WEB PENETRATION TEST REPORT

Web Penetration Test Report

ID CODE	VERSION	RELEASE DATE
SECQ120261000	v1.0	April 13, 2026

PREPARED FOR

Neeha

[Cient Name]

&

ASSESSMENT BY

SecureVity
Trust.Protect.Secure

[Company Name]

Document Control

I. DOCUMENT DETAIL

COMPANY	[Company Name]		
DOCUMENT TITLE	Web Penetration Test Report		
REPORT ID	SECQ120261000	**VERSION**	v1.0
START DATE	30-Nov--0001	**END DATE**	30-Nov--0001
APP TYPE	Web Application	**AUTH DATE**	April 13, 2026
CLASSIFICATION	PUBLIC ☐	INTERNAL ☐	**CONFIDENTIAL ☑**

II. DISTRIBUTION LIST

RECIPIENT NAME	TITLE / DESIGNATION	EMAIL ADDRESS
[Cient Name]	Stakeholder	

III. DOCUMENT HISTORY

VER.	DATE	PREPARED BY	SUMMARY OF CHANGE
v1.0	April 13, 2026	gopal.nagwanshi	Initial Release / Final Report

This report contains information concerning potential vulnerabilities of [Cient Name] assets. SECUREVITY recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein. SECUREVITY has retained and secured a copy of the report for customer reference. All other copies of the report have been delivered to [Cient Name].

Table of Contents

As a part of the ongoing security audit of [CLIENT NAME] system at locations, [CLIENT NAME] contracted [COMPANY NAME] to carry out a Penetration Testing exercise on Internal/public facing asset belonging to [CLIENT NAME].

The domain name to be tested was communicated prior to the exercise by [CLIENT NAME] to [COMPANY NAME] consultants. The objective of this exercise was to identify the known set of security vulnerabilities, weaknesses and exploit the same using the set of commercial and open-source tools and scripts.

The exercise was carried with an aim to simulate a hacker attack from the Internet on the target system identified in the scope. It is to be noted here that the results of this exercise may provide a feeling of security to the management, but there is no information system in this world that can be rated as absolutely secured. The system is secured till the extent a vulnerability that can be exploited is discovered. During the present exercise, "High", "Medium" and "Low" severity vulnerabilities were identified, details of which have been presented further in the document.

1.1 OBJECTIVE & OUTCOME

The objectives of the assessment were

- To provide information on any newly identified vulnerabilities/ security risk, if any
- To provide evidence that verifies the possibility of exploiting the security issues identified.
- To recommend measures to mitigate the identified set of vulnerabilities on the target systems.
- To ensures that your Infrastructure component is appropriately designed to protect internal critical / vital resources, information and prevents any unauthorized access.

SECUREVITY regards Penetration Testing activity as an important subset of overall security lifecycle management. The goal here is to identify and demonstrate possibility of unauthorized access to the critical assets that require authorized access, extract the information about the target hosts which may be available to a malicious or an unauthorized user. The aim of penetration testing is to find vulnerabilities at the Service, Operating System, and Application level and exploit the identified known set of vulnerabilities.

2.1 : INFORMATION GATHERING

During this phase of testing, information about the target hosts is gathered to identify the behavior of systems, servers, routers, firewalls etc. The information will help in build a picture or footprint of what the target network looks like.

Thorough Port Scanning	Port scans attempt to identifying both TCP and UDP ports opened/closed/filtered on the target system. A scan of all possible ports TCP (1–65535)
System and Service Identification	The objective of this step is to examination of the active services listening behind the services/ports.
Operating System Fingerprinting	The next objective is to determine the type of operating system. Different OS finger printing techniques along with reconnaissance tools.

2.2 : VULNERABILITY ASSESSMENT

The objective of this step is to identify various vulnerabilities associated with the hosts. This can be achieved by using various automated tools; the input to tools will be target host details like IP address or host OS or service details wherein the scan can be customized specifically for those applications / services running on the hosts. During this step, multiple automated tools are used and the output from these tools is correlated to ascertain the existing vulnerabilities and to reduce the number of false positives.

Vulnerability Research	The objective of this step is to identify, understand and research upon the vulnerabilities identified during the vulnerability identification step.
Vulnerability Verification	The objective of this step is to refine the list of various vulnerabilities associated with the target hosts using manual methods. need to be verified again to reduce any false positives and to increase the accuracy of the exercise.

2.3 : VULNERABILITY EXPLOITATION

MAPPING EXPLOIT

The objective of this step is to find and map exploits associated with various vulnerabilities.

