**Web Application Security Assessment Report**

**For**

**Web Application**

(https://beta.s2platform.com)

|  |  |
| --- | --- |
|  | **SoulAce Consulting Pvt Ltd.** |
| **P-166, Block G, New Alipore, Kolkata, West Bengal 700053** |

|  |  |
| --- | --- |
| **Report Release Date** | 29-05-2024 |
| **Type of Audit** | Web Application Security Assessment |
| **Type of Audit Report** | First Audit Report |
| **Period** | 23-05-2024 to 27-05-2024 |

**ITOrizin Technology Solutions Pvt. Ltd.**

An ISO 9001:2015, 20000-1:2011 and 27001:2013 Certified Company

8/14, Sahid Nagar, Gnd. Floor, Kolkata 700078

Ph: +91 33 2415 6011

E-Mail: [connect@itorizin.in](mailto:connect@itorizin.in)

[www.itorizin.com](http://www.itorizin.com/)

**Document Control**

|  |  |
| --- | --- |
| **Document Preparation** | |
| **Document Title** | Web Application (https://beta.s2platform.com) Security Assessment Report for SoulAce Consulting Pvt Ltd. |
| **Document ID** | ITOTSPL-SOULACE-WASA-2024-01-1 |
| **Document Version** | 1.0 |
| **Prepared by** | Dipanjan Mandal |
| **Reviewed by** | Susanta Saha |
| **Approved by** | Sirsendu Bharati |
| **Released by** | Susanta Saha |
| **Release date** | 29-05-2024 |

|  |  |  |
| --- | --- | --- |
| **Document Change History** | | |
| **Version** | **Date** | **Remarks / Reason of change** |
| 1.0 | 29-05-2024 | First Audit Report |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Distribution List** | | | |
| **Name** | **Organization** | **Designation** | **Email Id** |
| Sib Basu | SoulAce Consulting Pvt Ltd. | IT Head | sib@soulace.in |
| Asadul Hide | SoulAce Consulting Pvt Ltd. | System Admin | asadul@soulace.in |
| Dipanjan Mandal | ITOrizin Technology Solutions Pvt. Ltd. | Security Analyst | m.dipanjan@itorizin.in |
| Susanta Saha | ITOrizin Technology Solutions Pvt. Ltd. | Sr. Security Analyst | s.susanta@itorizin.in |
| Sirsendu Bharati | ITOrizin Technology Solutions Pvt. Ltd. | Sr. Security Analyst | b.sirsendu@itorizin.in |
| Sangeeta Ganguly | ITOrizin Technology Solutions Pvt. Ltd. | Sr. Manager - Business Development | g.sangeeta@itorizin.in |
| Anindya Kanti Ghosh | ITOrizin Technology Solutions Pvt. Ltd. | Sr. Vice President - Projects | gd.anindya@itorizin.in |

Contents

**[Introduction](#_Toc164340321)** [4](#_Toc164340321)

**[Engagement Scope](#_Toc164340322)** [5](#_Toc164340322)

**[Details of the Auditing team](#_Toc164340323)** [6](#_Toc164340323)

**[Audit Activities and Timelines](#_Toc164340324)** [7](#_Toc164340324)

**[Audit Methodology and Criteria / Standard referred for audit](#_Toc164340325)** [8](#_Toc164340325)

**[Tools/ Software used](#_Toc164340326)** [8](#_Toc164340326)

**[Executive Summary](#_Toc164340327)** [10](#_Toc164340327)

**[Detailed Observations](#_Toc164340328)** [14](#_Toc164340328)

**[Appendices](#_Toc164340329)** [48](#_Toc164340329)

# **Introduction**

This report presents the results and findings of the Web Application Security Assessment conducted for “SoulAce Consulting Pvt Ltd.” identified as the Web Application Security Assessment. This assessment was performed by “ITOrizin Technology Solutions Pvt Ltd”. The purpose of this assessment was to identify vulnerabilities and other security issues that could affect the Web Application (https://beta.s2platform.com) of “SoulAce Consulting Pvt Ltd.”. The security assessment was carried out from the “ITOrizin” premises in Kolkata. The findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions.

