Cyber Security Assessment Report

of

District EoDB,

Department of Industries,

Govt. of AP

06/03/2020

by

Andhra Pradesh Technology Services

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

Vijayawada – 520 010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc34400449)

[1.1. Introduction 3](#_Toc34400450)

[1.2. Engagement Specific Details 3](#_Toc34400451)

[1.3. Scope Details 4](#_Toc34400452)

[1.3.1. Inclusion 4](#_Toc34400453)

[1.3.2. Exclusion 4](#_Toc34400454)

[1.4. Approach & Methodology 5](#_Toc34400455)

[1.4.1. Information Gathering: 5](#_Toc34400456)

[1.4.2. Automated & Manual Scanning: 5](#_Toc34400457)

[1.4.3. Analyse results and reporting: 5](#_Toc34400458)

[1.5. Risk Categorization 6](#_Toc34400459)

[1.6. Vulnerability Summary 7](#_Toc34400460)

[1.6.1. Distribution of Observation 7](#_Toc34400461)

[2. Detailed Observation 8](#_Toc34400462)

[2.1. Web Application Security Assessment & Penetration Testing 8](#_Toc34400463)

[3. Scanned Items 15](#_Toc34400464)

[4. Limitations 15](#_Toc34400465)

1. Executive Summary

## Introduction

The Department of Industries and Commerce is primarily responsible for the development of industries in general and small-scale industries in particular. The Department also plans and implements various schemes for industrial development in the State.

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Cyber Security Assessment of DistrictEoDB Application for Department of Industries 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. 05/03/2020 |
| 1. 2. | 1. Submission date of initial report | 1. 07/03/2020 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 06/03/2020 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

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

Application Name: District EoDB

Application URL: http://125.17.121.166:8080/DistrictEoDB/Login.aspx

Environment: UAT

Version Number [or] Latest Compilation Timestamp: Not Provided

Type of Review: Blackbox

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 a black-box 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 | 3 | 3 |
| **Total** |  | | **6** |

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Improper Error Handling** | **Risk Rating**: Medium |
| **Description** | Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (hacker). These messages reveal implementation details that should never be revealed. Such details can provide hackers important clues on potential flaws in the site and such messages are also disturbing to normal users. | |
| **Affected Path(s)** | / (Throughout the application) | |
| **Impact** | An attacker makes use of the details found to perform the concentrated attacks based on the vulnerabilities present in the current version. | |
| **Evidence/Proof of Concept**  A screenshot of a computer screen  Description automatically generated  **Figure:** Error page disclosing the server version and stack trace errors. | | |
| **Recommendation** | Ensure that the pages which are disclosing error or warning messages should be properly configured to log errors to a file instead of displaying the error to the user. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **User Credentials are Sent in clear text** | **Risk Rating**: Medium |
| **Description** | User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users. | |
| **Affected Path(s)** | http://125.17.121.166:8080/DistrictEoDB/Login.aspx | |
| **Impact** | A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection | |
| **Evidence/Proof of Concept**  **Step1:**By capturing the request it is observed that the user credentials are sent in plain text as shown in image  A screenshot of a computer  Description automatically generated | | |
| **Recommendation** | It is recommended to:  The application should use transport-level encryption (SSL or TLS) to protect all sensitive communications passing between the client and the server. Communications that should be protected include the login mechanism and related functionality, and any functions where sensitive data can be accessed, or privileged actions can be performed. These areas of the application should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.  Reference Link-  https://www.owasp.org/index.php/Testing\_for\_Credentials\_Transported\_over\_an\_Encrypted  \_Channel | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 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://125.17.121.166:8080/DistrictEoDB/Login.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:** In the login page of the application the captcha is not implemented as shown below.  **A screenshot of a video game  Description automatically generated** | | |
| **Recommendation** | It is recommended to implement captcha.  Reference Links:  [http://www.captcha.net](http://www.captcha.net/) | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Password type input with auto-complete enabled** | **Risk Rating**: Low |
| **Description** | If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application. The stored credentials can be captured by an attacker who gains control over the user's computer. | |
| **Affected Path(s)** | http://125.17.121.166:8080/DistrictEoDB/Login.aspx | |
| **Impact** | Possible sensitive information disclosure. | |
| **Evidence/Proof of Concept**  **Step 1**: in the application It is observed that the input fields are enabled with auto complete as shown in below image.  A screenshot of a computer  Description automatically generated | | |
| **Recommendation** | To prevent browsers from storing credentials entered into HTML forms, include the attribute **auto complete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).  Reference Link: http://www.owasp.org/index.php/Testing\_for\_Vulnerable\_Remember\_Password\_(OTG-AUTHN-005) | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Content Security Policy not implemented** | **Risk Rating**: Medium |
| **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)** | /(WebServer) | |
| **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**  **Step 1:** the security headers are not implemented as shown in below image.  A screenshot of a social media post  Description automatically generated | | |
| **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.  Reference Links:  https://www.owasp.org/index.php/Content\_Security\_Policy\_Cheat\_Sheet  https://stackoverflow.com/questions/37992225/config-your-iis-server-to-use-the-content-security-policy-header  https://content-security-policy.com  https://www.ryadel.com/en/iis-web-config-secure-http-response-headers-pass-securityheaders-io-scan/ | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Version Disclosure** | **Risk Rating**: Low |
| **Description** | The error pages is returned by this web application include a header named version information reveals asp.net version. It is not necessary for production sites and should be disabled. | |
| **Affected Path(s)** | / (Web Server) | |
| **Impact** | The error pages is disclosing sensitive information. This information can be used to launch further attacks. | |
| **Evidence/Proof of Concept**  **Step 1:** The version of server that is being used are disclosed as shown in image.  A screenshot of a social media post  Description automatically generated | | |
| **Recommendation** | make sure that the technology /version number being used is not disclosed in any manner and redirect to custom error pages | |
| **Management Comments** |  | |

## Scanned Items

/

/Index.aspx

/js

/js/circle-progress.js

/js/jquery.backtotop.js

/js/jquery.flexslider-min.js

/js/jquery.mobilemenu.js

/Login.aspx

/Logout.aspx

/WebResource.axd

## Limitations

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