CYBERPWN
EMPOWERING CYBER RESILIENCE

THICK CLIENT APPLICATION PENETRATION TESTING REPORT

v1.3

Prepared for: Sutherland Global Services Pvt Ltd

31 July 2026

Disclaimer

This data shall not be disclosed and shall not be duplicated, used, or disclosed in whole or in part for any purpose. If a contract is awarded to 5Sec CyberPWN Technologies Pvt Ltd., as a result 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. The data subject to this restriction is contained in all marked sheets.

CONTENTS

DOCUMENT DETAILS **4**

SCOPE & DURATION 5

EXECUTIVE SUMMARY **6**

Risk Rating Definitions 8

APPROACH AND METHODOLOGY **9**

RESULT OVERVIEW **13**

HIGH LEVEL RECOMMENDATIONS **14**

VULNERABILITIES DETAILS: **15**

1. DLL HIJACKING 15

2. BROKEN AUTHENTICATION 17

3. NO RATE LIMIT ATTACK 19

4. MISSING SECURITY HEADERS 21

5. MISCONFIGURED CSP SECURITY HEADER 23

6. MISCONFIGURED CORS 24

7. MISSING CODE SIGNING 25

8. MISSING SECURITY FLAGS 26

OBSERVATION: **28**

CONCLUSION: **29**

Annexure A – CHANGES TO ENVIRONMENT **30**

Annexure B – TOOLS USED **30**

Annexure C – LIST OF VAPT TESTS PERFORMED **31**

DOCUMENT DETAILS

DOCUMENT CONTROL	
Document Title	**Thick-Client Penetration Testing Report**
Document Classification	Final Report
Last Edit Date	18-May-2026

DOCUMENT HISTORY			
DATE	**VERSION**	**PREPARED BY**	**STATUS**
18-May-2026	1.0	Anand kumar N	Initial Report
31-July-2026	1.3	Anand kumar N	Final Report

CUSTOMER INFORMATION	
Company Name	Sutherland Global Services Pvt Ltd
Address	Gateway Office Parks Pvt. Ltd 2nd, 3rd, 4th ,5th Floor, Block B2 No:16, GST Road, Perungalathur Chennai - Tamil Nadu – 600063 - India
Website	https://www.sutherlandglobal.com/
Contact Name	Sarfraz Amin
Title	Assistant Vice President
Email	sarfrazamin.a@sutherlandglobal.com

CONSULTANT INFORMATION		
Name	**Role**	**Responsibility**
Anand kumar N	Senior Security Engineer	Document Preparation
Manoj K	Security Architect	Document Review
Anuranjan Garnaik	Senior Manager	Document Final Approval

INTRODUCTION

CyberPWN Technologies conducted **Thick-Client Penetration testing** for Sutherland Global Services Pvt Ltd. Based upon the Authorization to Test the application provided by the Company, Cyberpwn followed a testing methodology that sought to identify vulnerabilities and, through manual pentesting determine the impact on to the Company's asset. Cyberpwn Technologies assigned a risk level based on goals achieved during testing.

SCOPE & DURATION

The scope includes **Thick-Client Penetration testing** for below mentioned targets.

Application Name	Version
RobilityDesigner.exe	26.5.0.2
RobilityRunner.exe	26.4.0.2

The test was performed from 11-05-2026 to 18-05-2026 including reporting.

The Re-test was performed from 31-07-2026

LIMITATIONS & CONSTRAINTS

Testing occurred under the following constraints:

- The assessment was performed with the knowledge shared by the sutherland team about the application.
- The assessments were conducted from CyberPWN and the findings made are highly subjective to target application and services visibility and availability at that given point of time.

EXECUTIVE SUMMARY

CyberPWN was engaged by Sutherland to conduct Thick Client penetration testing of client's application. The security assessment was conducted from the CyberPWN Lab at Bangalore, India.

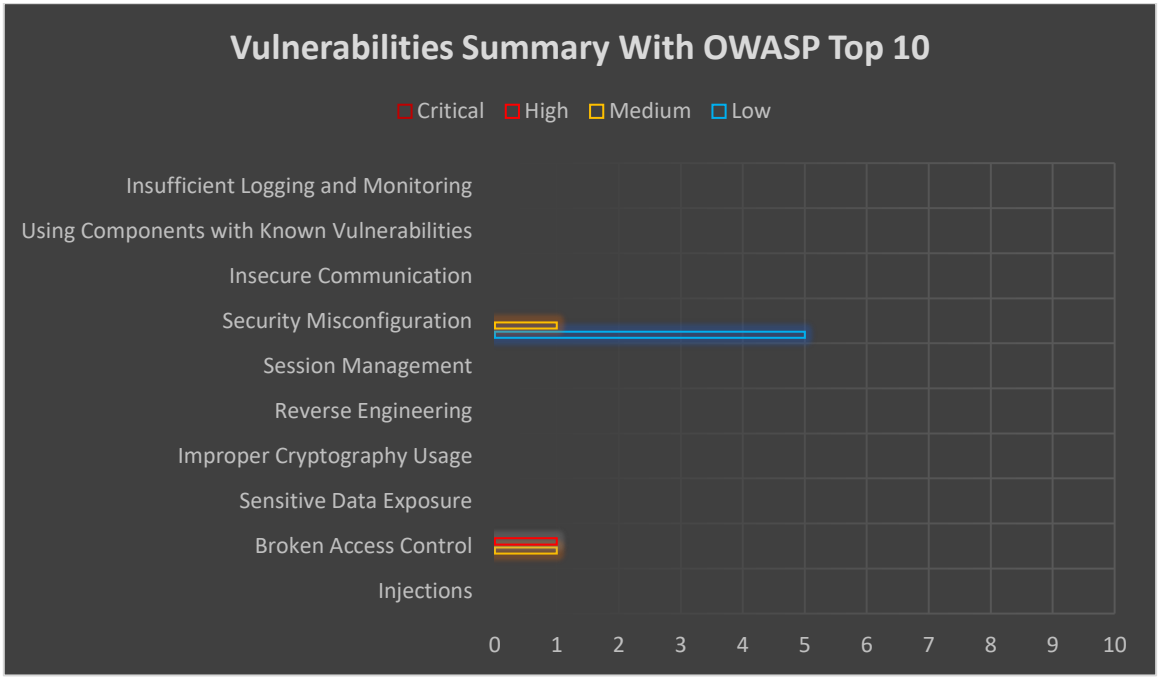
However, the assessment identified 01 High, 02 Medium and 05 Low risk findings as an outcome of thick client application penetration testing.

- The 01 High rated risks pertaining to exploitation vulnerability is DLL Hijacking.
- The 02 Medium rated risks pertaining to exploitation vulnerabilities are Broken Authentication and No Rate Limit Attack
- The 05 Low rated risks pertaining to vulnerabilities are Missing Security Headers, Misconfigured CSP Security Header, Misconfigured CORS, Missing Code Signing, Missing Security Flags.

Summary of Finding

Total Vulnerabilities						
Testing	**Critical**	**High**	**Medium**	**Low**	**Info**	**Total**
Assessment	**00**	**01**	**02**	**05**	**00**	**08**
Revalidation	**00**	**00**	**00**	**00**	**00**	**00**

Finding Categorization



Introduction to Thick Client Penetration Testing:

Thick Client Penetration Testing focuses on evaluating the security of applications installed on end-user systems, encompassing desktop, mobile, or standalone software. This assessment aims to uncover vulnerabilities, weaknesses, and potential attack vectors in the application like memory corruption, race conditions, injection vulnerabilities, transport layer encryption weakness etc.

Vulnerability Scoring

A scoring system is used to grade all of the vulnerabilities listed in this report. Cyberpwn employs the industry standard CVSSv4. It provides a system for determining the severity of vulnerabilities, regardless of the software/hardware platform or service function.

Every vulnerability is assigned a score between 0 and 10, giving each discovered vulnerability a score that aids in identifying the most vulnerable systems and prioritizing responses to each problem. The National Vulnerabilities Database (NVD) uses the CVSS system to calculate scores for almost all known vulnerabilities, and these are the scores referred to in this report.

Further information can be found at https://www.first.org/cvss/calculator/4.0.

https://nvd.nist.gov/

Severity Rating

Based on the severity of the vulnerability, they are assigned below ratings:

CVSS Severity Rating	CVSS Score
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
Informational	0.0

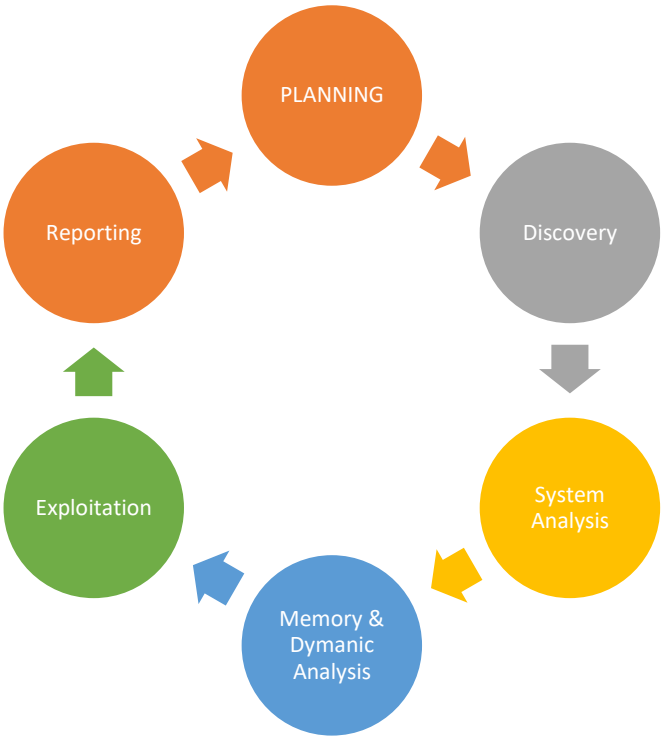
Risk Rating Definitions

Severity Rating	Definitions
Critical	Critical severity vulnerabilities usually have most of the following traits: • A successful attack may lead to complete compromise of the system. • Exploitation can be done remotely over an untrusted connection – such as the Internet. • Exploiting the vulnerability is very easy or straightforward. It may not require privilege accounts or user interaction. • It has a very significant impact on confidentiality, integrity and/or availability of the targeted system
High	High severity vulnerabilities demonstrate some of the following characteristics: • It is not straight-forward to exploit and may require some user interaction and has minimum dependency. • Usually gives an attacker elevated privilege. • It has a significant impact on confidentiality, integrity, and availability
Medium	• Vulnerabilities scored medium generally: • Require specific user privileges or conditions to execute the attack. • Grant attacker access to non-critical privileged functionality/data. • Moderately affects Confidentiality, Integrity, or availability
Low	Vulnerabilities scored low usually exhibit some of the following characteristics: • They have little impact on the confidentiality, integrity or availability of the organization's data or assets. • Requires a great amount of computational power to exploit the vulnerability. • Require excessive privileges or access to execute an attack. • Exploits are not known publicly.

