<redacted> WEB APPLICATION

SECURITY ASSESSMENT REPORT

Date: 06th September, 2023

Project SA-6923: VAPT version v1.0

Document Version Control

Document Details

Report Date	Version	Prepared By	Reviewed By	Changes Made
06-09-2023	v1.0	Gaurav Suryawanshi (Assessor)	Gaurav Suryawanshi	Created

Confidentiality Statement

This document is the exclusive property of <redacted> & its respective stakeholders/affiliates. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of <redacted>.
<redacted> may share this document with external/internal auditors under non-disclosure agreements to demonstrate website security assessment (VAPT) requirements or as a part of compliance.

Disclaimer

A website security assessment is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Contact Details

Name	Contact Information
<redacted>'s Team	
Sanjay XX	sanjay@redacted.com
Security Assessor	
Gaurav Suryawanshi	offsecgaurav@gmail.com

Key Sections of this Report

1. Executive Summary

The executive summary provides a high-level overview of the assessment, describing application strengths & weaknesses, strategic recommendations, summary & count of total vulnerabilities as per CVSS scoring system and testing details. It's designed for decision-makers who need a quick snapshot of the security posture without diving into technical details.

2. Environment details & Security Assessment approach

This section elaborates on the specifics of the Vulnerability Assessment & Penetration Testing (VAPT) process, such as the tools used, the type of testing (black-box, white-box, or grey-box) and the environment in which the testing took place (e.g., staging, production). Understanding the environment and tools used for testing can give insights into the comprehensiveness of the assessment.

3. Compliance w.r.t OWASP Top 10 & ISO/IEC 27001 (Application's Go-Live Readiness)

Here, the report details how well the application meets the security standards defined by ISO/IEC 27001 and OWASP Top 10. This is critical for understanding the business readiness of the application. Each vulnerability is compared against the ISO/IEC 27001 and OWASP Top 10 list to identify the level of risk, areas for improvement and compliance.

4. Detailed Findings

This is the heart of the report, detailing all the vulnerabilities identified during the assessment. Each vulnerability typically includes a description, evidence, severity level and recommended remediation steps. It offers both technical and non-technical personnel a deep dive into the vulnerabilities that exist within the application.

Key Sections of this Report

5. Security Assessment Summary & Remarks

This scorecard usually tabulates the vulnerabilities found in terms of their OWASP classification, risk level and other metrics. It provides a quick, quantified view of the application's security posture, often using risk scores to prioritize issues.

6. Appendix A (Risk Calculation)

Here, you'll find the detailed risk assessment metrics and how the risk scores were calculated for each vulnerability. This can include factors such as impact, likelihood and the equation used to arrive at a final risk score. This is especially useful for risk management teams or auditors who may need to understand the basis on which risks were assessed.

Each of these sections serves to provide a complete view of the security assessment from both a high-level and detailed perspective, helping various stakeholders make informed decisions on next steps.

Table of Contents

1. Executive Summary

In preparation for the deployment, <redacted>'s web application has undergone a comprehensive security assessment aligned with the OWASP Top 10 2021, Web Security Testing Guide (WSTG) v4.2 and ISO/IEC 27001 standards. The objective was to identify vulnerabilities and assess the application's ability to withstand external & internal threats.

The testing methodology utilized was Grey-Box, which combines elements of both Black-Box and White-Box testing - providing limited internal knowledge to simulate an attack from a partially privileged user.

1.1 Details of the Web application's strength & defense mechanisms

- Application has implemented strong measures against injection attacks such as SQL Injection, Cross-Site-Scripting (XSS), HTML injection, OS injection & LDAP injection.
- Application has disabled the 'right-click' functionality as a first line-of-defense, which restricts the end-user & intended audience to attempt client-side manipulation.
- Application is not vulnerable to directory traversal attacks. As a result, an attacker cannot read the sensitive files and/or contents from the server.
- Application does not allow concurrent sessions for the same user, which is a strong defense against session fixation/session-related attacks.
- Application has the functionality of MFA (OTP-based authentication) which adds an additional layer of security to the login (authentication) mechanism.
- ASP.NET's filtering module was detected to thwart/block the incoming malicious payloads at the application level.
- Application's data is encrypted both in transit and at rest.
- Application has strong password policy and implements account lockout mechanisms to prevent brute-force attacks.
- Application enforces HTTPS connection, when a user tries to downgrade the connection to a HTTP connection.

