hmfw.ap.gov.in/csip\_test/(S(gwcvs2d4vz0sllcux3w5enm4))/csilogin.aspx | |
| **Impact** | Not implementing a proper password policy, could allow the users to set very easy password that help the attackers to perform the dictionary attacks and gain access to the user accounts. | |
| **Evidence/Proof of Concept**  password policy.JPG  Fig. Weak Password Policy | | |
| **Recommendation** | Implement a strong password policy that contains: 1. one capital letter 2. One number 3. Minimum 8 characters 4. One special character. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Unencrypted Communication** | **Risk Rating**: Medium |
| **Description** | The application allows users to connect to it over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with the application and obtain any information the user supplies. Furthermore, an attacker able to modify traffic could use the application as a platform for attacks against its users and third-party websites. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** | Unencrypted connections have been exploited by attackers to track users, and to inject adverts or malicious JavaScript. | |
| **Evidence/Proof of Concept**  Untitled.png  Fig:HTTPS Not Implemented | | |
| **Recommendation** | Applications should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Forceful Browsing** | **Risk Rating**: Low |
| **Description** | Forceful browsing is an attack technique used to gain access to restricted pages or other sensitive resources in a web server by forcing the URL directly. If the restricted URLs, scripts, or files that reside in the web server directory are not enforced with appropriate authorization, they can be vulnerable to forceful browsing attacks. | |
| **Affected Path(s)** | http://hmfw.ap.gov.in/csip\_test/(S(e0ejqzpo5jtgl35pamjmat1z))/Handler.ashx?id\_Image=\* | |
| **Impact** | If a web server or a web application is vulnerable to forceful browsing attack, an attacker can access restricted files and view sensitive information. | |
| **Evidence/Proof of Concept**  **Step 1:** By Accessing the URLhttp://hmfw.ap.gov.in/csip\_test/(S(e0ejqzpo5jtgl35pamjmat1z))/Handler.ashx?id\_Image=453 the documents viewed without any authentication.  forcefull brow.png | | |
| **Recommendation** | There are two ways to protect against forceful browsing – enforcing an application URL space white list and using proper access control. | |
| **Management Comments** |  | |

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

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Internal File Path Disclosure** | **Risk Rating**: Low |
| **Description** | 1. 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)** |  | |
| **Impact** | 1. 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**  path discloser.JPG  Fig. Internal File Path Disclosure | | |
| **Recommendation** | Don’t disclose the internal file path of server. | |
| **Management Comments** |  | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **Vulnerability Name** | | **Improper Implementation Of Change Password** | | **Risk Rating**: Low |
| **Description** | | 1. the change password Functionality is not implemented correctly | |
| **Affected Path(s)** | | http://hmfw.ap.gov.in/csip\_test/(S(e0ejqzpo5jtgl35pamjmat1z))/CSIChangePassword.aspx | |
| **Impact** | | It helps the attacker to modify the current password after guessing the username and also automate the request for multiple times. | |
| **Evidence/Proof of Concept**  change password page on before login.JPG  Fig .Improper Implementation of change password | | | |
| **Recommendation** | | The change password functionality should be implemented after login | |
| **Management Comments** | |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Input Fields with auto-complete enabled** | **Risk Rating**: Low |
| **Description** | 1. The Web form contains passwords or other sensitive text fields for which the browser auto-complete feature is enabled. Auto-complete stores completed form field and passwords locally in the browser, so that these fields are filled automatically when the user visits the site again. | |
| **Affected Path(s)** |  | |
| **Impact** | 1. Data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. | |
| **Evidence/Proof of Concept**  **autocomplete.png**  Fig . auto-complete enabled | | |
| **Recommendation** | 1. The password auto-complete should be disabled in sensitive applications. 2. To disable auto-complete, you may use a code similar to:   <INPUT TYPE="password" AUTOCOMPLETE="off"> | |
| **Management Comments** |  | |

## Scanned Items

/

/CSIAttachmentLoader.aspx

/CSIGlobalRegPersonal.aspx

/CSIIndianApplicationView.aspx

/csilogin.aspx

/CSIRegistrationLaunch.aspx

/Default.aspx

/FacilityAdminView.aspx

/FacilityServicePreferencesReportView.aspx

/Handler.ashx

/script

/script/datetimepicker\_css.js

/SpecialistsCatalogView.aspx

/SpecialistsPendingAccreditionView.aspx

/ViewAttachments.aspx

## Limitations

1. The report has been prepared based on the information given by Department of Health,Medical & Family Welfare and is accordingly, given for the specific purpose of internal use by the Department of Health,Medical & Family Welfare. 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 Health,Medical & Family Welfare, being the express addressee to this document. Department of Health,Medical & Family Welfare 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 Health,Medical & Family Welfare, 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 Health,Medical & Family Welfare in writing in advance.
3. Without prior permission of Department of Health,Medical & Family Welfare, the contents of this report may not be quoted in whole or in part or otherwise referred to in any documents. The report is for the sole information of Department of Health,Medical & Family Welfare 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 Health,Medical & Family Welfare. Further, any quotation, citation or attribution of this report, or any extract from it, is strictly prohibited without Department of Health,Medical & Family Welfare’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.