Proposed Vulnerabilities	SNYK		Trivy		OWASP DC	
	CVE Numbers	Description	CVE Numbers	Description	CVE Numbers	Description
V1: Exposed API Endpoints without Authentication.	CVE-2022-37603	information disclosure identified in 2022				
V2: Accidental Exposure of Sensitive API Endpoints.						
V3: Unknown/ Untrusted APIs.						
V4: Weak authentication mechanisms for APIs.	CVE-2023-44270	cross-site scripting (XSS) identified in 2023	CVE-2022-37601	buffer overflow identified in 2022		
	CVE-2023-0215	improper access control identified in 2023				
V5: Insecure data serialization.						
V6: Misconfiguration of API gateways.	CVE-2023-27537	improper access control identified in 2023				
V7: Service Registration Poisoning.	CVE-2023-28320	improper access control identified in 2023				
V8: Unauthorized Access to Service Discovery.	CVE-2022-4304	improper access control identified in 2022				
V9: Unavailability of Service Registration Validation.						
V10: Unauthorized Service Deregistration.	CVE-2023-0465	unauthorized access identified in 2023				
V11: Reuse of Previous Service Requests.						
V12: Legitimate Service Spoofing.						
V13: Insufficient Network Segmentation.						
V14: Improper Service Mesh Implementation.						
V15: Misconfigured Network Access Controls.						
V16: Incorrect Firewall Configuration.						
V17: No Internet Traffic Encryption.						
V18: Using Default Network Configurations.						
V19: Using Weak or Deprecated Algorithms.						
V20: Lack of End-to-End Encryption.						
V21: Sensitive Data Exposure via Metadata.						
V22: Improper Encryption Key Management.						
V23: Improper Validation of Certificates.						
V24: Hardcoded Encryption Keys.						
V25: No Proper Rate Limiting.	CVE-2023-0464	denial of service identified in 2023				
	CVE-2022-40674	denial of service identified in 2022				
V26: Improper Handling of Suspicious.	CVE-2023-38039	denial of service identified in 2023				
	CVE-2021-42380	denial of service identified in 2021				
V27: Lack of Individualized Rate Limiting.	CVE-2023-2650	denial of service identified in 2023				
	CVE-2023-26136	information disclosure identified in 2023				
V28: Improper Configuration of Rate Limits.	CVE-2023-45133	information disclosure identified in 2023	CVE-2022-3517	denial of service identified in 2022	CVE-2023-28154	denial of service identified in 2023
	CVE-2023-27534	denial of service identified in 2023	CVE-2023-28154	denial of service identified in 2023		
	CVE-2022-27782	denial of service identified in 2022	CVE-2023-28155	privilege escalation identified in 2023		
V29: Targeted API Abuse.	CVE-2021-42375	denial of service identified in 2021				
	CVE-2023-1999	denial of service identified in 2023				
	CVE-2021-42384	denial of service identified in 2021				
V30: Weak or Non-existent Database Encryption.	CVE-2022-35252	remote code execution identified in 2022	CVE-2023-44270	cross-site scripting (XSS) identified in 2023		
	CVE-2022-43552	information disclosure identified in 2022				
	CVE-2023-35945	data leak vulnerability identified in 2023				
V31: Inadequate Database Hardening.	CVE-2023-23915	data leak vulnerability identified in 2023	CVE-2022-38900	cross-site scripting (XSS) identified in 2022		
	CVE-2023-3817	information disclosure identified in 2023				
	CVE-2022-41409	information disclosure identified in 2022				
V32: Using Default Database Credentials.	CVE-2021-36159	information disclosure identified in 2021	CVE-2022-37603	information disclosure identified in 2022	CVE-2022-25858	data leak vulnerability identified in 2022
	CVE-2023-27536	information disclosure identified in 2023	CVE-2023-30798	information disclosure identified in 2023		
	CVE-2022-42915	information disclosure identified in 2022				
	CVE-2022-2309	data leak vulnerability identified in 2022				
	CVE-2022-43680	data leak vulnerability identified in 2022				
V33: Exposure of Sensitive Data via Error Messages.						
V34: Non-existent Data Integrity Checks.	CVE-2023-3446	information disclosure identified in 2023				

V35: SQL Injection.	CVE-2021-46848	remote code execution identified in 2021	CVE-2022-25858	data leak vulnerability identified in 2022		
	CVE-2022-37599	buffer overflow identified in 2022				
	CVE-2023-29491	remote code execution identified in 2023				
	CVE-2022-27406	remote code execution identified in 2022				
	CVE-2022-27405	remote code execution identified in 2022				
V36: Cross-Site Scripting (XSS).	CVE-2021-42383	cross-site scripting (XSS) identified in 2021				
V37: Command Injection.	CVE-2023-27538	buffer overflow identified in 2023			CVE-2022-46175	buffer overflow identified in 2022
	CVE-2021-33587	buffer overflow identified in 2021			CVE-2022-37601	buffer overflow identified in 2022
	CVE-2021-42385	buffer overflow identified in 2021			CVE-2022-37599	buffer overflow identified in 2022
	CVE-2021-3803	privilege escalation identified in 2021				
V38: Insecure Deserialization of Data.						
