Cyber Security Assessment Report

of

Science City Of Andhra Pradesh,

Energy, Infrastructure & Investments Department(EIID),

Govt. of AP

Dated 12/07/2019

by

Andhra Pradesh Technology Services

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

Vijayawada – 520 010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc13835707)

[1.1. Introduction 3](#_Toc13835708)

[1.2. Engagement Specific Details 3](#_Toc13835709)

[1.3. Scope Details 4](#_Toc13835710)

[1.3.1. Inclusion 4](#_Toc13835711)

[1.3.2. Exclusion 4](#_Toc13835712)

[1.4. Approach & Methodology 5](#_Toc13835713)

[1.4.1. Information Gathering: 5](#_Toc13835714)

[1.4.2. Automated & Manual Scanning: 5](#_Toc13835715)

[1.4.3. Analyse results and reporting: 5](#_Toc13835716)

[1.5. Risk Categorization 5](#_Toc13835717)

[1.6. Vulnerability Summary 7](#_Toc13835718)

[1.6.1. Distribution of Observation 7](#_Toc13835719)

[2. Detailed Observation 8](#_Toc13835720)

[2.1. Web Application Security Assessment & Penetration Testing 8](#_Toc13835721)

[3. Appendix 16](#_Toc13835722)

[3.1. OWASP Checklist 16](#_Toc13835723)

[4. Scanned Items 20](#_Toc13835724)

[5. Limitations 21](#_Toc13835725)

1. Executive Summary

## Introduction

1. Science City acts as a Hub for inter-disciplinary science & technology, develop Science Popularization Programs, maintain Alliance with top-tier Global Universities and Companies, start Science Instrumentation, Science Policy, Science Journalism other Educational & Skill Development Programs.
2. Andhra Pradesh Technology Services (hereon referred as APTS) performed the Cyber Security Assessment of AP Science City Application for Energy, Infrastructure & Investments Departmentto 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. 11/07/2019 |
| 1. 2. | 1. Submission date of initial report | 1. 12/07/2019 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | APTS TEAM |  | Energy, Infrastructure & Investments Department |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 12/07/2018 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

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

Application Name: AP Science City Application URL:

Application URL: https://tptuat.aponline.gov.in/APScience

Environment: Staging Server

Version Number [or] Latest Compilation Timestamp: Not provided

Type of Review: Blackbox

Hash of Zipped Source Code (SHA512): Not Provided

User Accounts Tested:Not Applicable

### 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 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 | 3 |
| **Total** |  |  | **4** |
|

### Distribution of Observation

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 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)** | https://tptuat.aponline.gov.in/APscience | |
|  | Tricking the user to click on the link by framing the original page and showing a layer on top of it with dummy buttons which leads to Phishing attack | |
| **Evidence/Proof of Concept**  The website can be loaded in the iframe    Fig. click jacking code    Fig. click jacking | | |
| **Recommendation** | Sites can use X-Frame-Options to avoid click jacking 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. | |