1. Executive Summary

1.2 Details of the Web application's weakness & misconfigurations

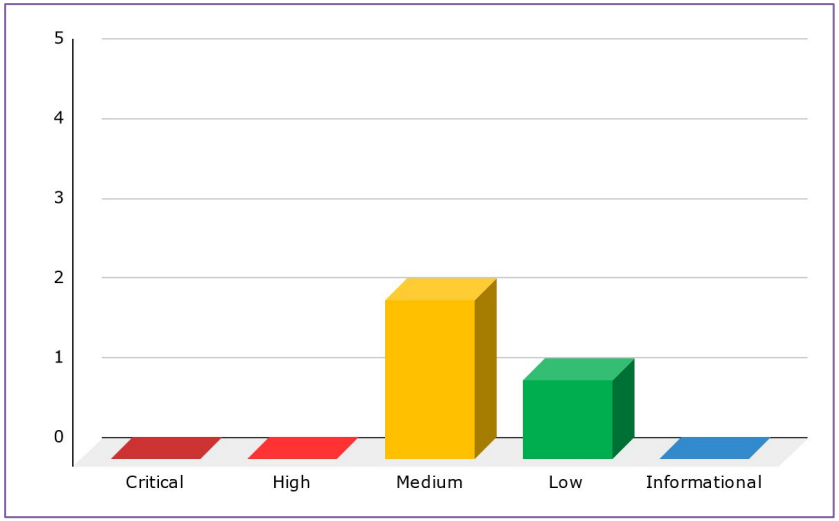
- In the application's server response, it was observed that the Content-Security-Policy (CSP) & certain security HTTP headers were missing.
- At the network-level, the application has enabled TLS v1.0 & TLS v1.1 which are outdated and should be disabled.
- During the assessment, it was observed that the application lacks the implementation of a dedicated WAF (Web Application Firewall). However, the services provided by the Cloud Hosting Provider (MochaHost) uses in-built defense mechanisms, offered by the current technology stack (like ASP .NET payload filtering) which can block malicious incoming payloads, to a certain extent.
- Application fails to validate an instance of a business logic on the server side, which should be implemented to ensure that the 'Assigned user' has no provision & permission to imitate the features, restricted to the 'Admin/Super' user.

1.3 Strategic Recommendations

- W.r.t to the first weakness point, missing HTTP security headers can be quickly implemented by the application development (AD) team to ensure defense-in-depth measures.
- W.r.t to the second weakness point, TLS v1.2 & TLS v1.3 should be enabled with 'A' suite ciphers only.
- Wr.t. to the third weakness point, a dedicated WAF (Web Application Firewall) such as F5, Imperva, CloudFlare, etc. should be implemented, as soon as possible.
- Wr.t. to the fourth weakness point, application should implement server-side validation & the policy of least privilege, in the codebase to ensure the restriction of sensitive operations by an unauthorized user.
- DNSSEC should be 'signed', in the (DNS/Domain settings), provisioned - by the hosting provider.
- After the integration and prior to the roll-out of payment gateway, web application should implement SSL certificate as per the Payments Card Industry (PCI) compliance standards.

1. Executive Summary

Total Issues/Vulnerabilities Count



Finding ID	Vulnerability Title	Severity	CVSS Score	OWASP Category	Status
M01	Improper Access Control ('Business Logic Validation Failure')	Medium	4.7	A01:2021- Broken Access Control	Open
M02	Forced Browsing ('Direct Request')	Medium	4.7	A01:2021- Broken Access Control	Open
L01	Security Misconfigurations	Low	3.8	A05:2021- Security Misconfiguration A02:2021- Cryptographic Failures	Open

The security assessment was carried out in strict adherence to the following industry-recognized guidelines and standards:

Web Security Testing Guide (WSTG) 4.2: Comprehensive guidelines were followed to ensure that all aspects of web security were scrutinized, including but not limited to authentication, data integrity and confidentiality. This guide consists of 100+ applicable manual test cases.

OWASP Top 10: The Open Web Application Security Project's (OWASP) top 10 most critical web application security risks were a significant focus of this assessment, ensuring that the application is safeguarded against the most common and impactful security vulnerabilities.