V39: User Inputs Directly Accessing Objects.	CVE-2022-3517	denial of service identified in 2022			CVE-2023-26115	buffer overflow identified in 2023
V40: Granting Higher than Required Level of Access.	CVE-2022-2097	unauthorized access identified in 2022				
V41: Credential Hardcoding in Source Code.	CVE-2022-27780	data leak vulnerability identified in 2022				
	CVE-2022-4450	data leak vulnerability identified in 2022				
V42: Granted Privilege Exploitation.						
V43: Race Condition Exploitation.	CVE-2022-40303	information disclosure identified in 2022				
V44: Improper Data Transaction Management.	CVE-2022-25858	data leak vulnerability identified in 2022	CVE-2023-45133	information disclosure identified in 2023		
	CVE-2021-42378	data leak vulnerability identified in 2021				
V45: Insecure Data Synchronization.					CVE-2022-37603	information disclosure identified in 2022
V46: Concurrent Data Access Mismanagement.					CVE-2023-26136	information disclosure identified in 2023
V47: Lack of Regular Backups.						
V48: Insecure Backup Storage.						
V49: Lack of Backup Validation.	CVE-2021-3711	information disclosure identified in 2021			CVE-2022-33987	data leak vulnerability identified in 2022
V50: Improper Disposal of Outdated Backups.						
V51: Insecure/Weak Authentication.						
V52: Enumeration of Accounts.						
V53: Continued Usage of Breached Credentials.						
V54: Identity Federation Misconfiguration.						
V55: Provision of Higher Privileges.						
V56: Improper Token Invalidation.	CVE-2023-26115	buffer overflow identified in 2023				
V57: Insecure Access Token Storage.						
V58: Embedded Static Credentials.						
V59: Reuse of Passwords.						
V60: Vulnerable Password Recovery Process.						
V61: MFA not Used/Enforced.						
V62: Phishing Attacks on Users.	CVE-2022-37434	privilege escalation identified in 2022				
V63: Unenforced Access Controls.			CVE-2022-46175	buffer overflow identified in 2022		
V64: Human Error in Granting Access.						
V65: Insecure Direct Object Reference.	CVE-2023-27535	remote code execution identified in 2023	CVE-2023-29159	remote code execution identified in 2023		
	CVE-2023-28321	remote code execution identified in 2023				
	CVE-2022-46175	buffer overflow identified in 2022				
	CVE-2023-38545	remote code execution identified in 2023				
	CVE-2023-0286	remote code execution identified in 2023				
	CVE-2023-29159	remote code execution identified in 2023				
V66: Vulnerable APIs Having Higher Control.	CVE-2023-38546	unauthorized access identified in 2023				
	CVE-2022-28391	unauthorized access identified in 2022				
V67: Session Hijacking.						
V68: Cross-Site Request Forgery.	CVE-2022-32206	unauthorized access identified in 2022				
V69: Session Control Exploitation.	CVE-2022-37601	buffer overflow identified in 2022				
V70: Improper Session Expiry.						
V71: Container Misconfigurations.	CVE-2022-32207	privilege escalation identified in 2022				

V72: Improper Container Isolation.	CVE-2022-32208	privilege escalation identified in 2022				
	CVE-2023-28154	denial of service identified in 2023				
V73: Direct Storage of Sensitive Data on Container Image.						
V74: Outdated/Insecure Container Image Usage.			CVE-2022-37599	buffer overflow identified in 2022		
V75: Misconfiguration of Orchestration Dashboards.	CVE-2022-37434	privilege escalation identified in 2022				
V76: Orchestration Tools Having Unrestricted API Access.						
V77: Poor Definition of RBAC.						
V78: Vulnerabilities in Orchestration Tools.	CVE-2022-32205	privilege escalation identified in 2022				
	CVE-2022-25883	injection vulnerability identified in 2022				
V79: Insecure Service Configuration.						
V80: Service Deployments with no Configuration Validation.						
V81: Embedded Passwords/Tokens in Configuration Files.						
V82: Insecure Configuration File Validation.	CVE-2023-23914	remote code execution identified in 2023				
V83: Adding Components with Known Vulnerabilities.						