|  |  |  |
| --- | --- | --- |
| 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)** | https://tptuat.aponline.gov.in/APscience/Feedback.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**  In the feedback form the captcha is not implemented  automation.png  Fig. Insufficient Anti Automation | | |
| **Recommendation** | It is recommended to implement captcha.  <http://www.captcha.net>  <http://projects.webappsec.org/w/page/13246938/Insufficient%20Anti-automation> | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Email Id Disclosure** | **Risk Rating**: Low |
| **Description** | During assessment, we found the email ids in web page and documents which is not a good practice suggested by the OWASP community. The mail ids displayed here are not any generic ones (ex: helpdesk@gmail.com) rather they belong to the respective individuals based on their designation.  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. Spam bot programs look for strings like myname@mydomain.com and then record any addresses found. | |
| **Affected Path(s)** | https://tptuat.aponline.gov.in/APScience/Home.aspx  https://tptuat.aponline.gov.in/APScience/Documents/Tender/JRF%20Brocher-1.jpg  https://tptuat.aponline.gov.in/APScience/Documents/Tender/KA-Modified-RFP-DMP-ScienceCityofAPasJul202018(2filesmerged).pdf | |
| **Impact** | Disclosing the individual mail ids sometimes lead to social engineering attacks and often affected with the spam mails. However, email addresses of developers and other individuals (whether appearing on-screen or hidden within page source) may disclose information that is useful to an attacker; for example, they may represent usernames that can be used at the application's login. | |
| **Evidence/Proof of Concept**  email.png  Fig. Email Address disclosure | | |
| **Recommendation** | 1. Obfuscate email address or Spell out email addresses(Please enclose the email address with example [at] gmail [dot] com)   Refer:  https://stackoverflow.com/questions/748780/best-way-to-obfuscate-an-e-mail-address-on-a-website  https://stackoverflow.com/questions/11563283/why-write-at-and-dot-in-email-rather-than-and  https://academia.stackexchange.com/questions/55612/why-do-people-in-academia-tend-to-write-their-email-address-with-dot-at  https://stackoverflow.com/questions/483212/effective-method-to-hide-email-from-spam-bots | |
| **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Name** | **Technology/Version Disclosure** | **Risk Rating**: Low |
| **Description** | The HTTP responses returned by this web application include a header named Server reveals Microsoft version. This information is ignored by most people, with the exception of hackers, who use this information to launch targeted attacks against your web server and version. It is not necessary for production sites and should be disabled. | |
| **Affected Path(s)** | https://tptuat.aponline.gov.in/APscience | |
| **Impact** | The HTTP header may disclose sensitive information. This information can be used to launch further attacks. | |
| **Evidence/Proof of Concept**  TECHNOLOGY VERSION DISCLOSER.png  Fig. technology or version disclosure | | |
| **Recommendation** | Remove unwanted HTTP Headers like Server etc.,  Reference:  https://www.saotn.org/remove-iis-server-version-http-response-header/  https://scotthelme.co.uk/hardening-your-http-response-headers/  https://cwe.mitre.org/data/definitions/200.html  https://www.saotn.org/remove-iis-server-version-http-response-header/  https://github.com/aspnet/Hosting/issues/571  https://www.tunetheweb.com/security/http-security-headers/server-header/  https://www.tecmint.com/hide-apache-web-server-version-information/ | |
| **Management Comments** |  | |

1. Appendix

## OWASP Checklist

The Application Security Assessment has been evaluated as per Open Web Application Security Project Testing guide v4.0 as follows:

