Cyber Security Assessment Report

of

arch museums ,

Department of Archaeology & Museums,

Govt. of AP

05/09/2019

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

1. [One Liner about the Department]

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Cyber Security Assessment of arch museums Application for Department of Archaeology & Museums 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. 05/09/2019 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | 1. APTS TEAM | 1. Name | 1. Department of Archaeology & Museums |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 05/09/2019 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

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

Application Name: arch museums

Application URL: http://aparchmuseums.nic.in/

Environment: Production

Type of Review: Blackbox

## 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 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 | 3 | 1 |
| **Total** |  | | **21** |

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | Possibility of sql injection | **Risk Rating**: High |
| **Description** | SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. | |
| **Affected Path(s)** | http://aparchmuseums.nic.in/wp-login.php | |
| **Impact** | An attacker can use SQL injection it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further. | |
| **Evidence/Proof of Concept**  **Step 1:** Access the URL http://aparchmuseums.nic.in/wp-login.php and capture the request and perform the sql injection attack on the parameters in the request and by using the injectable parameter the database information can be retrieved as shown below:  sql.JPG | | |
| **Recommendation** | Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection  Reference Links:  https://dzone.com/articles/aspnet-preventing-sql-injectio  https://www.aspsnippets.com/Articles/SQL-Injection-Attack-its-examples-and-Prevention-mechanisms-and-Techniques-in-ASPNet.aspx  https://stackoverflow.com/questions/305044/how-can-i-avoid-sql-injection-attacks-in-my-asp-net-application | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Username Enumeration** | **Risk Rating**: Low |
| **Description** | User enumeration is found in any system that requires user authentication and malicious actor can use brute-force to either guess or confirm valid user names in a system. | |
| **Affected Path(s)** | http://aparchmuseums.nic.in/wp-login.php | |
| **Impact** | The information obtained can be used by an attacker to gain a list of users on system. This information can be used to attack the web application, for example, through a brute force or default username/password attack. | |
| **Evidence/Proof of Concept**  Step 1: access the login page of the URL http://aparchmuseums.nic.in/wp-login.php and provide different usernames and password combination which is generating the error as shown below:  Capture.JPG | | |
| **Recommendation** | There are several options available that will help you boost the security of your Word Press login page. You can authentication or you can implement [two-factor authentication for Word Press](https://www.wpwhitesecurity.com/wordpress-security/two-factor-authentication-wordpress/). We can also use the different plug-in available in word press. | |
| **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://aparchmuseums.nic.in/?page\_id=25 | |
| **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 contact us page of the application the captcha is not implemented as shown below, the attacker can take advantage of this and can send the continuous fake request  **Captcha.JPG** | | |
| **Recommendation** | It is recommended to implement captcha.  References Links:  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)** | http://aparchmuseums.nic.in/xmlrpc.php | |
| **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:** By accessing the URLhttp://aparchmuseums.nic.in/xmlrpc.php we can access the xmlrpc file  xml1.JPG | | |
| **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. | |
| **Affected Path(s)** | http://aparchmuseums.nic.in/wp-login.php | |
| **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**  **Step1:** By Accessing the URL https://www.apcob.org/wp-login.php,the word press login page can be accessed as shown in the image.  wp-admin.JPG | | |
| **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** |  | |

## Scanned Items

http://aparchmuseums.nic.in

## Limitations

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