# **Engagement Scope**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S.**  **No** | **Asset**  **Description** | **Criticality**  **of Asset** | **Internal**  **IP Address** | **URL** | **Public**  **IP Address** | **Location** | **Hash Value**  **(in case of applications)** | **Version (in**  **case of applications)** | **Other**  **details such as make and model**  **in case of network devices or security devices.** |
| 1 | CSR Monitoring Application | High | NA | https://beta.s2platform.com | NA | Mumbai | NA | 7.1.1 | NA |

Date up to which the list has been updated: 23.05.2024

# **Details of the Auditing team**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S. No | Name | Designation | Email Id | Professional  Qualifications/ Certifications | Whether the resource has Been listed in  the Snapshot information published on CERT-In’s website (Yes/No) |
| 1 | Dipanjan Mandal | Security Analyst | m.dipanjan@itorizin.in | B Tech (CSE) | No |
| 2 | Susanta Saha | Sr. Security Analyst | s.susanta@itorizin.in | B Tech (IT) | Yes |
| 3 | Sirsendu Bharati | Sr. Security Analyst | b.sirsendu@itorizin.in | B Tech (IT) | Yes |

# **Audit Activities and Timelines**

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No. | Activities | Start Date | End Date |
| 1. | Testing/Staging (UAT) URL's Received | 23.05.2024 | 23.05.2024 |
| 2. | Automated Scan | 24.05.2024 | 24.05.2024 |
| 4. | Manual Testing | 24.05.2024 | 27.05.2024 |
| 5. | Report Preparation | 27.05.2024 | 28.05.2024 |
| 6. | Report Review | 28.05.2024 | 28.05.2024 |
| 7. | Report Submission | 29.05.2024 | 29.05.2024 |

# **Audit Methodology and Criteria / Standard referred for audit**

Website/web application security assessment is a form of security testing used to analyse security posture of a web site/application. That built on OWASP Web Application Top 10 vulnerability standard & SANS 25 standard. Website/application security methodology is kept up-to-date according to changes in the threat environment and industry best practices provides consistency and structure to security testing. ITOrizin Technology Solutions Pvt Ltd keeps its Web site/Application Security Assessment methodology updated with new tools, processes, techniques, or as trend develops. Our methodology is a comprehensive blend of the following methodologies and IT Security industry best practices:

Open-Source Security Testing Methodology Manual (OSSTMM) from the Institute for Security and Open Methodologies (ISECOM);

NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

OWASP Top 10 vulnerability

SANS 25 standard

**OWASP Top 2021 Ten Most Critical Web Application Vulnerabilities Mapping**

|  |  |  |
| --- | --- | --- |
| Sl. No. | Security Risk | Present in Web Application |
| 1 | **Broken Authentication** | **No (Examined & Not Found)** |
| 2 | **Cryptographic Failures** | **No (Examined & Not Found)** |
| 3 | **Injection** | **No (Examined & Not Found)** |
| 4 | **Insecure Design** | **No (Examined & Not Found)** |
| 5 | **Security Misconfiguration** | **No (Examined & Not Found)** |
| 6 | **Vulnerable and Outdated Components** | **No (Examined & Not Found)** |
| 7 | **Identification and Authentication Failures** | **No (Examined & Not Found)** |
| 8 | **Software and Data Integrity Failures** | **No (Examined & Not Found)** |
| 9 | **Security Logging and Monitoring Failures** | **No (Examined & Not Found)** |
| 10 | **Server-Side Request forgery (SSRF)** | **No (Examined & Not Found)** |