| **Ref. No.** | | **Category** | | **Test Name** | **Safe?** | **Remarks** |
| --- | --- | --- | --- | --- | --- | --- |
| 1.1 | | **Information Gathering** | | | | |
| 1.1.1 | | OTG-INFO-001 | | Conduct Search Engine Discovery and Reconnaissance for Information Leakage | Yes | Tested Not Vulnerable |
| 1.1.2 | | OTG-INFO-002 | | Fingerprint Web Server | No | Refer the vulnerability reported in 2.1 |
| 1.1.3 | | OTG-INFO-003 | | Review Web server Metafiles for Information Leakage | Yes | Tested Not Vulnerable |
| 1.1.4 | | OTG-INFO-004 | | Enumerate Applications on Web server | No | Refer the vulnerability reported in 2.1 |
| 1.1.5 | | OTG-INFO-005 | | Review Webpage Comments and Metadata for Information Leakage | Yes | Tested Not Vulnerable |
| 1.1.6 | | OTG-INFO-006 | | Identify application entry points | Yes | Tested Not Vulnerable |
| 1.1.7 | | OTG-INFO-007 | | Map execution paths through application | Yes | Tested Not Vulnerable |
| 1.1.8 | | OTG-INFO-008 | | Fingerprint Web Application Framework | Yes | Tested Not Vulnerable |
| 1.1.9 | | OTG-INFO-009 | | Fingerprint Web Application | No | Refer the vulnerability reported in 2.1 |
| 1.1.10 | | OTG-INFO-010 | | Map Application Architecture | NA | Not Applicable |
| 1.2 | | **Configuration and Deploy Management Testing** | | | | |
| 1.2.1 | | OTG-CONFIG-001 | | Test Network/Infrastructure Configuration | NA | Not Applicable |
| 1.2.2 | | OTG-CONFIG-002 | | Test Application Platform Configuration | NA | Not Applicable |
| 1.2.3 | | OTG-CONFIG-003 | | Test File Extensions Handling for Sensitive Information | Yes | Tested Not Vulnerable |
| 1.2.4 | | OTG-CONFIG-004 | | Backup and Unreferenced Files for Sensitive Information | Yes | Tested ,not vulnerable |
| 1.2.5 | | OTG-CONFIG-005 | | Enumerate Infrastructure and Application Admin Interfaces | Yes | Tested Not Vulnerable |
| 1.2.6 | | OTG-CONFIG-006 | | Test HTTP Methods | Yes | Tested Not Vulnerable |
| 1.2.7 | | OTG-CONFIG-007 | | Test HTTP Strict Transport Security | Yes | Strict Transport Security policy implemented |
| 1.2.8 | | OTG-CONFIG-008 | | Test RIA cross domain policy | No | Cross-domain policy page not found |
| 1.3 | | **Identity Management Testing** | | | | |
| 1.3.1 | | OTG-IDENT-001 | | Test Role Definitions | NA | Not Applicable |
| 1.3.2 | | OTG-IDENT-002 | | Test User Registration Process | NA | Not Applicable |
| 1.3.3 | | OTG-IDENT-003 | | Test Account Provisioning Process | NA | Not Applicable |
| 1.3.4 | | OTG-IDENT-004 | | Testing for Account Enumeration and Guessable User Account | NA | Not Applicable |
| 1.3.5 | | OTG-IDENT-005 | | Testing for Weak or unenforced username policy | NA | Not Applicable |
| 1.3.6 | | OTG-IDENT-006 | | Test Permissions of Guest/Training Accounts | NA | Not Applicable |
| 1.3.7 | | OTG-IDENT-007 | | Test Account Suspension/Resumption Process | NA | Not Applicable |
| 1.4 | **Authentication Testing** | | | | | |
| 1.4.1 | OTG-AUTHN-001 | | | Testing for Credentials Transported over an Encrypted Channel | NA | Not Applicable |
| 1.4.2 | OTG-AUTHN-002 | | | Testing for default credentials | NA | Not Applicable |
| 1.4.3 | OTG-AUTHN-003 | | | Testing for Weak lock out mechanism | NA | Not Applicable |
| 1.4.4 | OTG-AUTHN-004 | | | Testing for bypassing authentication schema | NA | Not Applicable |
| 1.4.5 | OTG-AUTHN-005 | | | Test remember password functionality | NA | Not Applicable |