APPROACH AND METHODOLOGY

Cyberpwn Technologies penetration testing methodology is based upon frameworks and standards mentioned below and it contains the following phases:

OWASP TOP 10
SANS TOP 25
The Penetration Testing Execution Standard (pentest-standard.org)
National Institute of Standards and Technology (NIST)
OSSTMM (Open-Source Security Testing Methodology Manual)



PLANNING

- Cyberpwn Technologies prepares for initial planning sessions with the Company by reviewing the Company's business processes, key personnel, physical locations, and Internet-accessible footprint.
- Cyberpwn Technologies and the Company collaborate to create the rules, attack scenarios, and goals for testing.
- The Company may provide additional documentation and access to applications, systems and networks to facilitate targeted testing.
- The Customer Company is responsible for ensuring that the scope contains all targets for testing and that the Company has the authority to permit Cyberpwn Technologies to perform penetration testing against the identified targets.

Thick client security assessment can be divided into below four major parts.

Static test

- **Source code decompilation**

  Based on the technology stack used to generate the binary file, one can attempt with a relevant decompiler to access the source code. For .Net, one can use ILSpy or dnSpy. Jd-gui or jadx for java-based application. IDA Pro can be used for C/C++ with varied degree of success.

- **Code Injection**

  If an attacker is successful in decompiling the source code then attempt to introduce new or edit existing code to perform malicious actions such as a backdoor, etc. and recompile the application.

- **Configuration files in cleartext**

  If configuration and set-up files are in cleartext then they may contain information such as username, password, API key and other sensitive client server details. Report if such information found during inspection.

- **Test storage mechanism.**

  Observe how the application is storing data at rest.

Dynamic test

- **Input validation**

  Test all input fields for issues such as SQL injection, command injection, buffer overflow, file system attack, etc.

- **Test File upload**

  If application provides file upload feature, then test if an attacker can upload malicious custom file. Also, test how does application parses very big file size.

- **Broken authentication & session management**

  Test how application performs authentication and handles session management. Report the usage of weak password, possibility of user enumeration, improper session expiry, etc.

- **Log forging**

  If the application is maintaining logs, then attempt to tamper log entries with malicious out-of-band payloads, spoof data, append large data to file, etc.

- **Weak GUI control**

  Inspect GUI controls of the application to learn if it is possible to enable additional/unintended features or options to current user. Tools that can aid in testing this are WinSpy++ and WinManipulate.

System test

- **Test for sensitive data in memory**

  Check RAM memory for how data is present when application is running. One can potentially find credential in cleartext and other important information. Winhex or ProcDump along with Volatility can extract and analyze memory.

- **Dependency mapping**

  An Attacker can use Process Explorer and ProcMon from SysInternals Suite to observe what dependency the application has.

- **Privilege level**

  Using icacls, one should check for privilege/permissions on the files and directories the thick client uses. If any excessive permission is provided, a missing .dll, DLL hijacking should be checked.

Network Test

- **Testing transmission of sensitive data**

  Observe how data is passed over the wire. Report usage of sensitive data such as user credentials, personally identifiable information (PII), etc. transmitted in cleartext.

- **Testing weak encryption**

  Usage of weak encryption such as MD5, RC4, etc. may result in broken authentication, spoofing attack, key leakage and poor integrity of data in transit and must be reported.

- **Testing SSL/TLS usage**

  Check for presence of usage of weak cipher suites, security policies, deprecated protocols and misconfigurations.

REPORTING

Cyberpwn Technologies creates a report that contains, at minimum, the following items:

- **Executive Summary** - provides a high-level overview of the testing results and is intended to be read by executives, customers, and business partners.

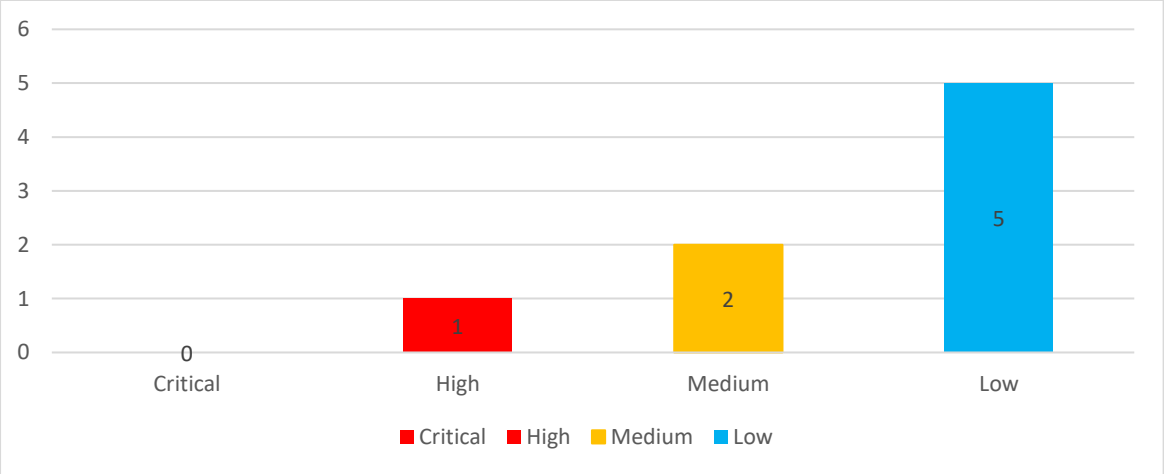
- **Findings** - describes each exploitable vulnerability. The findings results are intended to be distributed.
- to technical teams
- **Recommendations** - recommendations on how to resolve each identified issue.
- **Risk Ranking** - each issue identified is assigned a risk ranking that is derived from the Common Vulnerability Scoring System (CVSS). The rating is based on the specific instances identified in the company environment.
- **Steps to Reproduce** - additional details that provide enough information such that the issue can be replicated by technical teams.
- **Rescan** - updates about the finding, such as retesting status or management responses and revalidation report.

RESULT OVERVIEW

Cyberpwn Technologies Security team discovered 08 vulnerabilities in Robility.AI. The below table summarizes the list of vulnerabilities with corresponding risk ratings.

SL. No.	Vulnerability Name	Severity Rating	Revalidation status
1.	DLL Hijacking	High	CLOSED(EXCEPTION)
2.	Broken Authentication	Medium	CLOSED
3.	No Rate Limit Attack	Medium	CLOSED
4.	Missing Security Headers	Low	CLOSED
5.	Misconfigured CSP Security Header	Low	OUT OF SCOPE
6.	Misconfigured CORS	Low	CLOSED
7.	Missing Code Signing	Low	CLOSED
8.	Missing Security Flags	Low	CLOSED

GRAPHICAL PRESENTATION



HIGH LEVEL RECOMMENDATIONS

The following recommendations offer guidance on enhancing the security posture of Robility.AI:

- Load DLLs only from trusted absolute paths and validate all external dependencies before execution.
- Enforce proper authentication checks and validate user credentials before granting access tokens or protected resources.
- Implement rate limiting and throttling controls on sensitive API endpoints to prevent abuse.
- Configure all recommended HTTP security headers to enhance client-side protection.
- Implement a strict Content Security Policy that allows resources only from trusted sources.
- Restrict CORS to specific trusted origins instead of allowing wildcard or untrusted domains.
- Digitally sign application binaries to ensure integrity and authenticity.

