Application Security Assessment Report

of

AP Ports,

Department Of Ports,

Govt. of AP

14/11/2019

by

Andhra Pradesh Technology Services

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

Vijayawada – 520 010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc24617427)

[1.1. Introduction 3](#_Toc24617428)

[1.2. Engagement Specific Details 3](#_Toc24617429)

[1.3. Scope Details 3](#_Toc24617430)

[1.3.1. Inclusion 3](#_Toc24617431)

[1.3.2. Exclusion 3](#_Toc24617432)

[1.4. Approach & Methodology 4](#_Toc24617433)

[1.4.1. Information Gathering: 4](#_Toc24617434)

[1.4.2. Automated & Manual Scanning: 4](#_Toc24617435)

[1.4.3. Analyse results and reporting: 4](#_Toc24617436)

[1.5. Risk Categorization 5](#_Toc24617437)

[1.6. Vulnerability Summary 6](#_Toc24617438)

[1.6.1. Distribution of Observation 6](#_Toc24617439)

[2. Detailed Observation 7](#_Toc24617440)

[2.1. Web Application Security Assessment & Penetration Testing 7](#_Toc24617441)

[3. Scanned Items 14](#_Toc24617442)

[4. Limitations 14](#_Toc24617443)

1. Executive Summary

## Introduction

Ports fortify imports and exports. For India, with a vast coastline of over 6000 km, ports are gateways to international trade and commerce. Ports offer tremendous potential for development and growth of a wide spectrum of maritime activities such as international shipping, coastal shipping, ship repairs, fishing, captive ports for specific industries, all weather ports, tourism and sports are 13 major ports and 185 non-major ports all along the coastline of the country.

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Application Security Assessment of AP Ports Application for Department of Ports 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. 12/11/2019 |
| 1. 2. | 1. Submission date of initial report | 1. 14/11/2019 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 14/11/2019 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

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

Application Name: AP Ports

Application URL: http://13.233.40.63/

Environment: UAT

Version Number [or] Latest Compilation Timestamp: Not Provided

Type of Review: Grey box

Hash of Zipped Source Code (SHA512): Not Provided

### Exclusion

1. Server Vulnerability Assessment
2. Secure Code Review
3. Process Review
4. Secure Network Architecture Review

## Approach & Methodology

1. The web application security assessment was conducted in line with the leading security standards and guidelines for web application security such as OWASP.
2. The approach followed for the security assessment is detailed below:

### Information Gathering:

We conducted a walkthrough of the web application to assess the scope of the security assessment and obtain the following information to identify the potential attack vectors:

* 1. Functionalities available in the web application
  2. Entry points for the web application
  3. Web application is custom developed or off-the-shelf application
  4. Protocols used by the web application
  5. Back-end technology including web server, framework, and development language
  6. Conduct search engine discovery and reconnaissance
  7. Banner grabbing (finger printing) to identify the running version of web server / application server and framework
  8. Enumerate application on web server to identify other applications running on the server
  9. View source of the web application to review the comments and metadata
  10. Map functionalities and data flow to identify attack vectors

### Automated & Manual Scanning:

We performed an unauthenticated automated & Manual scanning (without the knowledge of user credentials) of the web application URL using commercial and open source tools. The scanning was conducted to identify any known vulnerabilities in the subjected application.

### Analyse results and reporting:

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

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

## Risk Categorization

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

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

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

The final risk ratings are defined as follows:

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

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

## Vulnerability Summary

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Review Area** | **Initial Review** | | |
| **High** | **Medium** | **Low** |
| **Web Application Security Assessment** | 0 | 1 | 4 |
| **Total** |  | | **5** |

### 

### 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://13.233.40.63/#/contact-us | |
| **Impact** | Attackers could repeatedly exercise web site functionality attempting to exploit or defraud the system. An automated robot could potentially execute thousands of requests a minute, causing potential loss of performance or service. | |
| **Evidence/Proof of Concept**  **Step 1:** Captcha not implemented.  captcha not implemented.png | | |
| **Recommendation** | It is recommended to implement captcha on Contact Us page. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Version Disclosure** | **Risk Rating**: Low |
| **Description** | The HTTP responses returned by this web application include a header named **Server**. This value of this header includes the version of server nginx. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** | The HTTP header may disclose sensitive information. This information can be used to launch further attacks. | |
| **Evidence/Proof of Concept**  **Step 1:** Application discloses the server version details in response headers.  version disclosure.png | | |
| **Recommendation** | Add the following line to your nginx.conf file to prevent information leakage from the SERVER header of its HTTP response:  **server\_tokens off** | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Cross-origin Resource Sharing** | **Risk Rating**: Low |
| **Description** | The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request. If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk. Since the Vary: Origin header was not present in the response, reverse proxies and intermediate servers may cache it. This may enable an attacker to carry out cache poisoning attacks. | |
| **Affected Path(s)** | (/Web Sever) | |
| **Impact** | If another domain is allowed by the policy, then that domain can potentially attack users of the application. If a user is logged in to the application, and visits a domain allowed by the policy, then any malicious content running on that domain can potentially retrieve content from the application, and sometimes carry out actions within the security context of the logged in user. | |
| **Evidence/Proof of Concept**  **cors.png** | | |
| **Recommendation** | Any inappropriate domains should be removed from the CORS policy. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **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. Spambot programs look for strings like myname@mydomain.com and then record any addresses found. | |
| **Affected Path(s)** | http://13.233.40.63/#/contact-us  http://13.233.40.63/#/boardmembers | |
| **Impact** | Email addresses posted on Web sites may attract spam. | |
| **Evidence/Proof of Concept**  **email.png**  Fig. Email Address disclosure | | |
| **Recommendation** | Obfuscate email address by replacing **’@‘**with [at] and **‘.’** with [dot]. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Content Security Policy not Implemented** | **Risk Rating**: Low |
| **Description** | It is observed that the application is missing CSP directives in the response header. Content Security Policy (CSP) is an important standard by the W3C that is aimed to prevent a broad range of content injection attacks such as cross-site scripting (XSS). Content Security Policy (CSP) is an effective "defence in depth" technique to be used against content injection attacks. It is a declarative policy that informs the user agent what are valid sources to load from. | |
| **Affected Path(s)** | (/Web Server) | |
| **Impact** | There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. | |
| **Evidence/Proof of Concept**  **csp not implemented.png**  Fig. Content Security Policy header not implemented | | |
| **Recommendation** | Enable CSP on your website by sending the Content-Security-Policy in HTTP response headers that instruct the browser to apply the policies you specified. | |
| **Management Comments** |  | |

## Scanned Items

http://13.233.40.63/

http://13.233.40.63/images

http://13.233.40.63/images/anchorage

http://13.233.40.63/images/anchorage/DSC\_1\_tn.jpg

http://13.233.40.63/images/maps

http://13.233.40.63/images/maps/industrial-corridor\_tn.jpg

http://13.233.40.63/js

http://13.233.40.63/js/app.min.js

http://13.233.40.63/js/templates.min.js

http://13.233.40.63/js/vendor.min.js

## Limitations

1. The report has been prepared based on the information given by department Of Ports and is accordingly, given for the specific purpose of internal use by the department Of Ports. 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 Ports, being the express addressee to this document. department Of Ports 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 Ports, 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 Ports in writing in advance.
3. Without prior permission of department Of Ports, 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 Ports 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 Ports. Further, any quotation, citation or attribution of this report, or any extract from it, is strictly prohibited without department Of Port’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.