ISO/IEC 27001: Compliance with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001 standards for Information Technology ensures that our security management is of the highest caliber, with an emphasis on continual improvement.

2. Environment details & Security Assessment approach

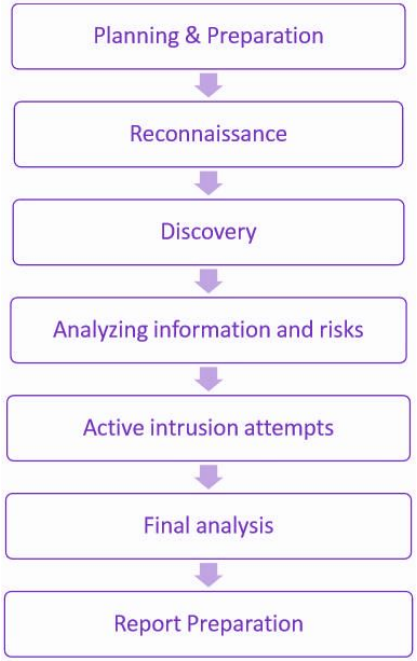
Vulnerability Assessment & Penetration Testing (VAPT) environment details

Assessment URL(s):	- https://clientsregion301.<redacted>.com - https://<redacted>.com	**Assessor:**	Gaurav Suryawanshi (Independent eJPT certified Professional)
User Credentials:	- offsecgaurav@gmail.com - admin@<redacted>.biz	**User Roles:**	- Assigned User - Admin/Super User
Assessment Start Date:	02-09-2023	**Assessment End Date:**	05-09-2023
Tools:	- Burp Suite Professional - Kali Linux Distribution & Tools - WAS (Acunetix)	**Test Standard & Policy:**	- OWASP Top 10 2021 - ISO/IEC 27001 (ISMS) - WSTG v4.1
Application Environment:	- Development (Production)	**Test Classification:**	Grey-Box (Manual 90% + Automated 10%)
Assessment Scope Exclusion(s):	- None (i.e. All the endpoints were tested - with every applicable test case) - However, other <redacted>'s Modules & Web applications were not a part of this assessment.		

Assessment approach

Phases of penetration testing activities include the following methodical attack strategy -

Planning – Customer goals are gathered and rules of engagement obtained.
Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
Reporting – Document all found vulnerabilities and exploits, failed attempts and company strengths and weaknesses.



3. Compliance w.r.t OWASP Top 10 2021 & ISO/IEC 27001 (Application's Go-Live Readiness)

OWASP Top 10 Risk Classification	ISO/IEC 27001 - Clause Mapping	Assessment Status	Security risk Compliance Status	Responsible Person/Team	Remediation Timeline
A01: Broken Access Control	A.9 Access control	Assessed	Area for Improvement (Can be 100% compliant, after fixing the related issue)	Development Team	15 days (1/2 month)
A02: Cryptographic Failures	A.10 Cryptographic controls	Assessed	Area for Improvement (Can be 100% compliant, after fixing the related issue)	Network Team/Application Owner	30 days (1 month)
A03: Injection	A.13 Communications security	Assessed	Compliant (<redacted>'s Web application has implemented strong defense)	Not applicable	
A04: Insecure Design	A.14 System acquisition, development, and maintenance	Assessed	Compliant (<redacted>'s Web application has implemented strong defense)		
A05: Security Misconfiguration	A.12 Operations security	Assessed	Area for Improvement (Can be 100% compliant, after fixing the related issue)	Development Team	30 days (1 month)
A06: Vulnerable and Outdated Components	A.14 System acquisition, development, and maintenance	Assessed	Compliant (<redacted>'s Web application has implemented strong defense)	Not applicable	
A07: Identification and Authentication Failures	A.9 Access control	Assessed	Compliant (<redacted>'s Web application has implemented strong defense)		
A08: Software and Data Integrity Failures	A.12 Operations security	Assessed	Compliant (<redacted>'s Web application has implemented strong defense)		
A09: Security Logging and Monitoring Failures	A.12 Operations security	Assessed	Compliant (<redacted>'s Web application has implemented strong defense)		
A10: Server-Side Request Forgery (SSRF)	A.13 Communications security	Assessed	Compliant (<redacted>'s Web application has implemented strong defense)		