EXPLOITATION

The vulnerabilities discovered in the previous step are exploited using various exploit method and tools, both open source and commercial.

RECORDING EVIDENCE

The logs or proof of successful exploitation (if any) will be recorded as screenshots.

2.4 : REPORTING & DOCUMENTATION

This report will detail about exercise conducted and the successful penetration / assessment along with the proof of exploitation (if any) and mitigation strategies recommended against the security issues identified.

2.5 : MITIGATION APPROACH

The report will include detailed mitigation strategies recommended against the security issues identified during the penetration testing exercise. Each vulnerability will be addressed with specific remediation steps and priority levels.

4.1 TESTING TOOLSET

Open source and commercial tools (not limited to) were used by SECUREVITY during the course of PT exercise like:

Burp Suite

Web Application Security Testing

Nessus

Automated Vulnerability Scanning

Acunetix

Web Vulnerability Assessment

Nmap

Network Discovery & Port Scanning

SQLmap

Automated SQL Injection Testing

Nikto:Web server scanner that tests Web servers for dangerous files/CGIs, outdated server software and other problems.

Specialized Security Analysis

Sslscan:Is a very efficient program that allows you to detect SSL versions & cipher suites (including TLS version checker) and checks for vulnerabilities like Heartbleed and POODLE.

Specialized Security Analysis

Metasploit

Exploitation and Validation

3. SEVERITY CLASSIFICATION

Throughout the document, each vulnerability or risk identified has been labeled as a finding and categorized as High, Medium or Low. These terms are defined below:

Vulnerability Name		
Vulnerable URL / IP		
Risk	**Risk Level**	**Description**
	High	• The vulnerability may result in high-risk exposure and should be addressed immediately. • The vulnerability may be exploited to compromise the system.
	Medium	• The vulnerability may result in medium risk exposure and should be addressed as soon as possible. • The vulnerability may be exploited to compromise the system.
	Low	• The vulnerability may result in low-risk exposure and may be addressed in due time. • These vulnerabilities cannot compromise the system; these vulnerabilities coupled with other vulnerabilities may be exploited to compromise a part of an IT system.

Level of access required	**Ease of Exploitation**	**Impact**		
		High	**Medium**	**Low**
Internal (Local Network)	Easy	**MEDIUM**	**MEDIUM**	**LOW**
	Moderate	**MEDIUM**	**LOW**	**LOW**
	Difficult	**LOW**	**LOW**	**LOW**
External (Public Facing)	Easy	**HIGH**	**HIGH**	**MEDIUM**
	Moderate	**HIGH**	**MEDIUM**	**LOW**
	Difficult	**MEDIUM**	**MEDIUM**	**LOW**

4. EXECUTIVE SUMMARY

This current assignment has been focused on the risk assessment and the open vulnerabilities exposure. This testing did not explicitly attempt Denial of Service (DOS) attacks. We performed the security assessment of the web application as an authorized and an unauthorized user. A black box test simulating a typical external hacker\'s view of the organization was performed.

4.1 Engagement Scope

The URLs within the scope of the PT have been tested:

Sr No.	Application URL
1	https://abc.socope.com.

4.2 Severity Graph:

4.3 Recommendation Summary

This current assignment has been focused on the risk assessment and the open vulnerabilities exposure. This testing did not explicitly attempt Denial of Service (DOS) attacks. We performed the security assessment of the web application as an authorized and an unauthorized user. A black box test simulating a typical external hacker's view of the organization was performed.

5. VULNERABILITY SUMMARY:

SR. NO	VULNERABILITY NAME	SEVERITY	OWASP TOP 10
1	Insecure File Upload	HIGH	A1-2021-Injection

Vulnerability Re-Assessment Summary

SR. NO	VULNERABILITY NAME	SEVERITY	RE-VALIDATION STATUS
1	Insecure File Upload	HIGH	Closed

6. Penetration Test Vulnerability Details:

6.1 INSECURE FILE UPLOAD

1	VULNERABILITY NAME	**Insecure File Upload**
	VULNERABLE URL	https://abc.com/
	OWASP TOP 10	**A1-2021-Injection**
	VULNERABLE PARAMETER	URL
	VULNERABILITY STATUS	Open
	RISK	**HIGH**
	DESCRIPTION	It is observed that application is accepting insecure file while uploading svg formate.
	IMPACT	Dangerous files can be uploaded causing RCE.
	MITIGATION	• Validate file types • Enforce size limits
	REFERENCE	https://portswigger.net/web-security/file-upload

Proof of Concept (POC):