| 1.4.6 | OTG-AUTHN-006 | | | Testing for Browser cache weakness | NA | Not Applicable |
| 1.4.7 | OTG-AUTHN-007 | | | Testing for Weak password policy | NA | Not Applicable |
| 1.4.8 | OTG-AUTHN-008 | | | Testing for Weak security question/answer | NA | Not Applicable |
| 1.4.9 | OTG-AUTHN-009 | | | Testing for weak password change or reset functionalities | NA | Not Applicable |
| 1.4.10 | OTG-AUTHN-010 | | | Testing for Weaker authentication in alternative channel | NA | Not Applicable |
| 1.5 | **Authorization Testing** | | | | | |
| 1.5.1 | OTG-AUTHZ-001 | | | Testing Directory traversal/file include | No | Tested Not Vunlerable |
| 1.5.2 | OTG-AUTHZ-002 | | | Testing for bypassing authorization schema | Yes | Tested Not Vulnerable |
| 1.5.3 | OTG-AUTHZ-003 | | | Testing for Privilege Escalation | Yes | Tested Not Vulnerable |
| 1.5.4 | OTG-AUTHZ-004 | | | Testing for Insecure Direct Object References | Yes | Tested Not Vulnerable |
| 1.6 | **Session Management Testing** | | | | | |
| 1.6.1 | OTG-SESS-001 | | | Testing for Bypassing Session Management Schema | NA | Not Applicable |
| 1.6.2 | OTG-SESS-002 | | | Testing for Cookies attributes | Yes | Tested Not Vulnerable |
| 1.6.3 | OTG-SESS-003 | | | Testing for Session Fixation | NA | Not Applicable |
| 1.6.4 | OTG-SESS-004 | | | Testing for Exposed Session Variables | Yes | Tested Not Vulnerable |
| 1.6.5 | OTG-SESS-005 | | | Testing for Cross Site Request Forgery | NA | Not Applicable |
| 1.6.6 | OTG-SESS-006 | | | Testing for logout functionality | Yes | Not Applicable |
| 1.6.7 | OTG-SESS-007 | | | Test Session Timeout | Yes | Not Applicable |
| 1.6.8 | OTG-SESS-008 | | | Testing for Session puzzling | NA | Not Applicable |
| 1.7 | **Data Validation Testing** | | | | | |
| 1.7.1 | OTG-INPVAL-001 | | | Testing for Reflected Cross Site Scripting | Yes | Tested Not Vulnerable |
| 1.7.2 | OTG-INPVAL-002 | | | Testing for Stored Cross Site Scripting | Yes | Tested Not Vulnerable |
| 1.7.3 | OTG-INPVAL-003 | | | Testing for HTTP Verb Tampering | Yes | Tested Not Vulnerable |
| 1.7.4 | OTG-INPVAL-004 | | | Testing for HTTP Parameter pollution | Yes | Tested Not Vulnerable |
| 1.7.5 | OTG-INPVAL-005 | | | Testing for SQL Injection | Yes | Tested Not Vulnerable |
| 1.7.5.1 |  | | | Oracle Testing | Yes | Tested Not Vulnerable |
| 1.7.5.2 |  | | | MySQL Testing | Yes | Tested Not Vulnerable |
| 1.7.5.3 |  | | | SQL Server Testing | Yes | Tested Not Vulnerable |
| 1.7.5.4 |  | | | Testing PostgreSQL | Yes | Tested Not Vulnerable |
| 1.7.5.5 |  | | | MS Access Testing | Yes | Tested Not Vulnerable |
| 1.7.5.6 |  | | | Testing for NoSQL injection | Yes | Tested Not Vulnerable |
| 1.7.6 | OTG-INPVAL-006 | | | Testing for LDAP Injection | NA | Not Applicable |
| 1.7.7 | OTG-INPVAL-007 | | | Testing for ORM Injection | NA | Not Applicable |
| 1.7.8 | OTG-INPVAL-008 | | | Testing for XML Injection | NA | No XML Pages |
| 1.7.9 | OTG-INPVAL-009 | | | Testing for SSI Injection | Yes | Tested Not Vulnerable |
| 1.7.10 | OTG-INPVAL-010 | | | Testing for XPath Injection | Yes | Tested Not Vulnerable |
| 1.7.11 | OTG-INPVAL-011 | | | IMAP/SMTP Injection | NA | Not Applicable |
| 1.7.12 | OTG-INPVAL-012 | | | Testing for Code Injection | NA | Not Applicable |
| 1.7.12.1 |  | | | Testing for Local File Inclusion | NA | Not Applicable |