4. Detailed Findings

01: Improper Access Control ('Business Logic Validation Failure') [M01]				
Observation : During the assessment, it was observed that the 'assigned user' can raise a ticket on behalf of the 'admin/super' user, by manipulating the JSON input value. This can be fixed easily by using the server-side validation that verifies the user-intended JSON request.				
Severity/Business Impact : Medium (4.7/10)				
Impact: In context to <redacted>'s business logic & use, this could be exploited for raising false customer service issues to trigger unwarranted actions. It is recommended that we fix and close this vulnerability, before the Go-Live of the application.				
CWE ID :	284	**Status of the vulnerability :**	Pending for re-validation ('Open')	OPEN
OWASP Top 10 2021 Category :	A01: Broken Access Control	**ISO/IEC 27001 Mapping :**	A.9 Access control	
CVSS Metric Score :	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L	**WSTG Control ID :**	WSTG-ATHZ-02	
Steps To Reproduce :	1. After a successful login, the assessor navigated to the 'Raise Ticket' functionality as an 'Assigned User'. 2. After clicking on the 'Raise Ticket' option, the assessor intercepted the request and modified the following JSON input parameter. (refer evidence Fig 1.1) 3. Assessor forwarded this manipulated request and observed that the ticket was raised successfully and an alert was generated for the same. (refer evidence Fig 1.2)			
Recommendations :	- Enforce Authorization checks. - Use the principle of least-privilege and deny-by-default. - Use RBAC (Role-based-access-control) security mechanism. - Ensure server-side validation of every sensitive request.			
References :	https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html			
Revalidation Remarks :	None, as of 6th September, 2023. To be populated, after the re-validation of this vulnerability.			

4. Detailed Findings

02: Forced Browsing ('Direct Request') [M02]

Observation :
During the assessment, it was observed that the 'assigned user' can force-browse to the 'E Files' functionality which is intended only to the 'admin/super user'. This can be prevented by using a strong access-control mechanism.

Severity/Business Impact : Medium (4.7/10)

Impact:
In context to <redacted>'s business logic & use, this could be exploited to allow unauthorized (assigned user) to view, edit or delete sensitive data, execute administrative functions, that are only allowed to the (admin/super) user. It is recommended that we fix and close this vulnerability, before the Go-Live of the application.

CWE ID :	425	**Status of the vulnerability :**	Pending for re-validation ('Open')
OWASP Top 10 2021 Category :	A01: Broken Access Control	**ISO/IEC 27001 Mapping :**	A.9 Access control
CVSS Metric Score :	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L	**WSTG Control ID :**	WSTG-ATHN-04

Steps To Reproduce :	1. Assessor logged into the application, as an 'assigned user', using Mozilla Firefox. 2. Assessor logged into the application, as an 'admin/super user', using incognito mode of Mozilla Firefox. 3. This allowed the assessor to have 2 concurrent sessions from a single IP address, for 2 different users. 4. Assessor captured the 'E Files' functionality URL from the 'admin/super user's session. 5. In the assigned user's session, the admin copy-pasted this captured URL and was able to view/access the 'E Files' functionality. (refer evidence Fig 2.1)
Recommendations :	- Ensure strong access control policies are in place. - Every resource should check if the requesting user has the appropriate permissions to access it. - Implement role-based access control to ensure that users can only access resources based on their role. This should be implemented at both the function and data level.
References :	https://owasp.org/www-community/attacks/Forced_browsing
Revalidation Remarks :	None, as of 6th September, 2023. To be populated, after the re-validation of this vulnerability.

OPEN

4. Detailed Findings

03: Security Misconfigurations [L01]

Observation :

During the assessment, it was observed that there are minor security misconfigurations in the <redacted> web application, which increase the attack-surface for an external adversary or an attacker. This can be fixed by implementing the suggested recommendations.

Severity/Business Impact : **Low (3.8/10)**

Impact:

In context to <redacted>'s business logic & use, these security misconfigurations do not pose a direct, immediate threat to the business. However, they do create a more permissive environment for potential attackers. Over time, these minor gaps can add up to create significant security risks, leading to compromised data, loss of customer trust, and potential regulatory fines. It's similar to leaving the windows unlocked in a secure building - while it may not guarantee theft, it certainly makes the job easier for thieves. Therefore, while not directly harmful, these issues should not be overlooked and should be addressed to enhance the overall security posture of the web application & business. It is recommended that fix these misconfigurations, as soon as possible.