1 Step-1: Upload SVG

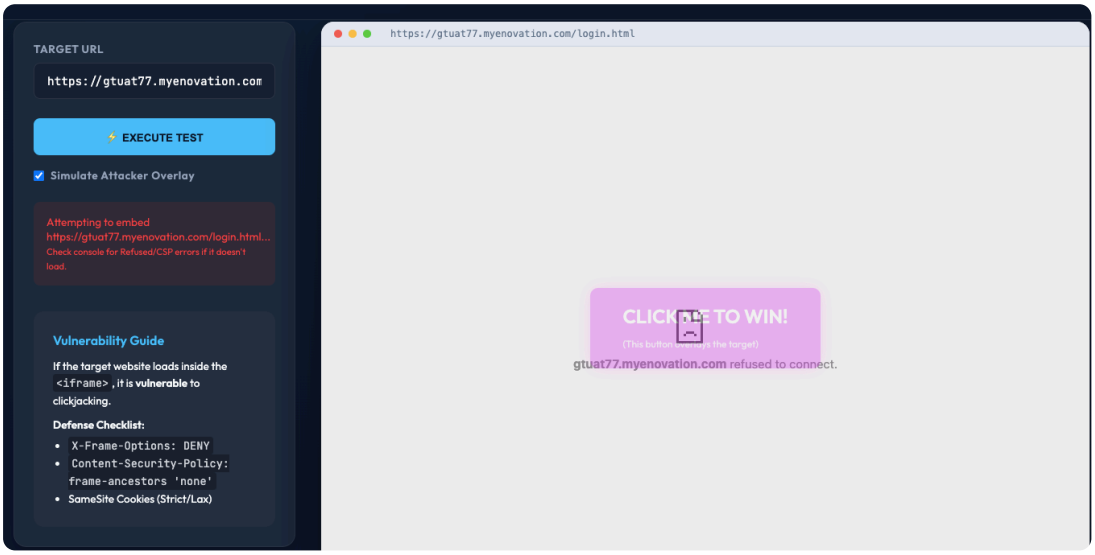

EXHIBIT 1.1: CLICKJACKING.PNG

FINAL CONCLUSION

OVERALL RISK: MEDIUM

This analysis is based on the assessment and with the newly identifies flaws, known threats and best practices as of the date of this report.
We recommend that all modifications suggested in this document be performed in order to ensure the overall security of critical IT infrastructure components.
Please note that the technologies and risks change over time, the weaknesses with the operation of the systems described in this report, as required, reducing exposure to these vulnerabilities related actions.
It is observed that after completion of testing, website is vulnerable with Sensitive Data Exposure and Test Functionality in Production Server and other vulnerability which you need to be patched.

? Security Assessment Validated

April 13, 2026

REPORT AUTHORITY:

Web Application (OWASP Top 10 2021) Coverage

CATEGORY	TEST CASE	STATUS
A01:2021-Broken Access Control	Insecure direct object references (IDOR)	**PASS**
	Bypassing access control checks	**PASS**
	Permissions delegation issues	**PASS**
A02:2021-Cryptographic Failures	Sensitive data transmitted in clear text	**PASS**
	Weak cryptographic algorithms	**PASS**
	Insufficient entropy	**PASS**
	Hardcoded keys	**PASS**
A03:2021-Injection	SQL/NoSQL Injection	**PASS**
	Cross-site Scripting (XSS)	**PASS**
	OS Command Injection	**PASS**
	LDAP Injection	**FAIL**
A04:2021-Insecure Design	Business logic vulnerabilities	**FAIL**
	Insecure error handling	**FAIL**
	Missing rate limiting	**FAIL**
A05:2021-Security Misconfiguration	Default credentials	**FAIL**
	Verbose error messages	**FAIL**
	Directory listing enabled	**PASS**

CATEGORY (CONTINUED)	TEST CASE	STATUS
A06:2021-Vulnerable and Outdated Components	Vulnerable libraries/frameworks	**PASS**
	Outdated web server	**PASS**
	Known CVEs in OS	**FAIL**
A07:2021-Identification and Authentication Failures	Brute force/Credential stuffing	**PASS**
	Insecure session management	**FAIL**
	Weak password policy	**PASS**
A08:2021-Software and Data Integrity Failures	Insecure deserialization	**FAIL**
	Unverified software updates	**PASS**
	Untrusted CDN usage	**FAIL**
A09:2021-Security Logging and Monitoring Failures	Lack of logging for sensitive actions	**PASS**
	Insufficient log monitoring	**FAIL**
A10:2021-Server-Side Request Forgery (SSRF)	Internal service scanning	**PASS**
	Unauthorized cloud metadata access	**FAIL**