**SANS-25 Most Critical Web Application Vulnerabilities Mapping**

|  |  |  |
| --- | --- | --- |
| Sl. No. | Security Risk | Present in Web Application |
| 1 | **Out-of-bounds Write** | **No (Examined & Not Found)** |
| 2 | **Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')** | **No (Examined & Not Found)** |
| 3 | **Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')** | **No (Examined & Not Found)** |
| 4 | **Improper Input Validation** | **No (Examined & Not Found)** |
| 5 | **Out-of-bounds Read** | **No (Examined & Not Found)** |
| 6 | **Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')** | **No (Examined & Not Found)** |
| 7 | **Use After Free** | **No (Examined & Not Found)** |
| 8 | **Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')** | **No (Examined & Not Found)** |
| 9 | **Cross-Site Request Forgery (CSRF)** | **No (Examined & Not Found)** |
| 10 | **Unrestricted Upload of File with Dangerous Type** | **No (Examined & Not Found)** |
| 11 | **NULL Pointer Dereference** | **No (Examined & Not Found)** |
| 12 | **Deserialization of Untrusted Data** | **No (Examined & Not Found)** |
| 13 | **Integer Overflow or Wraparound** | **No (Examined & Not Found)** |
| 14 | **Improper Authentication** | **No (Examined & Not Found)** |
| 15 | **Use of Hard-coded Credentials** | **No (Examined & Not Found)** |
| 16 | **Missing Authorization** | **No (Examined & Not Found)** |
| 17 | **Improper Neutralization of Special Elements used in a Command ('Command Injection')** | **No (Examined & Not Found)** |
| 18 | **Missing Authentication for Critical Function** | **No (Examined & Not Found)** |
| 19 | **Improper Restriction of Operations within the Bounds of a Memory Buffer** | **No (Examined & Not Found)** |
| 20 | **Incorrect Default Permissions** | **No (Examined & Not Found)** |
| 21 | **Server-Side Request Forgery (SSRF)** | **No (Examined & Not Found)** |
| 22 | **Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')** | **No (Examined & Not Found)** |
| 23 | **Uncontrolled Resource Consumption** | **No (Examined & Not Found)** |
| 24 | **Improper Restriction of XML External Entity Reference** | **No (Examined & Not Found)** |
| 25 | **Improper Control of Generation of Code ('Code Injection')** | **No (Examined & Not Found)** |

# **Tools/ Software used**

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No | Name of Tool/Software  used | Version of the tool  /Software used | Open Source/Licensed |
| 1 | OWASP Zap | 2.15.0 | Open Source |
| 2 | Burp Suite Professional | 2024.2.1.4 | Open Source |
| 3 | Nmap | 7.95 | Open Source |
| 4 | Custom Scripts | Not Applicable | Not Applicable |

# **Appendices**

**Risk Ranking Approach**

Each assessment finding is assigned a risk rating. The risk rating used in this report is based on the following criteria:

**High**

**Medium**

**Low**

**Info**

Under specific conditions, these vulnerabilities can potentially make the system unusable and lead to serious security breaches. These vulnerabilities violate basic security design parameters and should be handled with the highest priority.

Though the threat is not critical at the moment, it has the potential to become a High risk threat in the future under certain circumstances if not mitigated. Medium risk vulnerabilities require significant mitigation to lower the impact of the threat.

The information found is useful to the attacker, but is not a threat in itself. Existing security controls are likely to be adequate or the risk is acceptable, but over the period this may give rise to more serious problems.

The data revealed is an additional piece of information and there are no serious security implications related to it.

The likelihood of an attack occurring and the impact of a successful attack are used in calculating the risk rating:

Medium

High

Low

Medium

High

Low

**Likelihood**

**Impact**

**Observation Summary**

The overall analytical report is based on the technologies and known threats as of date of Web Application Security Assessment. We suggest that all recommendations mentioned in this Web Application Security Assessment Report should be undertaken in order to ensure the overall security of the concerned web application.

As a result of the assessment, we found that the current security posture of the Web application within the scope requires considerable security fixes with many of them falling in ‘High/Medium/ Low’ severity/priority buckets. During our web application security assessment, total of seventeen (17) vulnerabilities were discovered out of which two (2) vulnerabilities are of high risk eleven (11) vulnerabilities are of medium-risk and four (4) vulnerabilities are of low-risk category. We suggest the “SoulAce Consulting Pvt Ltd.” team to implement the recommendations mentioned against all security issues in this report with respect to the affected web application. The implementation priority should be based on the risk ratings associated with findings i.e., high risks should be closed first and then should be headed towards ‘Medium’ and ‘Low’ findings. We recommend that a follow-on security assessment should be done on the concerned Web application after all security recommendations are implemented to confirm the mitigation of security issues.

**Acronyms:**

* CVE- common vulnerabilities and exposures
* CWE- common weakness enumeration
* MASVS-Mobile Application Security Verification Standard)
* OWASP- Open Web Application Security Project
* OSSTMM- Open-Source Security Testing Methodology Manual
* ISECOM- ISECOM
* NIST- National Institute of Standards and Technology
* VA-Vulnerability Assessment
* PT-Penetration Testing

**Disclaimer**

The data contained in this document shall not be disclosed, duplicated, used, or disclosed in whole or in part for any purpose. If a contract is awarded because of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client’s or prospective client’s right to use the information contained in the data if it is obtained from another source without restriction.

Although the author or ITOrizin Technology Solutions Pvt. Ltd. have made every effort to ensure that the information in this book was correct at the time of writing, the author and ITOrizin Technology Solutions Pvt. Ltd. do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.