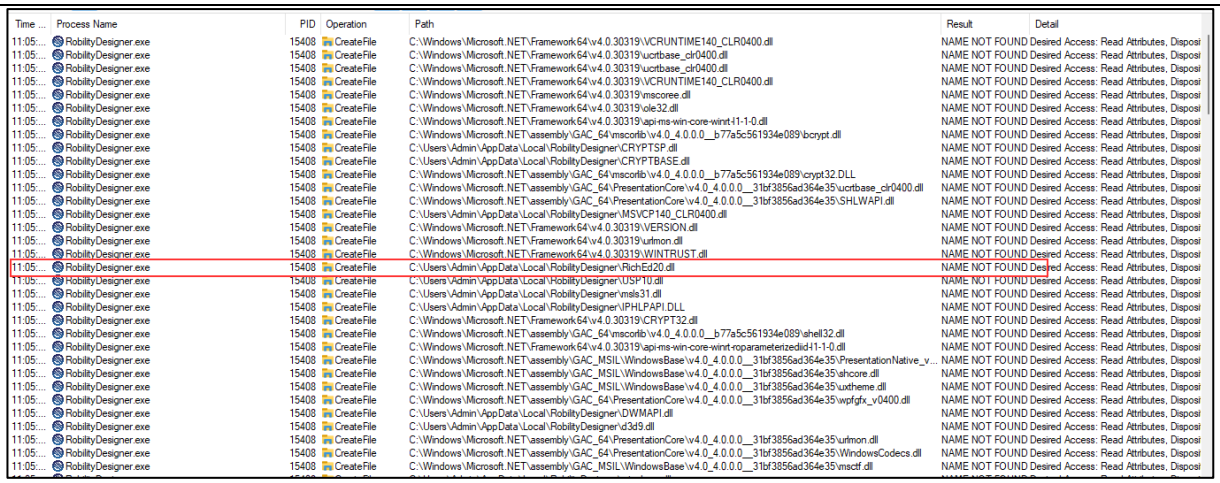
VULNERABILITIES DETAILS:

1. DLL HIJACKING	
Application	RobilityRunner.exe RobilityDesigner.exe
Revalidation Status	**CLOSED(EXCEPTION)**
Severity	High
CVSS Score	7.1
CVSS String	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N
Description	During the assessment, it was observed that application is Vulnerable to DLL Hijacking. DLL Hijacking happens by placing a malicious DLL in a directory (in the absence of a legitimate DLL), which is then loaded by the application instead of the legitimate DLL. This causes the malicious DLL to load with the same privileges as the application, thus causing a privilege escalation.
Impact	The impact includes unauthorized execution of arbitrary code, privilege escalation, data theft, manipulation of applications, system persistence, propagation to other vulnerable applications, and bypassing security measures.
Remediation	It is recommended to: • Latest updates should be installed to the security software and operating system. • Disable loading of DLL files from remote network shares. • Use Hash Signature mechanism to identify trusted DLL files.
Reference	https://learn.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-security

Proof of Concept:

Steps:

1. Open the filtering tool and run the RobilityDesigner Application.
2. Apply the filter to show RobilityDesigner Application processes and to only display active files with a path that ends with .dll and filter the result with NAME NOT FOUND Keyword.
3. From below POC we can notice RichEd20.dll is not present in Application folder. Creating a Malicious RichEd20.dll file.
4. Start the Application again with the filter process as RobilityDesigner and to only display active files with a path that ends with RichEd20.dll and filter the result with SUCCESS keyword.
5. After running the RobilityDesigner malicious code in RichEd20.dll file will be executed.



Time ...	Process Name	PID	Operation	Path	Result	Detail
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\VCRUNTIME140_CLR0400.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ucrtbase_clr0400.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ucrtbase_clr0400.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\VCRUNTIME140_CLR0400.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoree.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ole32.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\api-ms-win-core-winrt-l1-1-0.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\bcrypt.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\CRYPTSP.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\CRYPTBASE.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\crypt32.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_64\PresentationCore\v4.0_4.0.0.0__31bf3856ad364e35\ucrtbase_clr0400.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_64\PresentationCore\v4.0_4.0.0.0__31bf3856ad364e35\SHLWAPI.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\MSVCP140_CLR0400.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\VERSION.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\urlmon.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\WINTRUST.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\RichEd20.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\USP10.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\msls31.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\IPHLPAPI.DLL	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\CRYPT32.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_64\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\shell32.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\api-ms-win-core-winrt-roparameterizediid-l1-1-0.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_MSIL\WindowsBase\v4.0_4.0.0.0__31bf3856ad364e35\PresentationNative_v...	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_MSIL\WindowsBase\v4.0_4.0.0.0__31bf3856ad364e35\uxtheme.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_64\PresentationCore\v4.0_4.0.0.0__31bf3856ad364e35\wpfgfx_v0400.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\DWMAPI.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\d3d9.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_64\PresentationCore\v4.0_4.0.0.0__31bf3856ad364e35\urlmon.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_64\PresentationCore\v4.0_4.0.0.0__31bf3856ad364e35\WindowsCodecs.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\Microsoft.NET\assembly\GAC_MSIL\WindowsBase\v4.0_4.0.0.0__31bf3856ad364e35\msctf.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposi

FIGURE 1:APPLICATION PROCESS WITH .DLL FILES

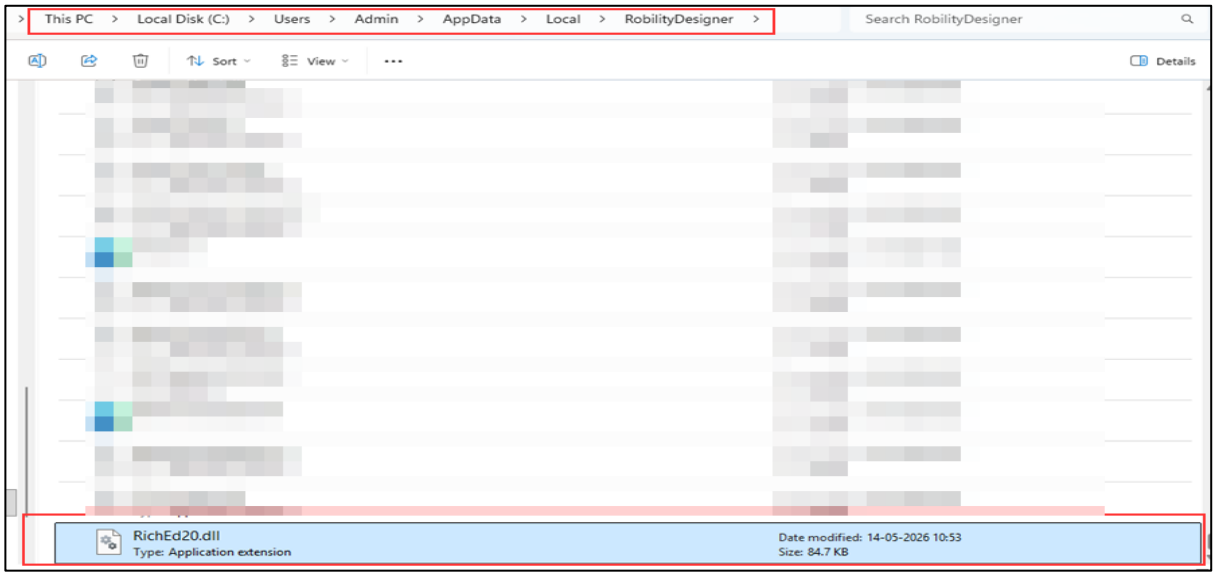
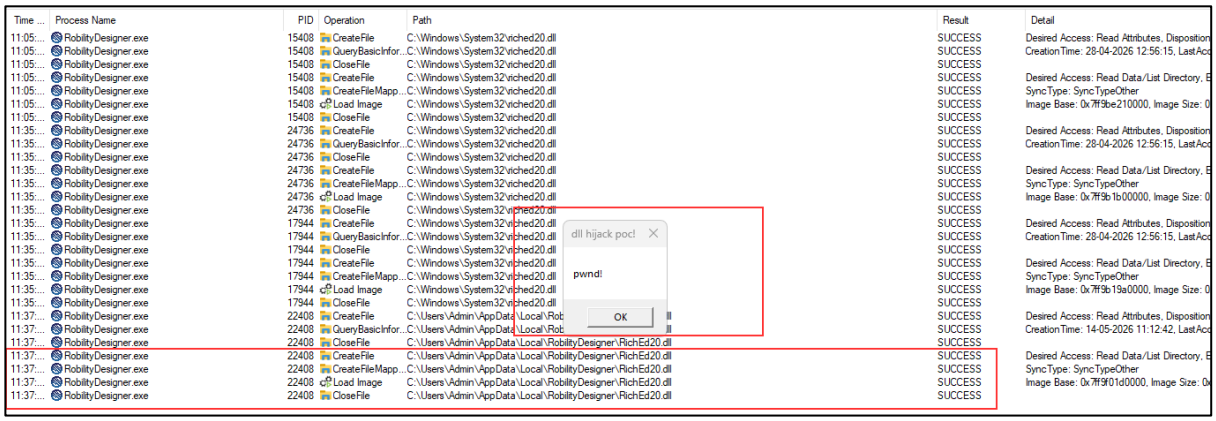


