Security Audit Report

Madhya Pradesh Jail
Government of Madhya Pradesh

Highly Confidential

©

All rights reserved to Sandrock eSecurities Pvt. Ltd., 2017

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Sandrock eSecurities.
1 INTRODUCTION ........................................................................................................3
  1.1 OBJECTIVE ........................................................................................................3
    1.1.1 Application Black Box Penetration Testing ................................................3
  1.2 TESTING METHODOLOGY ..............................................................................3
  1.3 REPORT AND COMPLIANCE ..........................................................................3

2 EXECUTIVE SUMMARY ......................................................................................4
  2.1 SCOPE OF ACTIVITY ......................................................................................4
  2.2 VULNERABILITIES’ CRITICALITY SUMMARY ............................................4
  2.3 VULNERABILITIES’ TECHNICAL SUMMARY ...............................................4
  2.4 TEST CASE’ ARTIFACTS/SCREENSHOTS ....................................................4
  2.4.1 Server Misconfiguration ..............................................................................4
    2.4.1.1 CMS is updated: Failed .........................................................................4
    2.4.1.2 CMS Modules/Plugins/Addons updated: Failed .....................................4
    2.4.1.3 Server Version Disclosure: Passed .......................................................5
    2.4.1.4 Application Framework Version Disclosure: Passed .........................5
    2.4.1.5 Clickjacking (X-Frame-Options): Passed .............................................5
    2.4.1.6 XSS Protection: Passed .......................................................................6
    2.4.1.7 MIME Sniffing: Passed .......................................................................6
    2.4.1.8 Cache Poisoning: Passed .....................................................................6
    2.4.1.9 Cross Origin Resource Sharing: Passed .............................................7
    2.4.1.10 Other Miscellaneous Server/Application Information Disclosure: Passed 7
    2.4.1.11 Errors and Exceptions: Passed ...........................................................7
  2.4.2 User Authentication ....................................................................................8
    2.4.2.1 Default/Guessable Admin Login URL: Passed ...................................8
    2.4.2.2 Default/Guessable Username: Passed ................................................9
    2.4.2.3 User Self Registration: Passed .............................................................9
    2.4.2.4 Encrypted Credentials Submission: Failed .........................................9
    2.4.2.5 Strong Password Policy: Passed .........................................................9
  2.4.3 Session Management ..................................................................................10
    2.4.3.1 Session Expiration: Passed .................................................................10
    2.4.3.2 Concurrent Sessions: Passed ...............................................................10
    2.4.3.3 Cross Site Request Forgery: Passed ....................................................11
1 Introduction

A security vulnerability assessment identifies and reports noted vulnerabilities in the web application, followed by a penetration test which attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible.

1.1 Objective

1.1.1 Application Black Box Penetration Testing

Black box testing of the application includes, identifying and collecting all the possible application security vulnerabilities, from the front end of the application. This type of testing is suitable for all internal and business applications.

1.2 Testing Methodology

Sandrock eSecurities was tasked with following methodical approach in obtaining access to the objective goals.

1. Information Gathering
   - Looking for information on publicly available resources
   - Inserting technical information provided by the organization
   - Non-intrusive scan to determine systems, servers and services

2. Planning and Analysis
   - Analyzing the possible risks and vulnerabilities
   - Planning for a High Level Intense Penetration Test
   - Designing the overall testing approach

3. Vulnerability Detection and Identification
   - Searching for vulnerabilities on the resources
   - Enumerating known flaws, loopholes and mis-configurations
   - Manually probing the target, looking for vulnerabilities

4. Attack or Active Penetration
   - Customizing and using readymade exploits for a few known vulnerabilities
   - Building exploits for uncommon specific security loophole
   - Testing the exploits against vulnerabilities
   - Escalating the privileges to exploit higher roles, systems and services

5. Reporting
   - Executive Report for Top Management
   - Comprehensive Technical Report for Technical Personnel with solutions

1.3 Report and Compliance

The penetration testing report includes the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, etc
- Any additional items that were not included

This report can be used to support the regulatory and compliance requirements of:
- CERT-IN
- ISO 27001 ISMS
- PCI-DSS
- HIPAA
- GLBA
2 Executive Summary

A vulnerability assessment and penetration test was performed on the web application.

