|  |
| --- |
|  |
|  |

Application Security Assessment Report

Of

E-Panta,

Agriculture, Horticulture, Revenue Dept, Govt. of AP

Dated 04/11/2019

by

Andhra Pradesh Technology Services Ltd

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

Vijayawada – 520010. Andhra Pradesh

Contents

[1. Executive Summary 3](#_Toc23766613)

[1.1. Introduction 3](#_Toc23766614)

[1.2. Engagement Specific Details 3](#_Toc23766615)

[1.3. Scope Details 3](#_Toc23766616)

[1.3.1. Inclusion 3](#_Toc23766617)

[1.3.2. Exclusion 3](#_Toc23766618)

[1.4. Approach & Methodology 4](#_Toc23766619)

[1.4.1. Information Gathering: 4](#_Toc23766620)

[1.4.2. Automated & Manual Scanning: 4](#_Toc23766621)

[1.4.3. Analyse results and reporting: 4](#_Toc23766622)

[2. Detailed Observation 7](#_Toc23766623)

[2.1. Web Application Security Assessment & Penetration Testing 7](#_Toc23766624)

[3. Scanned Items 19](#_Toc23766625)

[4. Limitations 20](#_Toc23766626)

1. Executive Summary

## Introduction

The Department of Agriculture has been dedicated to implement “Sustained and coordinated efforts" for facilitating a second green revolution and device strategies for optimum use of natural resources to create new avenues in Agriculture for livelihood and strengthen the rural areas. Government site-specific system to ensure that at least a part of the fallow lands are brought under cultivation by increasing irrigation sources. New seed technology and post harvest technology are need to be addressed.

Andhra Pradesh Technology Services (hereon referred as APTS) performed the Application Security Assessment of E-Panta application for Agriculture, Horticulture, Revenue 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. 31/10/2019 |
| 1. 2. | 1. Submission date of initial report | 1. 04/11/2019 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. **S. No** | **Area** | **Review Performed By** | **Application SPOC** | **Department Name** |
| 1. 1. | 1. Application Security Assessment | 1. APTS Security Audit Team |  | 1. Agriculture, Horticulture, Revenue Department |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **S. No** | **Date** | **Version Number** | 1. **Remarks** |
| 1. 1. | 1. 31/10/2019 | 1. v1.0 | 1. Initial Review |

## Scope Details

### Inclusion

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

Application Name: E-Panta

Application URL: http://36.255.252.196/epantakharif/login

Environment: Staging Server

Version Number [or] Latest Compilation Timestamp: Not provided

Type of Review: Gray box

Hash of Zipped Source Code (SHA512): Not Provided

User Accounts Tested: test\_login

### Exclusion

1. Server Vulnerability Assessment
2. Secure Code Review
3. Process Review
4. Secure Network Architecture Review
5. Search input field not working inside login

## 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 Gray 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
   1. **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.

* 1. **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 | 5 |
| **Total** |  |  | **8** |

