Web Application Security Reassessment Report for Webel Technology Limited – http://172.20.140.116

Confidential: v1.1

Technical Report

Dates of Audit: 8th Jan 2020

Number of Auditors: 1

Date of Report: 9th Jan 2020

Submitted To,

Sunil Bhattacharjee
Webel Technology Limited,
Plot-5, Block-BP, Sector-V,
Salt Lake City, Kolkata - 700091
West Bengal, India

Prepared by:
Digital Age Strategies

Business With Wisdom
Growth With Assurance

Digital Age Strategies Pvt. Ltd.
IT Security Solution Providers & IS Auditors
Corporate Office # 28, "Om Arcade"
Thimmappa Reddy Layout, Hulimavu,
Bannerghatta Road, Bangalore 560 076
Mobile No: +91 9448088666 / +91 9448055711
Tel No: +91 (80) 26484636/ 49568066/ 26485148 / 41503825
audit@digitalage.co.in
http://www.digitalage.co.in

Table of Contents

Executive Summary

About Digital Age Strategies

DIGITAL AGE is dedicated to providing its customers with excellent services in the area of Information Security for robust security architecture.

DIGITAL AGE has been empaneled as IT Security Audit Organization by the CERT-In, Ministry of Information Technology, Govt. of India and the CCA, Ministry of Information Technology, Govt. of India.

CERT-In is operational since January 2004. The constituency of CERT-In is the Indian Cyber Community. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur.

In the recent Information Technology amendment act 2008, CERT-In has been designated to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents.
  Forecast and alerts of cyber security incidents.
- Emergency measures for handling cyber security incidents.
- Coordination of cyber incident response activities.
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to in prevention, response and reporting of cyber incidents.
- Such other functions relating to cyber security as may be prescribed

Scope of the Exercise

The purpose of this Reassessment is to cross check whether the vulnerabilities identified during phase I audit has been mitigated or not and to check for any new vulnerability on the given Web Application of Webel Technology Limited. The scope limits Reassessment of the web application with the identification, categorization and providing mitigation strategies of vulnerabilities. The audit activities carried out based on OWASP guidelines.

Disclaimer

This document is highly confidential and sensitive and is meant for circulation only to authorized people with in Webel Technology Limited and Digital Age Strategies Pvt. Ltd.

This report is being supplied by us upon request and on the basis, that no part of this document may be copied, disclosed, referred or duplicated in part or whole (except for your own internal purpose and to authorized signatories) in any form. It is also hereby assumed that you shall not quote our name or reproduce our logo or other trademarks in print or in any form or medium without our express acquiescence. You may disclose this report to your legal and other professional advisors for the purpose of your seeking advice in relation to the report and the data contained herein, provided that when doing so, it is understood that disclosure in part or full of the contents or any information derived from the report to unauthorized personnel is strictly prohibited.

Digital Age Strategies Pvt. Ltd. has performed Web Application Security Reassessment on the request of Webel Technology Limited. The intent of which is to identify the existing vulnerabilities in the web application and to explore the possibilities of these vulnerabilities may be exploited by malicious users, if not mitigated.

Any advice, opinion, remedial measures, forecast or recommendation provided by Digital Age Strategies Pvt. Ltd. in this report is based on the information provided to us and we believe such advice, opinion, remedial measures, forecast or recommendation to be valid. Due professional care has been taken by Digital Age Strategies Pvt. Ltd. during the execution of this exercise. Digital Age Strategies Pvt. Ltd. is not liable for any damage of any form caused directly or indirectly during and post completion of this exercise. Digital Age Strategies Pvt. Ltd. would not be accountable for the outcome of implementing any of the recommendations contained herein.

The data contained in this report does not amount to guarantee that we have predicted future events or circumstances but shall ensure accuracy, competency, correctness or completeness of the report based on the information provided to us. This exercise has been undertaken within a given time period in a comprehensive manner. Digital Age Strategies Pvt. Ltd. cannot guarantee security of the target site, though mitigation of the findings can substantially reduce the risks of a security breach.

Approach

VAPT Auditor of Digital Age Strategies carried out Web Application Security Reassessment on the Web Application provided by the organization. The same Reassessment was carried out using tools and research-based methods. The vulnerabilities were tested in a non-obtrusive manner to substantiate if they actually affect the IT security and as to what more information can be obtained that can be used for assuaging possibility and impact of attacks.

Research based investigation

Digital Age Strategies Security Auditor analyzed the web application manually for information related to the modules, page sections, etc. The specific configurations, entry points, URL parameters, etc. were then tested for specific vulnerabilities. These possible vulnerabilities were then tested and the results obtained as proofs.