CWE IDs :	614, 310	**Status of the vulnerability :**	Pending for re-validation ('Open')
OWASP Top 10 2021 Category :	A05: Security Misconfiguration A02: Cryptographic Failures	**ISO/IEC 27001 Mappings :**	A.12 Operations security A.10 Cryptographic controls
CVSS Metric Score :	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:L	**WSTG Control IDs :**	WSTG-SESS-02 WSTG-CRYP-01
Proof of Concept (PoC) :	Assessor observed the following security misconfigurations : a. Missing HTTP Security Headers (ref. evidence Fig. 3.1 & Fig. 3.2) b. Outdated TLS Version supported (ref. evidence Fig. 3.3) c. 'Secure' cookie attribute for session cookie was observed as 'false' (ref. evidence Fig. 3.4) d. Server Information Disclosure (ref. evidence Fig. 3.5) e. Unsigned DNSSEC record (ref. evidence Fig. 3.6 & Fig 3.7) f. Dedicated WAF (Firewall) solution was found missing (ref. evidence Fig. 3.8)		
Recommendations :	- Implement the missing security HTTP headers, in the application's response. Make sure these are implemented for all the pages of the website. Set 'Secure' flag to 'True' for the ASP .NET session cookie. - Disable outdated TLS version 1.0 & 1.1. Use TLS 1.2 & TLS 1.3 with strength A 'ciphers'. Sign the DNSSEC record. - Implement a dedicated WAF (Firewall) solution, such as Imperva, Cloudflare, Akamai, etc.		
References :	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/		
Revalidation Remarks :	None, as of 6th September, 2023. To be populated, after the re-validation of this vulnerability.		

OPEN

5. Security Assessment Summary & Remarks [OWASP Risk Assessment Scorecard]

OWASP Risk Assessment Calculator					
Likelihood factors		**Scale factor**	**Impact factors**		**Scale factor**
Threat Agent Factors			***Technical Impact Factors***		
Skills required	Security penetration skills [9]	9	Loss of confidentiality	Minimal non-sensitive data disclosed [2]	2
Motive	Possible reward [4]	4	Loss of Integrity	Minimal slightly corrupt data [1]	1
Opportunity	Full access or expensive resources required [0]	0	Loss of Availability	Minimal secondary services interrupted [1]	1
Population Size	Internet Users [4]	4	Loss of Accountability	Attack fully traceable to individual [1]	1
Vulnerability Factors			***Business Impact Factors***		
Easy of Discovery	Difficult [3]	3	Financial damage	Damage costs less than to fix the issue [1]	1
Ease of Exploit	Difficult [3]	3	Reputation damage	Minimal damage [1]	1
Awareness	Hidden [4]	4	Non-Compliance	Minor violation [2]	2
Intrusion Detection	Logged and reviewed [3]	3	Privacy violation	Not Applicable [0]	0
Likelihood score:	**3.75**		**Impact score:**	**1.125**	
	Overall Sysilo's Web Application Risk Severity :	**Low**			
OWASP/ISMS Risk severity which is lower than **5.5, confirms that the application is ready for deployment [live staging / launch / CAB approval]					
OWASP/ISMS Risk severity which is greater than **5.5, requires immediate attention before proceeding with the deployment or that includes [live staging / launch / CAB approval]					

Fig. 5.1 <redacted>'s Web Application Risk Severity

OWASP Risk Assessment Summary

Upon applying the OWASP Risk Assessment framework and considering ISO/IEC 27001 risk management guidelines, it has been determined that the aforementioned vulnerabilities are of a manageable level of risk and do not pose a significant threat to data integrity, availability, or confidentiality of the current <redacted>'s in-scope web application. (ref. C-I-A triad)

Go-Live/Deployment Readiness remarks by the 'Assessor'

- According to the observed findings and subsequent risk assessments, the <redacted>'s Web application is ready for the 'Go-Live' stage or CAB approval, if applicable and/or required.
- The vulnerabilities identified do not present a significant level of risk that would warrant delaying the staging. Importantly, identified vulnerabilities can be addressed in parallel as the application goes live, without compromising the overall security posture or an impact to the business operations.