FIGURE 2:MALICIOUS RICHED20.DLL PLACED



Time ...	Process Name	PID	Operation	Path	Result	Detail
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\System32\riched20.dll	SUCCESS	Desired Access: Read Attributes, Disposition
11:05:...	RobilityDesigner.exe	15408	QueryBasicInfor...	C:\Windows\System32\riched20.dll	SUCCESS	CreationTime: 28-04-2026 12:56:15, LastAcc
11:05:...	RobilityDesigner.exe	15408	CloseFile	C:\Windows\System32\riched20.dll	SUCCESS	
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Windows\System32\riched20.dll	SUCCESS	Desired Access: Read Data/List Directory, E
11:05:...	RobilityDesigner.exe	15408	CreateFileMapp...	C:\Windows\System32\riched20.dll	SUCCESS	SyncType: SyncTypeOther
11:05:...	RobilityDesigner.exe	15408	Load Image	C:\Windows\System32\riched20.dll	SUCCESS	Image Base: 0x7ff9be210000, Image Size: 0
11:05:...	RobilityDesigner.exe	15408	CloseFile	C:\Windows\System32\riched20.dll	SUCCESS	
11:35:...	RobilityDesigner.exe	24736	CreateFile	C:\Windows\System32\riched20.dll	SUCCESS	Desired Access: Read Attributes, Disposition
11:35:...	RobilityDesigner.exe	24736	QueryBasicInfor...	C:\Windows\System32\riched20.dll	SUCCESS	CreationTime: 28-04-2026 12:56:15, LastAcc
11:35:...	RobilityDesigner.exe	24736	CloseFile	C:\Windows\System32\riched20.dll	SUCCESS	
11:35:...	RobilityDesigner.exe	24736	CreateFile	C:\Windows\System32\riched20.dll	SUCCESS	Desired Access: Read Data/List Directory, E
11:35:...	RobilityDesigner.exe	24736	CreateFileMapp...	C:\Windows\System32\riched20.dll	SUCCESS	SyncType: SyncTypeOther
11:35:...	RobilityDesigner.exe	24736	Load Image	C:\Windows\System32\riched20.dll	SUCCESS	Image Base: 0x7ff9b1b00000, Image Size: 0
11:35:...	RobilityDesigner.exe	24736	CloseFile	C:\Windows\System32\riched20.dll	SUCCESS	
11:35:...	RobilityDesigner.exe	17944	CreateFile	C:\Windows\System32\riched20.dll	SUCCESS	Desired Access: Read Attributes, Disposition
11:35:...	RobilityDesigner.exe	17944	QueryBasicInfor...	C:\Windows\System32\riched20.dll	SUCCESS	CreationTime: 28-04-2026 12:56:15, LastAcc
11:35:...	RobilityDesigner.exe	17944	CloseFile	C:\Windows\System32\riched20.dll	SUCCESS	
11:35:...	RobilityDesigner.exe	17944	CreateFile	C:\Windows\System32\riched20.dll	SUCCESS	Desired Access: Read Data/List Directory, E
11:35:...	RobilityDesigner.exe	17944	CreateFileMapp...	C:\Windows\System32\riched20.dll	SUCCESS	SyncType: SyncTypeOther
11:35:...	RobilityDesigner.exe	17944	Load Image	C:\Windows\System32\riched20.dll	SUCCESS	Image Base: 0x7ff9b19a0000, Image Size: 0
11:35:...	RobilityDesigner.exe	17944	CloseFile	C:\Windows\System32\riched20.dll	SUCCESS	
11:37:...	RobilityDesigner.exe	22408	CreateFile	C:\Users\Admin\AppData\Local\Rob	SUCCESS	Desired Access: Read Attributes, Disposition
11:37:...	RobilityDesigner.exe	22408	QueryBasicInfor...	C:\Users\Admin\AppData\Local\Rob	SUCCESS	CreationTime: 14-05-2026 11:12:42, LastAcc
11:37:...	RobilityDesigner.exe	22408	CloseFile	C:\Users\Admin\AppData\Local\RobilityDesigner\RichEd20.dll	SUCCESS	
11:37:...	RobilityDesigner.exe	22408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\RichEd20.dll	SUCCESS	Desired Access: Read Data/List Directory, E
11:37:...	RobilityDesigner.exe	22408	CreateFileMapp...	C:\Users\Admin\AppData\Local\RobilityDesigner\RichEd20.dll	SUCCESS	SyncType: SyncTypeOther
11:37:...	RobilityDesigner.exe	22408	Load Image	C:\Users\Admin\AppData\Local\RobilityDesigner\RichEd20.dll	SUCCESS	Image Base: 0x7ff9f01d0000, Image Size: 0
11:37:...	RobilityDesigner.exe	22408	CloseFile	C:\Users\Admin\AppData\Local\RobilityDesigner\RichEd20.dll	SUCCESS	

FIGURE 3:MALICIOUS RICHED20.DLL HAS BEEN LOADED WITH THE RESULT SUCCESS AND GOT EXECUTED

2. BROKEN AUTHENTICATION	
Application / URL	https://robility.sutherlandglobal.com/HubAPI/token
Revalidation Status	**CLOSED**
Severity	Medium
CVSS Score	6.3
CVSS String	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
Description	During assessment, it was observed that the application's token generation endpoint issued a valid access token without requiring user credentials. By sending a POST request containing only the grant_type=password parameter, the server returned a valid bearer token. The generated token could then be used to access application functionalities and APIs without prior authentication, indicating improper authentication enforcement.
Impact	An unauthenticated attacker can obtain valid access tokens and access protected application functionality without providing legitimate credentials. Depending on the token scope, this may lead to unauthorized access to sensitive information, account impersonation, or execution of privileged actions within the application.
Remediation	• Enforce strict credential validation before issuing access tokens. • Ensure grant_type=password requests require valid username and password parameters. • Validate token issuance flows against secure OAuth implementation guidelines. • Restrict token scopes and verify authorization on every backend API endpoint. • Log and monitor anomalous token generation attempts from unauthenticated sources.
Reference	https://owasp.org/API-Security/editions/2023/en/0xa2-broken-authentication/
Proof of Concept:	