Primary Tools for Testing

Although a wide variety of tools can be used for Web Application testing, the primary tool, which we use, is Burp Suite Professional and with the help of various Open Source tools we performed manual testing for ensuring the findings and also for the proof-of-concept.

Type of Test

Grey Box Testing

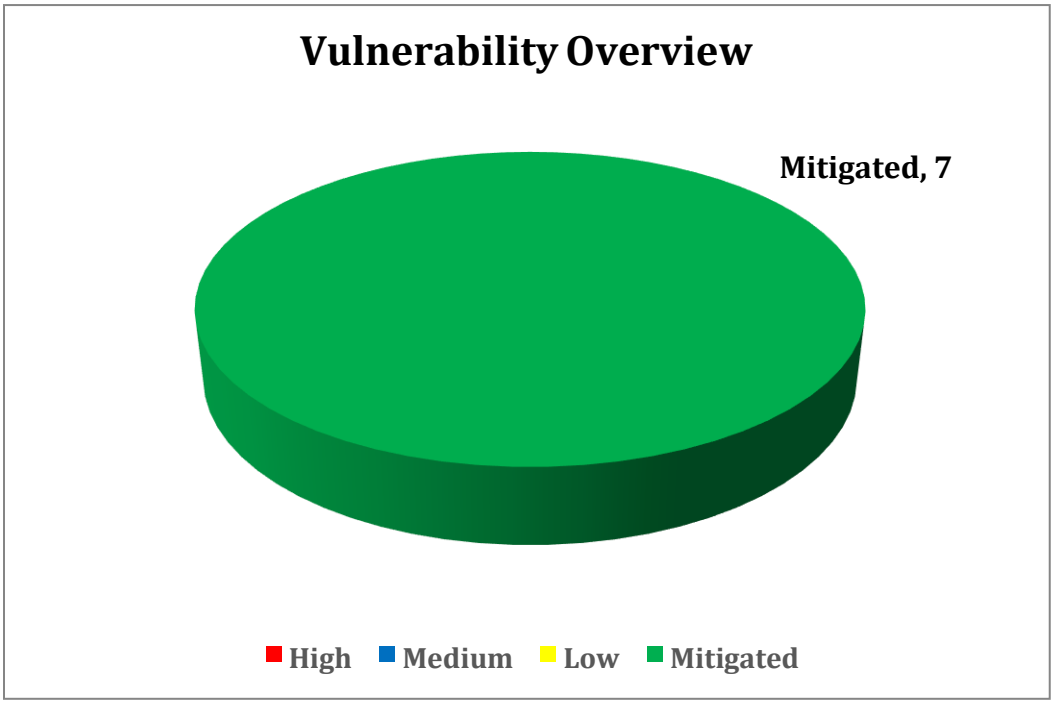
The Reassessment was entirely carried out with a Manual Grey Box Testing. Manual testing approach eradicates false positives that common automated tools throw up. The site was Also Subjected to various other tests based on the OWASP Testing Guidelines including Parameter manipulation, cookie manipulation, Request Modification and Testing for the OWASP Top 10.

Overview of Results

Distribution of Vulnerabilities – Census Report

The following graphical representation details the current threat level based on the severity of the vulnerabilities, business impact and ease of mitigation.

Census of Web Application Vulnerabilities



Host Details

Sl. No.	URL
1.	http://172.20.140.116

Vulnerabilities and Proof of Concept

This section enlists the vulnerabilities that exist on the stated web application. The vulnerabilities listed in the following pages are derived from the collective Reassessment of the web application using tools and the tested expertise of our Security Auditor.

Listed below are general observations made by Digital Age Strategies during and upon completion of the Reassessment.

Vulnerability Title:

The Vulnerability Title is a short one-line description of the vulnerability discovered. The title is color coded according to the risk level as follows:

High	This risk level indicates a vulnerability whose successful exploitation may result in a significant impact to the confidentiality, integrity or availability of information accessible through the system, network resource or web application. Backend resources like the database, connected systems and the network in general are likely to be affected. A successful exploit may lead to irrecoverable damage to data, resources and reputation.
Medium	This risk level indicates a vulnerability that when successfully exploited may cause disclosure of potentially sensitive information and exposure of underlying application or system architecture that when combined with other vulnerabilities may cause severe impact on resources and credibility.
Low	This risk level indicates a vulnerability that when exploited may result in disclosure of information that may help an attacker gain a substantial amount of understanding of the applications underlying architecture. This information could then be used to further an attack scenario on a target.
Mitigated	This level defines all the vulnerabilities that were found during the Previous phase as part of the current exercise have been mitigated now.