| 1.7.12.2 |  | | | Testing for Remote File Inclusion | NA | Not Applicable |
| 1.7.13 | OTG-INPVAL-013 | | | Testing for Command Injection | Yes | Tested Not Vulnerable |
| 1.7.14 | OTG-INPVAL-014 | | | Testing for Buffer overflow | NA | Not Applicable |
| 1.7.14.1 |  | | | Testing for Heap overflow | NA | Not Applicable |
| 1.7.14.2 |  | | | Testing for Stack overflow | NA | Not Applicable |
| 1.7.14.3 |  | | | Testing for Format string | Yes | Tested Not Vulnerable |
| 1.7.15 | OTG-INPVAL-015 | | | Testing for incubated vulnerabilities | Yes | Tested Not Vulnerable |
| 1.7.16 | OTG-INPVAL-016 | | | Testing for HTTP Splitting/Smuggling | Yes | Tested Not Vulnerable |
| 1.8 | **Error Handling** | | | | | |
| 1.8.1 | OTG-ERR-001 | | | Analysis of Error Codes | Yes | Tested Not Vulnerable |
| 1.8.2 | OTG-ERR-002 | | | Analysis of Stack Traces | Yes | Tested Not Vulnerable |
| 1.9 | **Cryptography** | | | | | |
| 1.9.1 | OTG-CRYPST-001 | | | Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection | No | Refer the vulnerability reported in 2.2 |
| 1.9.2 | OTG-CRYPST-002 | | | Testing for Padding Oracle | Yes | Tested Not Vulnerable |
| 1.9.3 | OTG-CRYPST-003 | | | Testing for Sensitive information sent via unencrypted channels | Yes | Tested Not Vulnerable. |
| 1.1 | **Business Logic Testing** | | | | | |
| 1.10.1 | OTG-BUSLOGIC-001 | | Test Business Logic Data Validation | | Yes | Tested Not Vulnerable |
| 1.10.2 | OTG-BUSLOGIC-002 | | Test Ability to Forge Requests | | Yes | Tested Not Vulnerable |
| 1.10.3 | OTG-BUSLOGIC-003 | | Test Integrity Checks | | Yes | Tested Not Vulnerable |
| 1.10.4 | OTG-BUSLOGIC-004 | | Test for Process Timing | | NA | Not Applicable |
| 1.10.5 | OTG-BUSLOGIC-005 | | Test Number of Times a Function Can be Used Limits | | Yes | Tested Not Vulnerable |
| 1.10.6 | OTG-BUSLOGIC-006 | | Testing for the Circumvention of Work Flows | | Yes | Tested Not Vulnerable |
| 1.10.7 | OTG-BUSLOGIC-007 | | Test Defenses Against Application Mis-use | | Yes | Tested Not Vulnerable |
| 1.10.8 | OTG-BUSLOGIC-008 | | Test Upload of Unexpected File Types | | NA | Not Applicable |
| 1.10.9 | OTG-BUSLOGIC-009 | | Test Upload of Malicious Files | | NA | Not Applicable |
| 1.11 | **Client Side Testing** | | | | | |
| 1.11.1 | OTG-CLIENT-001 | | Testing for DOM based Cross Site Scripting | | No | Tested Not Vulnerable. |
| 1.11.2 | OTG-CLIENT-002 | | Testing for JavaScript Execution | | No | Tested Not Vulnerable. |
| 1.11.3 | OTG-CLIENT-003 | | Testing for HTML Injection | | Yes | Tested Not Vulnerable |
| 1.11.4 | OTG-CLIENT-004 | | Testing for Client Side URL Redirect | | Yes | Tested Not Vulnerable |
| 1.11.5 | OTG-CLIENT-005 | | Testing for CSS Injection | | Yes | Tested Not Vulnerable |
| 1.11.6 | OTG-CLIENT-006 | | Testing for Client Side Resource Manipulation | | Yes | Tested Not Vulnerable |
| 1.11.7 | OTG-CLIENT-007 | | Test Cross Origin Resource Sharing | | Yes | Tested Not Vulnerable |
| 1.11.8 | OTG-CLIENT-008 | | Testing for Cross Site Flashing | | NA | Not Applicable |
| 1.11.9 | OTG-CLIENT-009 | | Testing for Clickjacking | | No | Tested Not Vulnerable |
| 1.11.10 | OTG-CLIENT-010 | | Testing WebSockets | | NA | Technology not in use |
| 1.11.11 | OTG-CLIENT-011 | | Test Web Messaging | | NA | Technology not in use |
| 1.11.12 | OTG-CLIENT-012 | | Test Local Storage | | Yes | Tested Not Vulnerable |

