Cyber Security Assessment Report

of

Application Name,

Department Name,

Govt. of AP

Dated

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

1. [One Liner about the Department]

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Cyber Security Assessment of\_\_\_\_\_\_\_\_\_\_\_ Application for \_\_\_\_\_\_\_\_\_ 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. DD/MM/YYYY |
| 1. 2. | 1. Submission date of initial report | 1. DD/MM/YYYY |
| 1. 3. | 1. Submission date of Final Confirmatory Review Report | 1. DD/MM/YYYY |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | 1. Name, Name | 1. Name | 1. Department |
| 1. 2. | 1. Server Vulnerability Assessment | 1. Name, Name | 1. Name | 1. Department |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. DD/MM/YYYY | 1. v1.0 | 1. Initial Review |
| 1. 2. | 1. DD/MM/YYYY | 1. v1.1 | 1. Confirmatory Security Review #1 |

## Scope Details

### Inclusion

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

Application Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Application URL: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Environment: Production/UAT/SIT

Version Number [or] Latest Compilation Timestamp: \_\_\_\_\_\_\_\_

Type of Review: Blackbox / Greybox

Hash of Zipped Source Code (SHA512):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Server Vulnerability Assessment**

Type of Review: Blackbox / Greybox

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No.** | **IP Address** | **OEM** | **Version No.** | **Server Type** |
| 1. | 192.168.10.2 | RHEL | 7.4 | Web Server |
| 2. | NGINX | 1.12.2 |
| 3. | 192.168.11.2 | RHEL | 7.4 | App Server |
| 4. | GUNICORN | 19.6.0 |
| 5. | 192.168.12.2 | RHEL | 7.4 | DB Server |
| 6. | ORACLE | 12c |

### Exclusion

[If any]

1. Application Security Assessment
2. Server Vulnerability Assessment
3. Secure Code Review
4. Process Review
5. 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/ 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** | | |
| **High** | **Medium** | **Low** |
| **Web Application Security Assessment** | 1 | 2 | 3 |
| **Server Vulnerability Assessment** | 4 | 5 | 6 |
| **Total** | **5** | **7** | **9** |
|  |  | **21** |

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Directory Listing** | **Risk Rating**: Medium |
| **Description** | The web server is configured to display the list of files contained in this directory. This is not recommended because the directory may contain files that are not normally exposed through links on the web site. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** | A user can view a list of all files from this directory possibly exposing sensitive information. | |
| **Evidence/Proof of Concept**  [Evidence & Screenshots] | | |
| **Recommendation** | There is not usually any good reason to provide directory listings, and disabling them may place additional hurdles in the path of an attacker. This can normally be achieved in two ways:   * Configure your web server to prevent directory listings for all paths beneath the web root; * Place into each directory a default file (such as index.htm) that the web server will display instead of returning a directory listing. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Click jacking** | **Risk Rating**: Low |
| **Description** | Click jacking 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. | |
| **Affected Path(s)** | /(Web Server) | |
| **Impact** | An attacker can host this domain in other evil site by using iframe and if a user fills the given field it can directly redirect as logs to attacker and after its redirect to your web server. Leading to steal user information too and use that host site as phishing of your site its CSRF and Click jacking. | |
| **Evidence/Proof of Concept**  [Evidence & Screenshots] | | |
| **Recommendation** | 1. Sites can use X-Frame-Options to avoid clickjacking 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. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Insufficient Anti-Automation** | **Risk Rating**: [Risk Rating] |
| **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)** | URL1 – Parameter 1, URL2 – Parameter 1&2 | |
| **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**  [Evidence & Screenshots] | | |
| **Recommendation** | It is recommended to implement captcha.  Reference Links:  [http://www.captcha.net](http://www.captcha.net/) | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Word Press XML-RPC authentication brute force** | **Risk Rating**: Medium |
| **Description** | Word Press provides an XML-RPC interface via the xmlrpc.php script. XML-RPC is remote procedure calling using HTTP as the transport and XML as the encoding. An attacker can abuse this interface to brute force authentication credentials using API calls such as **wp.getUsersBlogs**. | |
| **Affected Path(s)** | URL1 – Parameter 1, URL2 – Parameter 1&2 | |
| **Impact** | By using the xmlrpc file the attacker can perform the attacks like bruteforce attacks and XSPA or simply port scanning etc. | |
| **Evidence/Proof of Concept**  **Step 1:** | | |
| **Recommendation** | It is possible to disable the XML-RPC script if you do not want to use it. Consult references for a Word Press plug-in that does that. If you don't want to disable XML-RPC you can monitor for XML-RPC authentication failures with a Web Application Firewall like ModSecurity.  Reference link:  https://wordpress.org/plugins/prevent-xmlrpc/  https://isc.sans.edu/diary/+WordPress+brute+force+attack+via+wp.getUsersBlogs/18427 | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Word Press Admin Console Available to End user** | **Risk Rating**: High |
| **Description** | The application discloses Word Press admin console to end-user and Word Press doesn’t limit the number of login attempts, so brute force attacks can be very effective.and | |
| **Affected Path(s)** | URL1 – Parameter 1, URL2 – Parameter 1&2 | |
| **Impact** | Brute force attacks can be possible on the login page which may lead to the complete takeover of the website and can also change the design and layout of the website. | |
| **Evidence/Proof of Concept**  [Evidence & Screenshots] | | |
| **Recommendation** | The best defence against this vulnerability is installing a plug-in that will limit the number of allowed login attempts, such as iThemes Security Pro. You can also use a password manager to generate random passwords that are much less likely to be guessed. Stay away from passwords that seem obvious — don’t use anything like 123456, password, or anything related to you. | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | Email Id Disclosure | **Risk Rating**: [Risk Rating] |
| **Description** | [Description about the subjected Vulnerability] | |
| **Affected Path(s)** | URL1 – Parameter 1, URL2 – Parameter 1&2 | |
| **Impact** | [Potential Impact] | |
| **Evidence/Proof of Concept**  [Evidence & Screenshots] | | |
| **Recommendation** | [Recommendation steps & reference links] | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Default Login Credentials for Word Press Admin Console** | **Risk Rating**: [Risk Rating] |
| **Description** | [Descriptiolmn about the subjected Vulnerability] | |
| **Affected Path(s)** | URL1 – Parameter 1, URL2 – Parameter 1&2 | |
| **Impact** | [Potential Impact] | |
| **Evidence/Proof of Concept**  [Evidence & Screenshots] | | |
| **Recommendation** | [Recommendation steps & reference links] | |
| **Management Comments** |  | |

## Scanned Items

## Limitations

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