**Distribution of Observation**

1. Detailed Observation

## Web Application Security Assessment & Penetration Testing

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | 1. **Session Mismanagement** | 1. **Risk Rating**: Medium |
| 1. **Description** | Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users identities. Such flaws may allow some or even all accounts to be attacked. | |
| 1. **Affected Path(s)** | /(web application) | |
| 1. **Impact** | 1. Once successful, the attacker can do anything the victim could do privileged accounts are frequently targeted. | |
| 1. **Evidence/Proof of Concept** 2. First, we need to login into application using “test\_login” credentials. 3. **\** 4. After login, we capture random requests using proxy service and save the request. After saving the request we logout of the application. 5. **\** 6. By nature after logging out of the application, the previous requests shouldn’t work anymore, but we could still able to send previous requests using proxy service and get response from the web application. 7. **\** | | |
| 1. **Recommendation** | * Generate new session Id after login and destroy it after logout. * Use of a long random number or string as the session key. This reduces the risk that an attacker could simply guess a valid session key through trial and error or brute force attacks. * Use HTTPS to protect the session ID during transmission. * Set the Domain and Path parameters for the cookie correctly. * Immediately destroy cookie after pressing logout and make server not accept requests using these cookies anymore. | |
| 1. **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | 1. **Directory Listing** | 1. **Risk Rating**: Medium |
| 1. **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. | |
| 1. **Affected Path(s)** | 1. http://36.255.252.196/epantakharif/AdangalReport/ 2. **103.210.75.132 {Redirected to external URL}** | |
| 1. **Impact** | A user can view a list of all files from this directory possibly exposing sensitive information. | |
| 1. **Evidence/Proof of Concept** 2. Visit the above URL and try to view the image in the report and copy the URL path of that image. When we visit the URL path we were able to see every file in the following folder. | | |
| 1. **Recommendation** | * Disable directory browsing option in configuration files of web server. | |
| 1. **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  | |
|  |  | |
|  |  | |
|  | | |
|  |  | |
|  |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | 1. **Missing Content Security Policy** | 1. **Risk Rating**: Low |
| 1. **Description** | When a user visits a site through his/her browser, the server responds with HTTP Response Headers. These headers tell the browser how to behave during communication with the site. | |
| 1. **Affected URL(s)** | /(web application) | |
| 1. **Impact** | 1. These headers will be added additional security features which will protect from various weaknesses and act as second level of defence. | |
| 1. **Evidence/Proof of Concept** 2. Here, Content Security Policy header is missing. 3. **pass_last_prev_prev_prev_prev.jpg** | | |
| 1. **Recommendation** | Implement all the required security headers in the response from server.  Reference:  https://www.thesslstore.com/blog/http-security-headers/  https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP  https://www.owasp.org/index.php/HttpOnly  https://www.keycdn.com/blog/x-xss-protection  https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control  https://www.owasp.org/index.php/SecureFlag | |
| 1. **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | **Last Login Time not implemented** | 1. **Risk Rating**: Low |
| 1. **Description** | 1. The last login time should be displayed POST login, as soon as the user login to the application it displays the time the user has logged in. | |
| 1. **Affected URL(S)** | /(web application) | |
| 1. **Impact** | The login attempts for service and scheduled job users are tracked in the same way when this feature is activated. The feature assumes interactive users are only used for interactive login access. | |
| **Evidence/Proof of Concept**  last login time is not implemented after login  Last Login Time.png | | |
| 1. **Recommendation** | 1. It is recommended to implement the last login time after login so that If an account is used for multiple purposes, the last interactive login reporting would also report the last service or scheduled job login. | |
| 1. **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | 1. **Concurrent logins enabled** | 1. **Risk Rating**: Low |
| 1. **Description** | It is a feature which provides way to access same account from different locations at the same time, It may not be required for most web applications but if it is needed, then it needs to be implemented carefully with some precautions. | |
| 1. **Affected Path(s)** | /(web application) | |
| 1. **Impact** | 1. If there is no proper track of sessions then attacker’s source cannot be differentiated from legitimate sessions. | |
| 1. **Evidence/Proof of Concept** 2. Same account can be accessed from different browsers which had been assigned with different session Ids. | | |
| 1. **Recommendation** | If the business functionality doesn’t require concurrent logins, it is advisable to remove this feature.  It is recommended for web applications to add user capabilities that allow checking the details of active sessions at any time, monitor and alert the user about concurrent logons, provide user features to remotely terminate sessions manually, and track account activity history (logbook) by recording multiple client details such as IP address, User-Agent, login date and time, idle time, etc. | |
| 1. **Management Comments** |  | |

|  |  |  |
| --- | --- | --- |
| 1. **Vulnerability Title** | 1. **Password input field with auto-complete enabled** | 1. **Risk Rating**: low |
| 1. **Description** | When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. | |
| 1. **Affected Path(s)** | http://36.255.252.196/epantakharif/login | |
| 1. **Impact** | 1. An attacker with local access could obtain the clear text password from the browser cache. | |
| 1. **Evidence/Proof of Concept** 2. Input password field doesn’t have auto complete attribute disabled, by default it is considered enabled. | | |
| 1. **Recommendation** | The password auto complete should be disabled in sensitive applications. To disable auto complete, you may use a code similar to: <INPUT TYPE="password" AUTOCOMPLETE="off"> | |
| 1. **Management Comments** |  | |

## Scanned Items

http://36.255.252.196/

http://36.255.252.196/

http://36.255.252.196/epantakharif

http://36.255.252.196/epantakharif/

http://36.255.252.196/epantakharif/AdangalReport

http://36.255.252.196/epantakharif/AdangalReport1

http://36.255.252.196/epantakharif/AdangalReport1/06/49/logout.php

http://36.255.252.196/epantakharif/assets/

http://36.255.252.196/epantakharif/assets/files

http://36.255.252.196/epantakharif/assets/files1

http://36.255.252.196/epantakharif/DvWAbstract

http://36.255.252.196/epantakharif/DvWAbstract/all

http://36.255.252.196/epantakharif/DvWAbstract/assets

http://36.255.252.196/epantakharif/DvWAbstract/files

http://36.255.252.196/epantakharif/DvWAbstract/logout.php

http://36.255.252.196/epantakharif/DvWSAbstract

http://36.255.252.196/epantakharif/home

http://36.255.252.196/epantakharif/Index

http://36.255.252.196/epantakharif/Kharif2019CropWiseAbstract/

http://36.255.252.196/epantakharif/Kharif2019CWAnnexure2

http://36.255.252.196/epantakharif/Kharif2019CWAnnexure2/agriculture

http://36.255.252.196/epantakharif/Kharif2019CWAnnexure2/assets

http://36.255.252.196/epantakharif/Kharif2019CWAnnexure2/files

http://36.255.252.196/epantakharif/Kharif2019CWAnnexure2/files/

http://36.255.252.196/epantakharif/Kharif2019CWAnnexure2/horticulture

http://36.255.252.196/epantakharif/Kharif2019CWAnnexure2/logout.php

http://36.255.252.196/epantakharif/Kharif2019CWAnnexure2/sf

http://36.255.252.196/epantakharif/Kharif2019DWAnnexure3

http://36.255.252.196/epantakharif/Kharif2019DWAnnexure3Dept

http://36.255.252.196/epantakharif/Kharif2019MWAnnexure3

http://36.255.252.196/epantakharif/Kharif2019RegistrationReport

http://36.255.252.196/epantakharif/Kharif2019VWAnnexure3

http://36.255.252.196/icons

## Limitations

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

|  |
| --- |
|  |