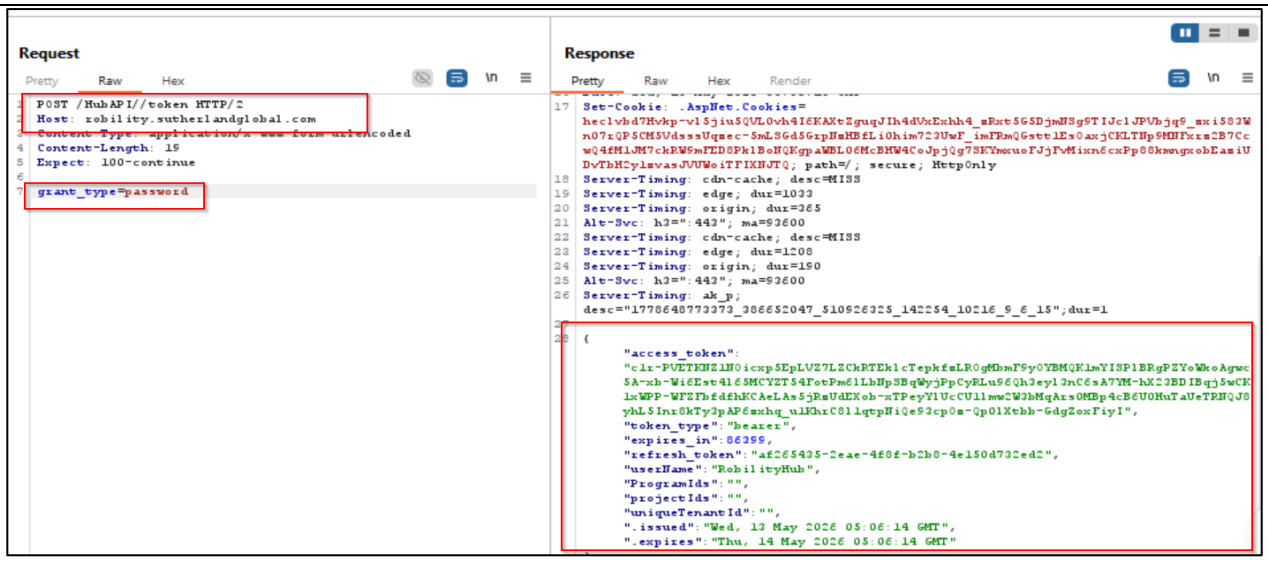


FIGURE 4:APPLICATION'S TOKEN GENERATION ENDPOINT ISSUED A VALID ACCESS TOKEN WITHOUT REQUIRING USER CREDENTIALS

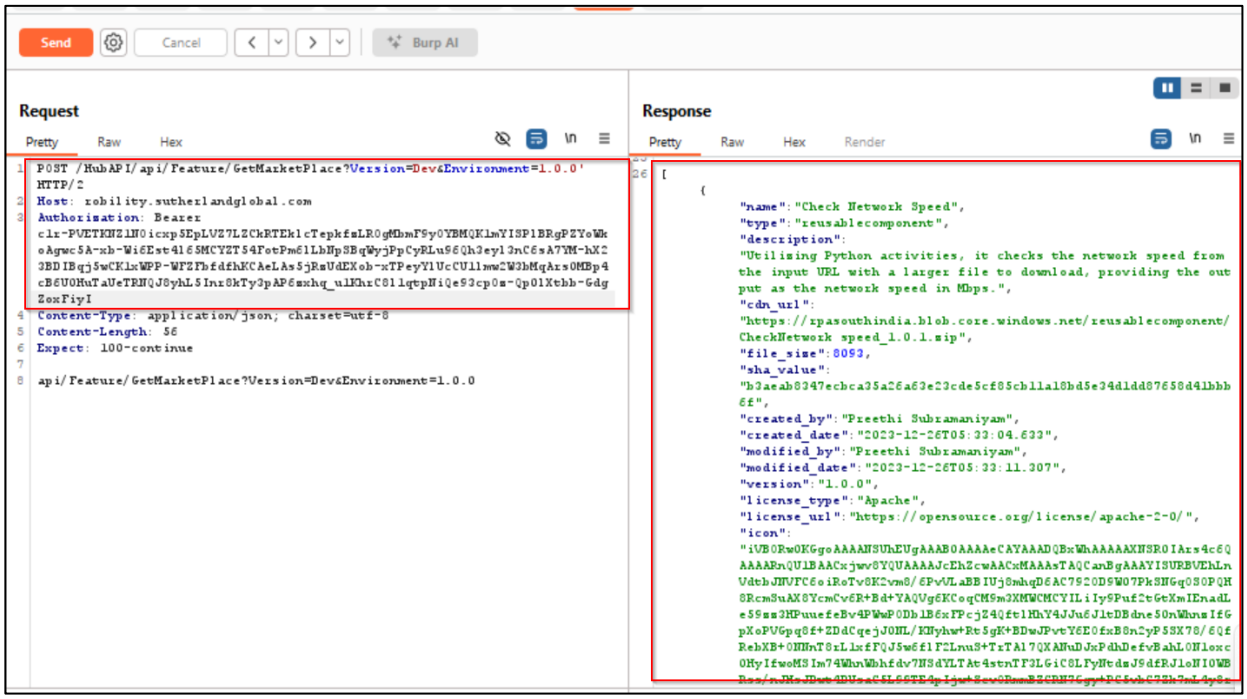


FIGURE 5:ACCESS APPLICATION FUNCTIONALITIES AND APIS WITHOUT PRIOR AUTHENTICATION

3. NO RATE LIMIT ATTACK	
Application / URL	https://robility.sutherlandglobal.com/HubAPI/token https://robility7.sutherlandglobal.com/RobilityServices/DesignerAPI/api/DesignerService/CheckUserLicenseValidation?TenantName=VAPT&Licenseid=908867 **Note: Entire application rate limit should be implemented**
Revalidation Status	**CLOSED**
Severity	Medium
CVSS Score	5.3
CVSS String	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:L/SC:N/SI:N/SA:N
Description	During assessment, it was observed that the token generation endpoint accepted repeated requests without any rate limiting or request throttling controls. An attacker can send unlimited requests to the endpoint and continuously generate access tokens without restriction.
Impact	**Denial of Service (DoS):** Attackers can flood the API with high volumes of requests, overwhelming the server and causing downtime or slow response for legitimate users. **Resource Exhaustion:** The server's computational resources, such as CPU, memory, and storage, can be quickly exhausted, leading to potential crashes or the need for expensive scaling
Remediation	It is recommended to implement the following • Add in rate limits preventing the request being submitted multiple times by the same user at the single time. • Implement Rate Limit Headers: 1. X-RateLimit-Limit: 2. X-RateLimit-Remaining: 3. X-RateLimit-Reset:
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html

Proof of Concept:

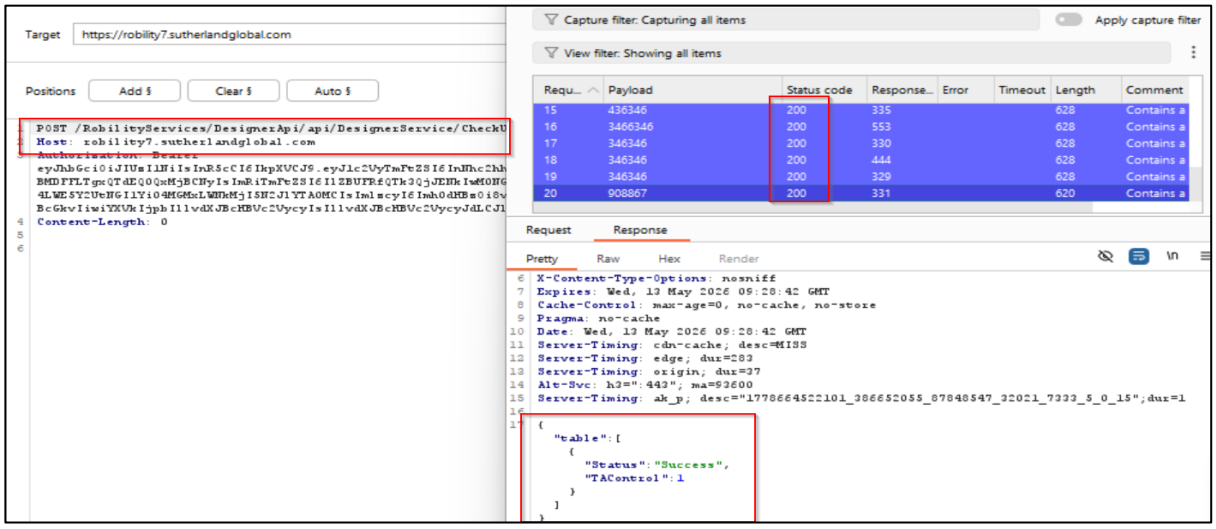


FIGURE 6: THE CHECKUSERLICENSEVALIDATION API SUCCESSFULLY PROCESSED ALL 20 REQUESTS SIMULTANEOUSLY WITHOUT ANY RESTRICTION OR THROTTLING.

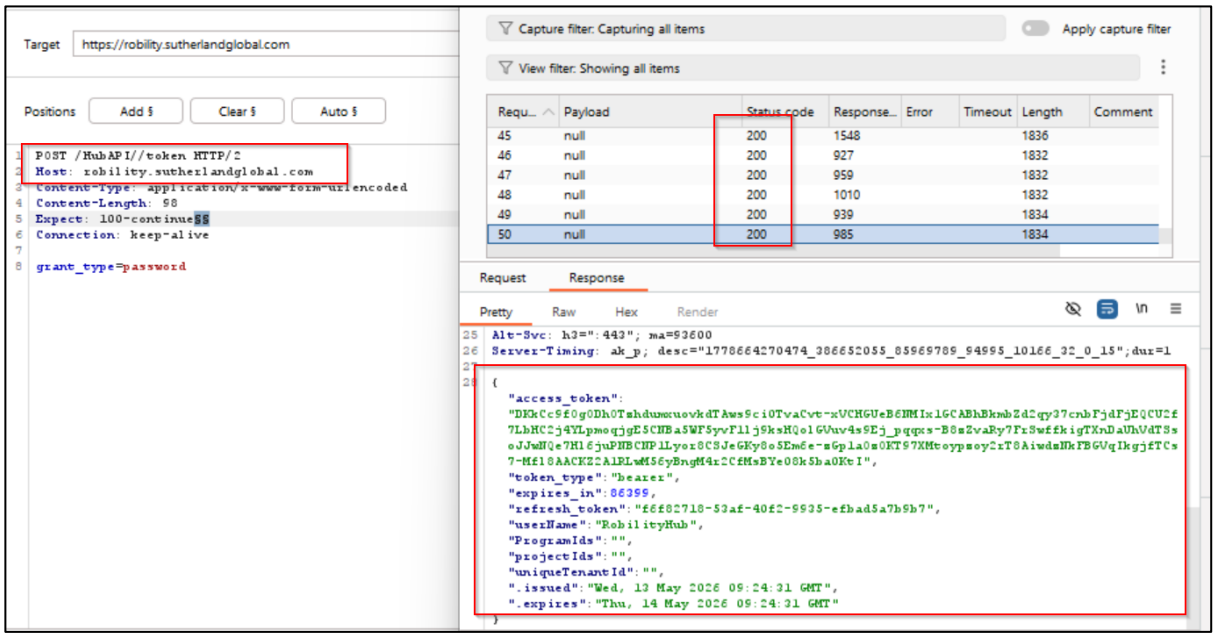


FIGURE 7: THE USER IS ABLE TO GENERATE ACCESS TOKENS MULTIPLE TIMES WITHOUT ANY RESTRICTION OR RATE LIMITING.

4. MISSING SECURITY HEADERS	
Application / URL	https://robility.sutherlandglobal.com/HubAPI/token
Revalidation Status	**CLOSED**
Severity	Low
CVSS Score	2.1
CVSS String	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
Description	During Analysis, it was observed that following is the Security header that is not present in the HTTP response headers. This security header will significantly increase the security state of the application.
Impact	Missing HTTPS Security Headers: 1. A Content Security Policy (CSP): CSP header requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browsers render pages (e.g., inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including Cross-site scripting and other cross-site injections. 2. X-Frame-Options: The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe>, <embed> or <object>. Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites. 3. X-Content-Type-Options: Setting this header will prevent the browser from interpreting files as something else than declared by the content type in the HTTP headers. 4.Strict-Transport-Security (HSTS): HTTP Strict-Transport-Security (HSTS) enforces secure (HTTP over SSL/TLS) connections to the server. This reduces impact of bugs in web applications leaking session data through cookies and external links and defends against Man-in-the-middle attacks. HSTS also disables the ability for users to ignore SSL negotiation warnings.
Remediation	It is recommended to implement these features, by returning the following HTTP headers: • Content-Security-Policy: script-src 'self' • X-Content-Type-Options: nosniff • X-Frame-Options: DENY • Strict-Transport-Security: max-age=16070400; includeSubdomains
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

Proof of Concept:

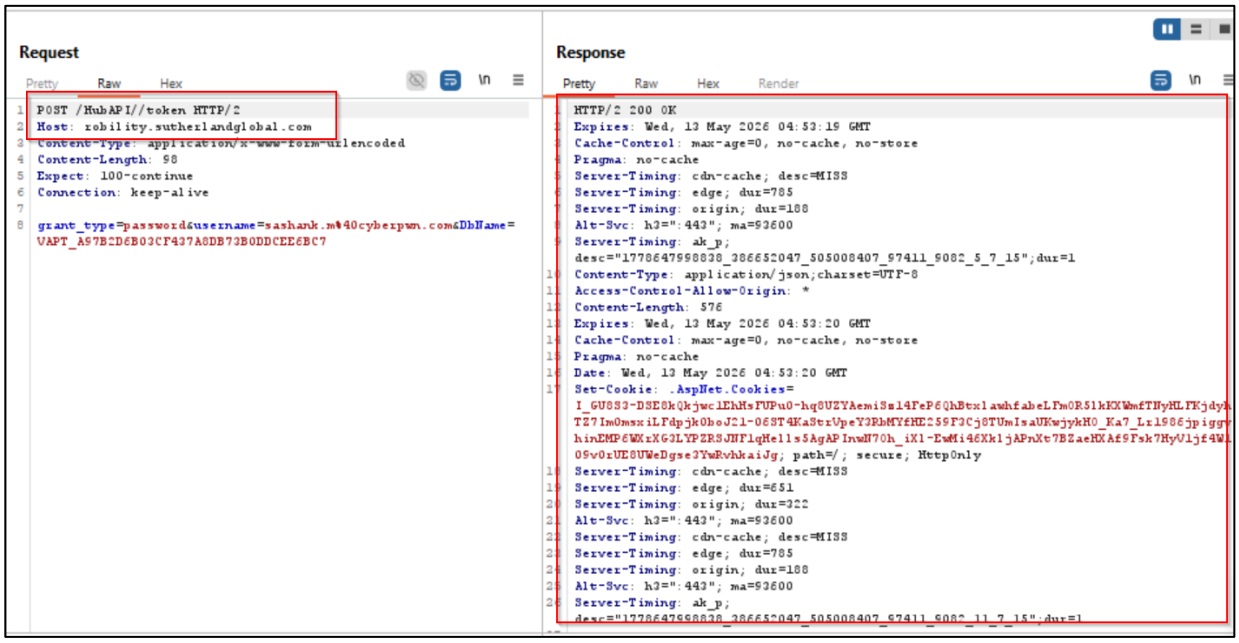


FIGURE 8:MISSING SECURITY HEADERS

5. MISCONFIGURED CSP SECURITY HEADER

Application / URL	https://robility7.sutherlandglobal.com/Robility/UnAuthorization/GetUtcTime
Revalidation Status	**OUT OF SCOPE**
Severity	Low
CVSS Score	2.1
CVSS String	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
Description	A Content Security Policy (CSP) requires careful tuning and precise definition of the policy. By using unsafe-eval, all the application will allow the use of string evaluation functions like eval. By using unsafe-inline, the application will allow the execution of inline scripts, which almost defeats the purpose of CSP.
Impact	When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on the website. An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully. script-src: Restricts the script loading resources to the ones it is declared. By default, it disables inline script executions unless it is permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
Remediation	It is recommended to implement these features, by returning the following HTTP header: • Remove unsafe-eval and unsafe-inline from CSP directives. • Use Hash / Nonce. • Switch to Report-Only and use a report-uri service.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

Proof of Concept:

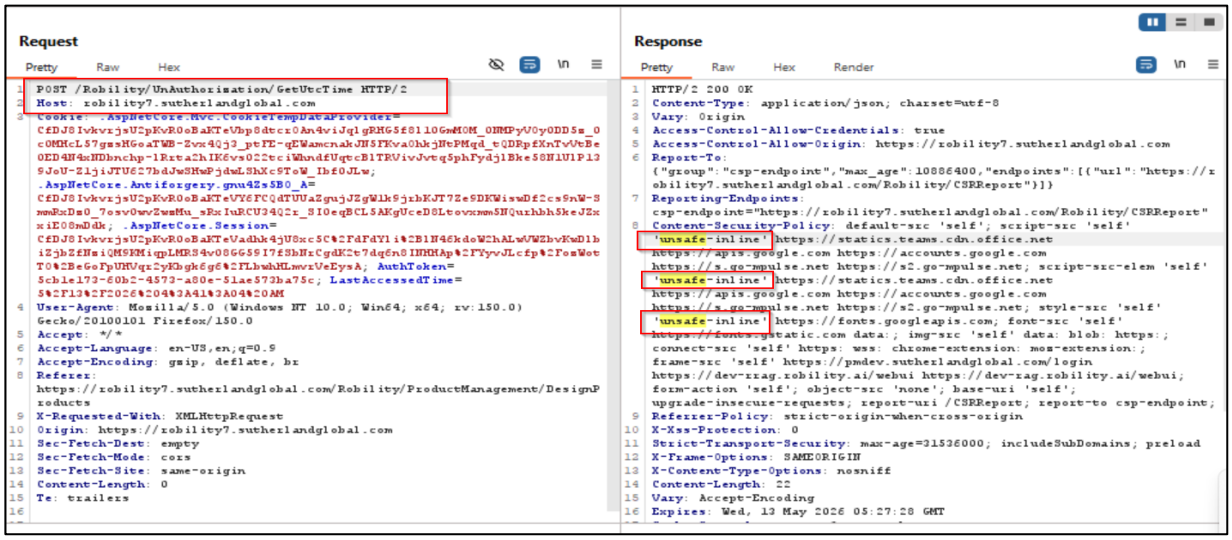


FIGURE 9:MISCONFIGURED CSP SECURITY HEADERS

6. MISCONFIGURED CORS

Application / URL	https://robility.sutherlandglobal.com/HubAPI/token
Revalidation Status	**CLOSED**
Severity	Low
CVSS Score	2.1
CVSS String	CVSS:4.0/AV:L/AC:H/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
Description	During testing, it was observed that the application's Cross-Origin Resource Sharing (CORS) configuration allows requests from any origin by using a wildcard (*) in the Access-Control-Allow-Origin response header. This insecure configuration permits external domains to interact with the application's resources without proper origin restrictions.
Impact	An attacker may host a malicious website and make cross-origin requests to the affected application from a victim's browser. If sensitive APIs are accessible and rely on browser-based authentication/session context, this may lead to unauthorized access to sensitive data, cross-origin data theft, or abuse of application functionality.
Remediation	• Replace the wildcard (*) origin setting with a strict allow list of trusted domains. • Restrict CORS access only to legitimate application domains. • Avoid enabling CORS for sensitive endpoints unless explicitly required. • Validate allowed origins on the server side and review CORS policy regularly.
Reference	https://portswigger.net/web-security/cors

Proof of Concept:

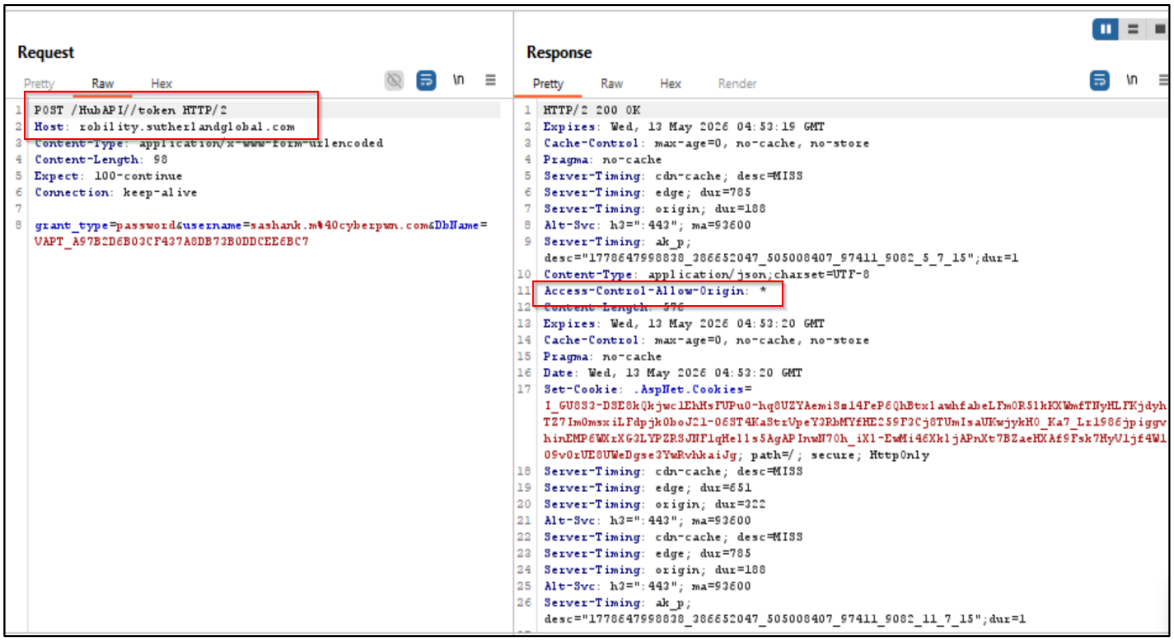
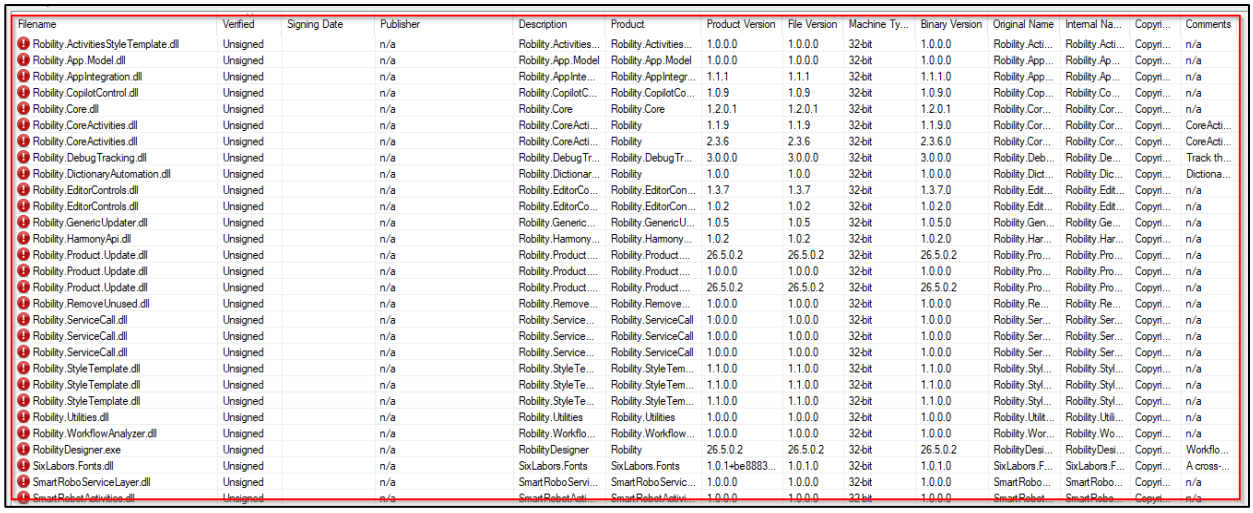