Description:

The description provides a brief outline of the vulnerability, including its common identifier, where applicable and available.

Affected Link & Parameter [Location of Vulnerability]:

The systems responsible or affected for or due to the vulnerability are listed here. If multiple systems are involved or are affected by different instances of the same vulnerability then they will be listed here along with the other targets. In case of web applications, the affected URL or the server configuration will be listed.

Audit Observation:

Final status of the vulnerability states whether reported vulnerability has been mitigated or to be mitigated else any other status according to the business requirements.

Vulnerability Summary

This section presents the analysis of vulnerabilities found on the Web Application as per OWASP Top 10 – 2017 guidelines.

OWASP Top 10 Vulnerabilities Status

Sl. No.	OWASP Top 10 Application Security Risk	Vulnerability Findings	Final Status
1.	Injection	Not Found	Not Found
2.	Broken Authentication	Not Found	Not Found
3.	Sensitive Data Exposure	Web Application Verbose Error Message	Mitigated
4.	XML External Entities (XXE)	Not Found	Not Found
5.	Broken Access Control	Not Found	Not Found
6.	Security Misconfiguration	1. Clickjacking 2. Missing X-XSS-Protection 3. Missing X-Content-Type-Options 4. Information disclosure via response headers	1. Mitigated 2. Mitigated 3. Mitigated 4. Mitigated
7.	Cross – Site Scripting (XSS)	Not Found	Not Found
8.	Insecure Deserialization	Not Found	Not Found
9.	Using Components with known Vulnerabilities	1. Vulnerable jQuery Version 2. Vulnerable Bootstrap version	1. Mitigated 2. Mitigated

10	Insufficient Logging & Monitoring	Not Found	Not Found

Observations

This section presents a descriptive analysis of the vulnerabilities found on the Web Application that were obtained while performing the tests.

1. Clickjacking

Description:
The application response headers contains missing X-Frame-Field options. Which may allow attacker to inject some other page using Iframe code.

Affected Link & Parameter [Location of Vulnerability]:
http://172.20.140.116/Default1.aspx

Audit Observation:
Vulnerability has been mitigated

2. Web Application Verbose error message

Description:
The web application displays verbose error messages in the event of a malformed SQL query being processed.

Affected System & Host [Location of Vulnerability]:
http://172.20.140.116/Page/Lading_Page.aspx/<>

Audit Observation:
Vulnerability has been mitigated

3. Missing X-XSS-Protection

Description:
This header is used to configure the built in reflective XSS protection found in Internet Explorer, Chrome and Safari (Webkit). Valid settings for the header are 0, which disables the protection, 1 which enables the protection and 1; mode=block which tells the browser to block the response if it detects an attack rather than sanitizing the script.

Affected Link & Parameter [Location of Vulnerability]:
http://172.20.140.116/Default1.aspx

Audit Observation:
Vulnerability has been mitigated

4. Missing X-Content-Type-Options

Description:
This header only has one valid value, nosniff. It prevents Google Chrome and Internet Explorer from trying to mime-sniff the content-type of a response away from the one being declared by the server. It reduces exposure to drive-by downloads and the risks of user uploaded content that, with clever naming, could be treated as a different content-type, like an executable.

Affected Link & Parameter [Location of Vulnerability]:
http://172.20.140.116/Default1.aspx

Audit Observation:
Vulnerability has been mitigated

5. Information disclosure via Response Headers

Description:
The application page header is displaying sensitive information such as version disclosure and other details.

Affected Link & Parameter [Location of Vulnerability]:
http://172.20.140.116/Default1.aspx

Audit Observation:
Vulnerability has been mitigated

6. Vulnerable jQuery version

Description:
This page is using an older version of jQuery that is vulnerable to a Cross Site Scripting vulnerability. Many sites are using to select elements using location. Hash that allows someone to inject script into the page. This problem was fixed in jQuery 1.3.2.

Affected Link & Parameter [Location of Vulnerability]:
http://172.20.140.116/Page/Lading_Page.aspx

Audit Observation:
Vulnerability has been mitigated

7. Vulnerable Bootstrap version

Description:
Bootstrap version 3.3.7 is an outdated and versions below 3.3.7 is vulnerable to many attacks.

Affected Link & Parameter [Location of Vulnerability]:
http://172.20.140.116/Default1.aspx

Audit Observation:
Vulnerability has been mitigated

Conclusion

Digital Age Strategies' Security Auditor conducted Web Application Security Reassessment on the given Web Application of Webel Technology Limited and found the above-mentioned vulnerabilities are mitigated.

VAPT Auditor
Digital Age Strategies Pvt. Ltd.
Bengaluru.
January 2020