## Scanned Items

https://tptuat.aponline.gov.in/APscience

https://tptuat.aponline.gov.in/APscience/Amaravati.aspx

https://tptuat.aponline.gov.in/APscience/ContactUs.aspx

https://tptuat.aponline.gov.in/APscience/css

https://tptuat.aponline.gov.in/APscience/Disclaimer.aspx

https://tptuat.aponline.gov.in/APscience/Documents

https://tptuat.aponline.gov.in/APscience/Documents/Downloads

https://tptuat.aponline.gov.in/APscience/Documents/Downloads/SCAP%20%20Executive%20Summary%20Shortcut.pdf

https://tptuat.aponline.gov.in/APscience/Documents/RTI

https://tptuat.aponline.gov.in/APscience/Documents/RTI/RTIACTFinal.pdf

https://tptuat.aponline.gov.in/APscience/Documents/Tender

https://tptuat.aponline.gov.in/APscience/Feedback.aspx

https://tptuat.aponline.gov.in/APscience/fonts

https://tptuat.aponline.gov.in/APscience/gallery

https://tptuat.aponline.gov.in/APscience/gallery/News\_Events

https://tptuat.aponline.gov.in/APscience/Governing.aspx

https://tptuat.aponline.gov.in/APscience/Home.aspx

https://tptuat.aponline.gov.in/APscience/images

https://tptuat.aponline.gov.in/APscience/images/home

https://tptuat.aponline.gov.in/APscience/js

https://tptuat.aponline.gov.in/APscience/js/bootstrap.min.js

https://tptuat.aponline.gov.in/APscience/js/highlight.js

https://tptuat.aponline.gov.in/APscience/js/jquery-3.3.1.min.js

https://tptuat.aponline.gov.in/APscience/js/jquery.easing.1.3.js

https://tptuat.aponline.gov.in/APscience/js/jquery.fancybox.pack.js

https://tptuat.aponline.gov.in/APscience/js/jquery.slimmenu.js

https://tptuat.aponline.gov.in/APscience/js/jquery.themepunch.revolution.min.js

https://tptuat.aponline.gov.in/APscience/js/jquery.themepunch.tools.min.js

https://tptuat.aponline.gov.in/APscience/js/owl.carousel.min.js

https://tptuat.aponline.gov.in/APscience/js/revolution.extension.kenburn.min.js

https://tptuat.aponline.gov.in/APscience/js/revolution.extension.layeranimation.min.js

https://tptuat.aponline.gov.in/APscience/js/revolution.extension.navigation.min.js

https://tptuat.aponline.gov.in/APscience/js/revolution.extension.slideanims.min.js

https://tptuat.aponline.gov.in/APscience/js/theme.js

https://tptuat.aponline.gov.in/APscience/Mission.aspx

https://tptuat.aponline.gov.in/APscience/Objectives.aspx

https://tptuat.aponline.gov.in/APscience/Origin.aspx

https://tptuat.aponline.gov.in/APscience/PhotoGallery.aspx

https://tptuat.aponline.gov.in/APscience/PrivacyPolicy.aspx

https://tptuat.aponline.gov.in/APscience/ScienceCityNews.aspx

https://tptuat.aponline.gov.in/APScience/ScriptResource.axd

https://tptuat.aponline.gov.in/APScience/ScriptResource. https://tptuat.aponline.gov.in/APScience/ScriptResource.axd

https://tptuat.aponline.gov.in/APscience/Sitemap.aspx

https://tptuat.aponline.gov.in/APscience/Terms\_Conditions.aspx

https://tptuat.aponline.gov.in/APscience/Tirupati.aspx

https://tptuat.aponline.gov.in/APscience/VideoGallery.aspx

https://tptuat.aponline.gov.in/APscience/Visakhapatnam.aspx

https://tptuat.aponline.gov.in/APScience/WebResource.axd

https://tptuat.aponline.gov.in/APScience/WebResource.axd

## Limitations

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