V84: Outdated/Unmaintained Dependency Usage.	CVE-2023-30798	information disclosure identified in 2023				
V85: Insufficient Scanning of Dependencies.						
V86: No Transitive Dependency Validation.						
V87: Inconsistent Security Practices.						
V88: Issues Within Specific Libraries.						
V89: Misconfiguration of Different Platforms.						
V90: Patch Management Complexity.						
V91: Legacy System Integration Vulnerabilities.						
V92: Mismatched Data Formats in Different Technologies.						
V93: Service Mesh Configuration Errors.						
V94: Inconsistent Security at Integration Points.						
V95: Compromised Supply Chain Attacks.						
V96: Third-Party Components Service Outages.						
V97: Insecure Third-Party Components.						
V98: No Proper Security Practices in Third-Party Components.						
V99: Various Injection Vulnerabilities.	CVE-2023-23916	injection vulnerability identified in 2023	CVE-2023-26136	information disclosure identified in 2023	CVE-2022-25883	injection vulnerability identified in 2022
	CVE-2021-42374	injection vulnerability identified in 2021				
	CVE-2022-0778	injection vulnerability identified in 2022				
	CVE-2018-25032	injection vulnerability identified in 2018				
	CVE-2021-3712	injection vulnerability identified in 2021				
	CVE-2021-42386	injection vulnerability identified in 2021				
	CVE-2021-42382	injection vulnerability identified in 2021				
	CVE-2022-38900	cross-site scripting (XSS) identified in 2022				
V100: Improper XSS Prevention Implementation.	CVE-2022-32221	cross-site scripting (XSS) identified in 2022	CVE-2021-3803	privilege escalation identified in 2021	CVE-2023-44270	cross-site scripting (XSS) identified in 2023
	CVE-2022-1587	cross-site scripting (XSS) identified in 2022	CVE-2022-25883	injection vulnerability identified in 2022	CVE-2022-38900	cross-site scripting (XSS) identified in 2022
	CVE-2023-44487	cross-site scripting (XSS) identified in 2023	CVE-2023-26115	buffer overflow identified in 2023		
	CVE-2022-40304	cross-site scripting (XSS) identified in 2022				
	CVE-2022-43551	cross-site scripting (XSS) identified in 2022				
	CVE-2023-28319	cross-site scripting (XSS) identified in 2023				
	CVE-2022-29458	cross-site scripting (XSS) identified in 2022				
	CVE-2021-42381	cross-site scripting (XSS) identified in 2021				
	CVE-2021-42379	cross-site scripting (XSS) identified in 2021				
	CVE-2022-42898	cross-site scripting (XSS) identified in 2022				
	CVE-2022-1304	cross-site scripting (XSS) identified in 2022				
	CVE-2021-46828	cross-site scripting (XSS) identified in 2021				
V101: Insecure Deserialization in components.						
V102: Flaws in Specific Frameworks.						
V103: Cloud Environment Misconfiguration.	CVE-2023-27533	privilege escalation identified in 2023			CVE-2021-3803	privilege escalation identified in 2021

	CVE-2022-27781	privilege escalation identified in 2022				
V104: Infrastructure Tools Misconfiguration.	CVE-2023-4863	privilege escalation identified in 2023				
V105: Mismanagement of VMs.	CVE-2022-42916	privilege escalation identified in 2022				
V106: Insufficient Network Security.						
V107: Lack of Integration Tool Security.						
V108: CI/CD Misconfigurations.	CVE-2023-28155	privilege escalation identified in 2023				
V109: Pipeline not having Security Controls.						
V110: Vulnerable Code Deployment.						
V111: Insecure IaC Scripts.	CVE-2022-1586	privilege escalation identified in 2022				
V112: Automated Deployment of Misconfigured Infrastructure.	CVE-2023-28322	privilege escalation identified in 2023				
V113: Secrets Hardcoded Within IaC Scripts.						
V114: No Version Control for IaC.						
V115: Insufficient Storage and Rotation of Secrets.						
V116: No Centralized Secrets Management System.						
V117: Committing Secrets in Version Control.						
V118: Failure to Monitor Secrets Access Logs.						
V119: Not Having Enough Automated Testing.						
V120: Poor/no Manual Reviews of Security.						
V121: Not Acting on Test Results.						
V122: Outdated Testing Tools Used.						
V123: No Proper Training Provided for Teams.					CVE-2022-25881	data leak vulnerability identified in 2022
V124: Not Considering Security in Early Phases of Development.						
V125: Inconsistent Security Practices Application.						
V126: Low/Poor Collaboration Levels of Security and DevOps.					CVE-2023-28155	privilege escalation identified in 2023