FIGURE 10:MISCONFIGURED CORS

7. MISSING CODE SIGNING

Application / URL	RobilityRunner.exe RobilityDesigner.exe
Revalidation Status	**CLOSED**
Severity	Low
CVSS Score	2.0
CVSS String	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
Description	During the assessment, it was observed that application is missing code signing. The absence of a digital signature in a thick client application refers to the lack of cryptographic validation to ensure the integrity and authenticity of the application. A thick client application is a software program that runs on a user's local machine and often communicates with a remote server for data processing. Without a digital signature, the application's executable files, libraries, or other components can be tampered with, replaced, or spoofed by malicious actors.
Impact	Code Tampering: Attackers can modify the application's binaries or resources to inject malicious code, leading to unauthorized functionality or data theft.
Remediation	It is recommended that to: • Code Signing: Sign the application with a valid code-signing certificate from a trusted Certificate Authority to ensure integrity and authenticity. This will help users and systems trust the application and prevent tampering. • Integrity Checks: Implement integrity verification mechanisms, such as hash checking, to ensure the application has not been modified before execution.
Reference	https://owasp.org/www-project-desktop-app-security-top-10/

Proof of Concept:



Filename	Verified	Signing Date	Publisher	Description	Product	Product Version	File Version	Machine Ty...	Binary Version	Original Name	Internal Na...	Copyri...	Comments
Robility.ActivitiesStyleTemplate.dll	Unsigned		n/a	Robility.Activities...	Robility.Activities...	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.Acti...	Robility.Acti...	Copyri...	n/a
Robility.App.Model.dll	Unsigned		n/a	Robility.App.Model	Robility.App.Model	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.App...	Robility.Ap...	Copyri...	n/a
Robility.AppIntegration.dll	Unsigned		n/a	Robility.AppInte...	Robility.AppIntegr...	1.1.1	1.1.1	32-bit	1.1.1.0	Robility.App...	Robility.Ap...	Copyri...	n/a
Robility.CopilotControl.dll	Unsigned		n/a	Robility.CopilotC...	Robility.CopilotCo...	1.0.9	1.0.9	32-bit	1.0.9.0	Robility.Cop...	Robility.Co...	Copyri...	n/a
Robility.Core.dll	Unsigned		n/a	Robility.Core	Robility.Core	1.2.0.1	1.2.0.1	32-bit	1.2.0.1	Robility.Cor...	Robility.Cor...	Copyri...	n/a
Robility.CoreActivities.dll	Unsigned		n/a	Robility.CoreActi...	Robility	1.1.9	1.1.9	32-bit	1.1.9.0	Robility.Cor...	Robility.Cor...	Copyri...	CoreActi...
Robility.CoreActivities.dll	Unsigned		n/a	Robility.CoreActi...	Robility	2.3.6	2.3.6	32-bit	2.3.6.0	Robility.Cor...	Robility.Cor...	Copyri...	CoreActi...
Robility.DebugTracking.dll	Unsigned		n/a	Robility.DebugTr...	Robility.DebugTr...	3.0.0.0	3.0.0.0	32-bit	3.0.0.0	Robility.Deb...	Robility.De...	Copyri...	Track th...
Robility.DictionaryAutomation.dll	Unsigned		n/a	Robility.Dictionar...	Robility	1.0.0	1.0.0	32-bit	1.0.0.0	Robility.Dict...	Robility.Dic...	Copyri...	Dictiona...
Robility.EditorControls.dll	Unsigned		n/a	Robility.EditorCo...	Robility.EditorCon...	1.3.7	1.3.7	32-bit	1.3.7.0	Robility.Edit...	Robility.Edit...	Copyri...	n/a
Robility.EditorControls.dll	Unsigned		n/a	Robility.EditorCo...	Robility.EditorCon...	1.0.2	1.0.2	32-bit	1.0.2.0	Robility.Edit...	Robility.Edit...	Copyri...	n/a
Robility.GenericUpdater.dll	Unsigned		n/a	Robility.Generic...	Robility.GenericU...	1.0.5	1.0.5	32-bit	1.0.5.0	Robility.Gen...	Robility.Ge...	Copyri...	n/a
Robility.HarmonyApi.dll	Unsigned		n/a	Robility.Harmony...	Robility.Harmony...	1.0.2	1.0.2	32-bit	1.0.2.0	Robility.Har...	Robility.Har...	Copyri...	n/a
Robility.Product.Update.dll	Unsigned		n/a	Robility.Product....	Robility.Product....	26.5.0.2	26.5.0.2	32-bit	26.5.0.2	Robility.Pro...	Robility.Pro...	Copyri...	n/a
Robility.Product.Update.dll	Unsigned		n/a	Robility.Product....	Robility.Product....	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.Pro...	Robility.Pro...	Copyri...	n/a
Robility.Product.Update.dll	Unsigned		n/a	Robility.Product....	Robility.Product....	26.5.0.2	26.5.0.2	32-bit	26.5.0.2	Robility.Pro...	Robility.Pro...	Copyri...	n/a
Robility.RemoveUnused.dll	Unsigned		n/a	Robility.Remove...	Robility.Remove...	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.Re...	Robility.Re...	Copyri...	n/a
Robility.ServiceCall.dll	Unsigned		n/a	Robility.Service...	Robility.ServiceCall	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.Ser...	Robility.Ser...	Copyri...	n/a
Robility.ServiceCall.dll	Unsigned		n/a	Robility.Service...	Robility.ServiceCall	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.Ser...	Robility.Ser...	Copyri...	n/a
Robility.ServiceCall.dll	Unsigned		n/a	Robility.Service...	Robility.ServiceCall	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.Ser...	Robility.Ser...	Copyri...	n/a
Robility.StyleTemplate.dll	Unsigned		n/a	Robility.StyleTe...	Robility.StyleTem...	1.1.0.0	1.1.0.0	32-bit	1.1.0.0	Robility.Styl...	Robility.Styl...	Copyri...	n/a
Robility.StyleTemplate.dll	Unsigned		n/a	Robility.StyleTe...	Robility.StyleTem...	1.1.0.0	1.1.0.0	32-bit	1.1.0.0	Robility.Styl...	Robility.Styl...	Copyri...	n/a
Robility.StyleTemplate.dll	Unsigned		n/a	Robility.StyleTe...	Robility.StyleTem...	1.1.0.0	1.1.0.0	32-bit	1.1.0.0	Robility.Styl...	Robility.Styl...	Copyri...	n/a
Robility.Utilities.dll	Unsigned		n/a	Robility.Utilities	Robility.Utilities	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.Utilit...	Robility.Utili...	Copyri...	n/a
Robility.WorkflowAnalyzer.dll	Unsigned		n/a	Robility.Workflo...	Robility.Workflow...	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	Robility.Wor...	Robility.Wo...	Copyri...	n/a
RobilityDesigner.exe	Unsigned		n/a	RobilityDesigner	Robility	26.5.0.2	26.5.0.2	32-bit	26.5.0.2	RobilityDesi...	RobilityDesi...	Copyri...	Workflo...
SixLabors.Fonts.dll	Unsigned		n/a	SixLabors.Fonts	SixLabors.Fonts	1.0.1+be8883...	1.0.1.0	32-bit	1.0.1.0	SixLabors.F...	SixLabors.F...	Copyri...	A cross-...
SmartRoboServiceLayer.dll	Unsigned		n/a	SmartRoboServi...	SmartRoboServic...	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	SmartRobo...	SmartRobo...	Copyri...	n/a
SmartRobotActivities.dll	Unsigned		n/a	SmartRobotActi...	SmartRobotActivi...	1.0.0.0	1.0.0.0	32-bit	1.0.0.0	SmartRobot...	SmartRobo...	Copyri...	n/a

FIGURE 11:MISSING CODE SIGNING

8. MISSING SECURITY FLAGS

Application / URL	RobilityRunner.exe RobilityDesigner.exe **Note: Implement appropriate security flags for all legitimate DLL files**
Revalidation Status	**CLOSED**
Severity	Low
CVSS Score	2.0
CVSS String	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
Description	It was observed that possible built-in support for OS-level mitigations against memory corruption is not configured. **Security Flags:** **CFG (Control Flow Guard)** - Generally programs are executed in predefined order flow. If CFG flag is not enabled then attacker can change the program execution flow and make his malicious code execute. **FORCE INTEGRITY** - The IMAGE_DLLCHARACTERISTICS_FORCE_INTEGRITY flag is set in the PE header at link time by using the /integrity check linker flag to indicate that the binary being loaded must be signed. This flag causes the Windows memory manager to enforce a signature check at load time on the binary file.
Impact	Control Flow Guard Mitigates many memory corruption attacks and reduces the success rate of ROP attacks. Whereas Force Integrity Prevents DLL planting and hijacking attacks. Increases the difficulty for attackers to inject malicious DLLs into the application's execution flow.
Remediation	It is recommended to configure application with above mentioned security flags for possible OS level mitigations.
Reference	https://docs.microsoft.com/en-us/windows/win32/secbp/control-flow-guard https://learn.microsoft.com/en-us/cpp/build/reference/integritycheck-require-signature-check

Proof of Concept:

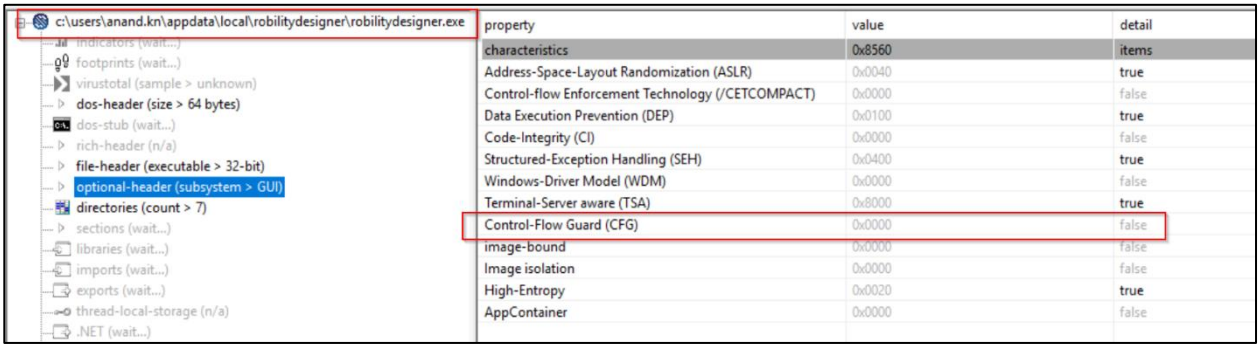


FIGURE 12:CFG DISABLED IN THE APPLICATION

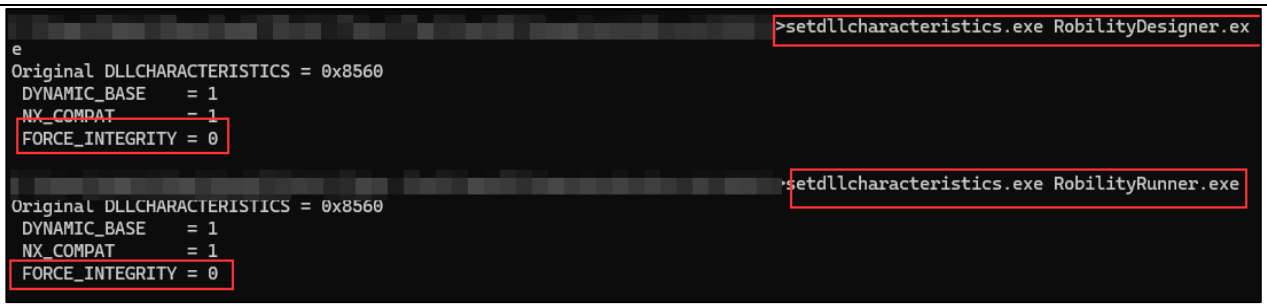


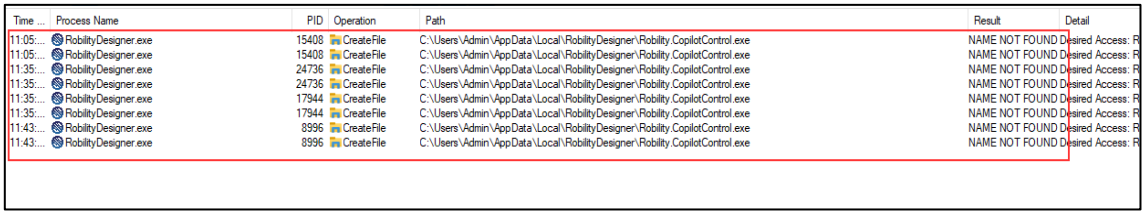
FIGURE 13:FORCE_INTEGRITY IS DISABLED

OBSERVATION:

- During dynamic analysis of the thick client application, it was observed that the application attempted to search for multiple executable (.exe) files in local directories that were not present on the system, resulting in NAME NOT FOUND events in process monitoring logs. This indicates that the application references external executable dependencies during runtime.

  Note

  Further testing confirmed that placing a crafted executable with the same filename in the searched location did not lead to execution. Therefore, no executable hijacking or code execution was observed, and this is recorded as an informational observation only.

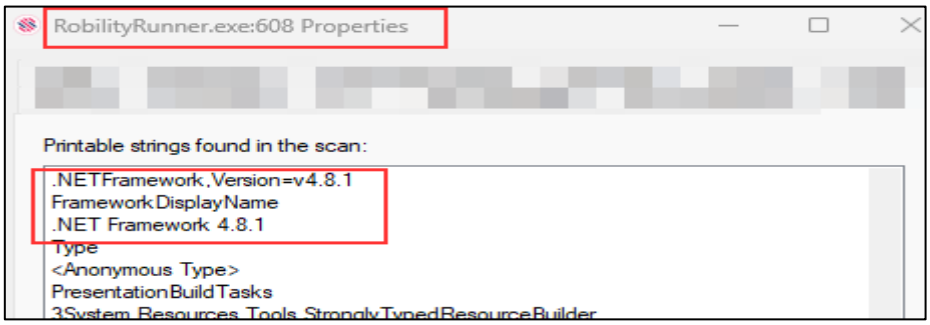


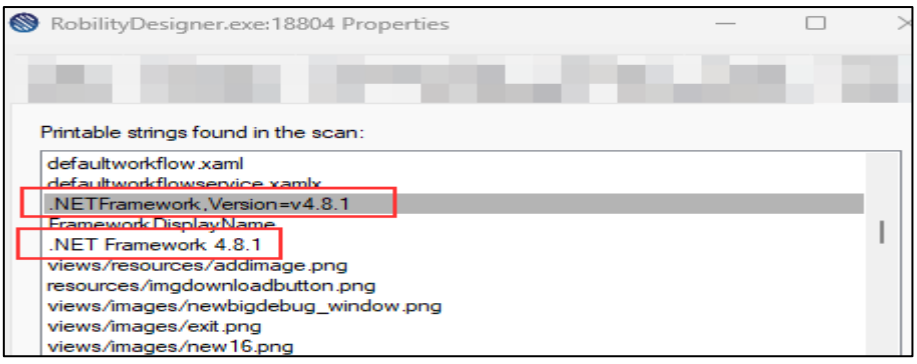
Time ...	Process Name	PID	Operation	Path	Result	Detail
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\Robility.CopilotControl.exe	NAME NOT FOUND	Desired Access: R
11:05:...	RobilityDesigner.exe	15408	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\Robility.CopilotControl.exe	NAME NOT FOUND	Desired Access: R
11:35:...	RobilityDesigner.exe	24736	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\Robility.CopilotControl.exe	NAME NOT FOUND	Desired Access: R
11:35:...	RobilityDesigner.exe	24736	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\Robility.CopilotControl.exe	NAME NOT FOUND	Desired Access: R
11:35:...	RobilityDesigner.exe	17944	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\Robility.CopilotControl.exe	NAME NOT FOUND	Desired Access: R
11:35:...	RobilityDesigner.exe	17944	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\Robility.CopilotControl.exe	NAME NOT FOUND	Desired Access: R
11:43:...	RobilityDesigner.exe	8996	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\Robility.CopilotControl.exe	NAME NOT FOUND	Desired Access: R
11:43:...	RobilityDesigner.exe	8996	CreateFile	C:\Users\Admin\AppData\Local\RobilityDesigner\Robility.CopilotControl.exe	NAME NOT FOUND	Desired Access: R

- During static analysis of the thick client application executable, it was observed that the binary contains readable strings disclosing the underlying framework version, specifically .NET Framework 4.8.1. This information was identified through string enumeration of the executable file.

  Note

  The exposed framework version information may assist an attacker in fingerprinting the application's technology stack. However, no direct exploitation was identified based on this information during the assessment, and it is recorded as an informational observation.





CONCLUSION:

Our security assessment revealed 08 vulnerabilities in the Robility.AI Application, issues are related to DLL Hijacking, Broken Authentication, No Rate Limit Attack, Missing Security Headers, Misconfigured CSP Security Header, Misconfigured CORS, Missing Code Signing and Missing Security Flags.

Annexure A – CHANGES TO ENVIRONMENT

N/A

Annexure B – TOOLS USED

Microsoft Sys-internal tools	Suite of powerful utilities for system management, troubleshooting, and analysis in Windows environments
SSLSCAN	The SSL Scanner uses a scanning engine based on the *testssl.sh* tool, together with multiple tweaks, adjustments, and improvements. The scanner works by connecting to the target SSL server and trying various ciphers and SSL/TLS protocol versions to determine existing vulnerabilities.
Metasploit	Metasploit is an open-source tool is used to probe systematic vulnerabilities on networks and servers.
WireShark	Wireshark is a network traffic analyzer, or "sniffer", for Unix and Unix-like operating systems.
Netspy	A tool to quickly detect the reachable network segments of the intranet
Kali Linux	Used to initiate advanced-level Security Auditing and Penetration Testing.
Customer Exploit Scripts	

CYBERPWN
EMPOWERING CYBER RESILIENCE

Annexure C – LIST OF VAPT TESTS PERFORMED

Test Cases	Status
Recon	Pass
Fingerprinting	Fail
Authentication and Authorization	Fail
Input Validation and Manipulation	Pass
Insecure Data Storage	Pass
Network Communication	Pass
Memory Corruption and Buffer Overflows	Pass
Code Execution and Arbitrary File Upload	Pass
Session Management	Pass
Cryptography	Pass
Client-Side Security	Pass
Unvalidated Redirects and Forwards	Pass
Error Handling and Information Disclosure	Pass
Application Logic	Pass
Third-Party Integration	Pass
Broken Access Control	Fail
Response Tampering	Pass
Weak Hashing Algorithm	Pass
Hardcoded Credentials	Pass
Lack of Code Obfuscation	Pass
DLL Hijacking	Fail
Missing Security Flags	Fail
Rate Limit Attack	Fail
Injection	Pass

THICK CLIENT APPLICATION

TESTING REPORT

A REPORT BY CYBERPWN
EMPOWERING CYBER RESILIENCE

2026

5SEC CYBERPWN TECHNOLOGIES PVT LTD