5. Security Assessment Summary & Remarks [Scan Report Summary]

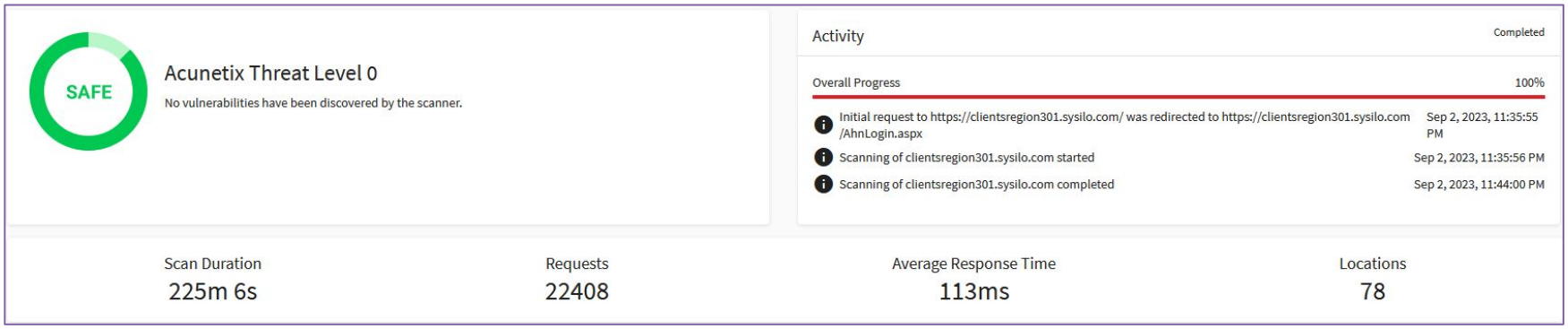


Fig. 5.2 Acunetix Threat & Vulnerability Summary

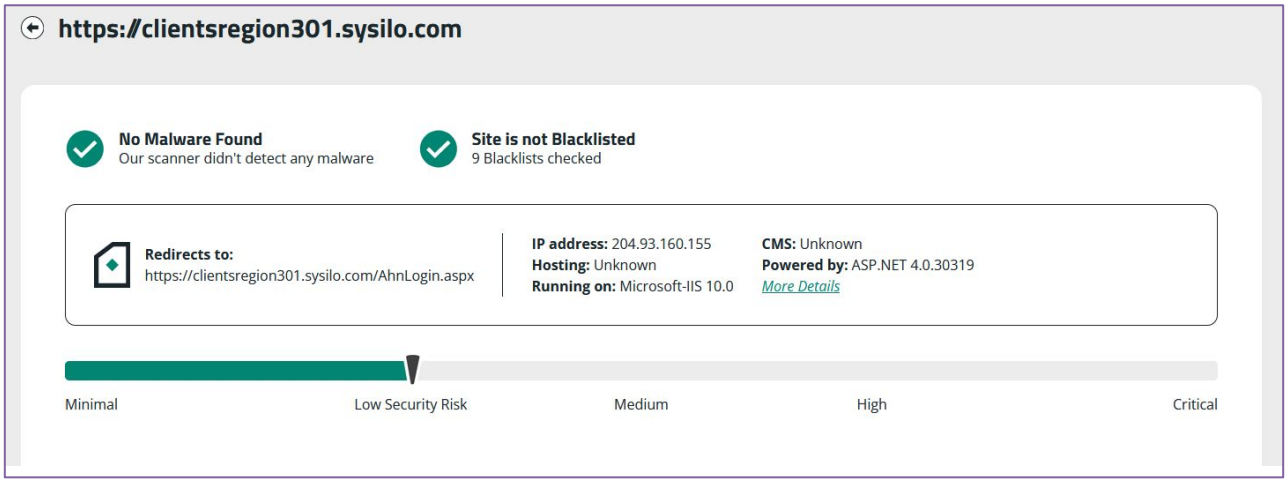


Fig. 5.3 Sucuri Scan - Website Risk Summary

<redacted>'s web application was extensively scanned with the industry leading tools like Acunetix WAS and Burp Suite Professional by the assessor, it was observed that the web application exhibited strong security controls.
These tests are aligned with the OWASP guidelines, which is considered as the gold standard in web application security.

6. Appendix A (Risk Calculation Metrics)

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but need an extreme security expertise to penetrate and attack the web application. It would also require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	0.0	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood X Impact

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm and financial loss.