Date of Penetration Test: 24th August – 25th August 2017
Number of Technical Personnel Involved: 1

2.1 Scope of Activity

Sandrock eSecurities was tasked with performing the security test toward the following:
- http://demosl56.rvsolutions.in/ernet/website-069/

2.2 Vulnerabilities’ Criticality Summary

<table>
<thead>
<tr>
<th>Total</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>Scan 1: C:0, H:2, M:1, L:0</td>
</tr>
</tbody>
</table>

2.3 Vulnerabilities’ Technical Summary

<table>
<thead>
<tr>
<th>S#</th>
<th>Vulnerability Description</th>
<th>Status</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CMS is updated CMS is not fully updated</td>
<td>Update CMS</td>
<td>High</td>
</tr>
<tr>
<td>2</td>
<td>CMS Modules/Plugins/Add ons updated CMS modules are not fully updated</td>
<td>Update CMS plugins</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>Encrypted Credentials Submission Application submits the user login password in unencrypted form.</td>
<td>Implement SSL/</td>
<td>High</td>
</tr>
</tbody>
</table>

2.4 Test Case’ Artifacts/Screenshots

2.4.1 Server Misconfiguration

2.4.1.1 CMS is updated: Failed
CMS is not fully updated.

Last checked: 7 hours 29 minutes ago (Check manually)

Drupal core

- Drupal core 8.2.5
- Recommended version: 8.3.7 (2017-Aug-16)

2.4.1.2 CMS Modules/Plugins/Addons updated: Failed
CMS modules are not fully updated.
2.4.1.3 Server Version Disclosure: Passed
Server does not disclose the web server version information

2.4.1.4 Application Framework Version Disclosure: Passed
Application does not disclose the application framework version information

2.4.1.5 Clickjacking (X-Frame-Options): Passed
Server responds with "X-Frame-Options: SAMEORIGIN" header
2.4.1.6  **XSS Protection: Passed**  
Server responds with “X-XSS-Protection” header

2.4.1.7  **MIME Sniffing: Passed**  
Server responds with “X-Content-Type-Options: nosniff” header

2.4.1.8  **Cache Poisoning: Passed**  
Server does not respond with “Cache-Control” header
2.4.1.9 Cross Origin Resource Sharing: **Passed**
Application does not allow all origins (*) for resource sharing, as the server does not respond with "Access-Control-Allow-Origin" header.

2.4.1.10 Other Miscellaneous Server/Application Information Disclosure: **Passed**
Application does not reveal the CMS in the HTTP Source Code.

2.4.1.11 Errors and Exceptions: **Passed**
Generic errors and messages are displayed to users, application does not reveal technical information in errors.
2.4.2 User Authentication

2.4.2.1 Default/Guessable Admin Login URL: Passed
Application uses a custom user login location, instead of Drupal default user location “/user/login”.

Madhya Pradesh Jail
Government Of Madhya Pradesh
2.4.2.2 Default/Guessable Username: **Passed**
Drupal default username “admin” is blocked in the application.

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>STATUS</th>
<th>ROLES</th>
<th>MEMBER FOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>enetweb</td>
<td>Active</td>
<td>● Administrator</td>
<td>3 days 1 hour</td>
</tr>
<tr>
<td>admin</td>
<td>Blocked</td>
<td>● Administrator</td>
<td>6 months 3 weeks</td>
</tr>
</tbody>
</table>

2.4.2.3 User Self Registration: **Passed**
Application does not allow visitors to register themselves.

▶ REGISTRATION AND CANCELLATION

**Who can register accounts?**
- Administrators only
- Visitors
- Visitors, but administrator approval is required

**Require email verification when a visitor creates an account**
New users will be required to validate their email address prior to logging into the site, and will be assigned a system registering, and may select their own passwords during registration.

**Enable password strength indicator**

Who can cancel a user account?
- Disable the account and keep its content.
- Disable the account and unpublish its content.
- Delete the account and make its content belong to the Anonymous user.

Users with the Select method for canceling account or Administrator users permissions can override this default method.

2.4.2.4 Encrypted Credentials Submission: **Failed**
Application submits the user login password in unencrypted form.
**Fix:** Please implement SSL.

2.4.2.5 Strong Password Policy: **Passed**
Application has configured strong password policy.
### 2.4.3 Session Management

#### 2.4.3.1 Session Expiration: Passed
Application expires the session cookies after a pre-defined timeframe.

**Timeout value in seconds**
- **1440**

The length of inactivity time, in seconds, before automated log out. Must be 60 seconds or greater. Will not be used if the session’s timeout is used.

**Max timeout setting**
- **1800**

The maximum logout threshold time that can be set by users who have the permission to set user level timeouts.

**Timeout padding**
- **20**

How many seconds to give a user to respond to the logout dialog before ending their session.

- [ ] Role Timeout
  Enable each role to have its own timeout threshold, a refresh maybe required for changes to take effect. Any role that is not set will use the global timeout.

#### 2.4.3.2 Concurrent Sessions: Passed
Application does not allow more than 1 active session.

**Default maximum number of active sessions**
- **1**

The maximum number of active sessions a user can have. 0 implies unlimited sessions.

**When the session limit is exceeded**
- [ ] Ask user which session to end.
- [ ] Automatically drop the oldest sessions.
- [ ] Prevent creating of any new sessions.
2.4.3.3 Cross Site Request Forgery: **Passed**

Application is able to defend against CSRF attacks.