TABLE VI: Taxonomy of Vulnerabilities.

	Category	Subcategory	Proposed Vulnerability
Vulnerabilities in Microservices	Communication and Networking	API Gateways and Endpoints	V_1: Exposed API Endpoints without Authentication [23], [24], [25] V_2: Accidental Exposure of Sensitive API Endpoints [23], [26], [5] V_3: Unknown/ Untrusted APIs [23], [26], [5] V_4: Weak authentication mechanisms for APIs [27], [5], [28] V_5: Insecure data serialization [29], [30], [31] V_6: Misconfiguration of API gateways [32], [24]
		Service Discovery	V_7: Service Registration Poisoning [33], [34], [35] V_8: Unauthorized Access to Service Discovery [31], [33], [34] V_9: Unavailability of Service Registration Validation [34] V_{10}: Unauthorized Service Deregistration [36], [35], [29] V_{11}: Reuse of Previous Service Requests [37], [38], [25] V_{12}: Legitimate Service Spoofing [39], [31], [40], [41], [42]
		Network Segmentation and Isolation	V_{13}: Insufficient Network Segmentation [43], [44] V_{14}: Improper Service Mesh Implementation [45], [46] V_{15}: Misconfigured Network Access Controls [40], [44] V_{16}: Incorrect Firewall Configuration [40], [44] V_{17}: No Internet Traffic Encryption [47], [46] V_{18}: Using Default Network Configurations [48], [46]
		Encryption and Secure Communication	V_{19}: Using Weak or Deprecated Algorithms [5], [49] V_{20}: Lack of End-to-End Encryption [50], [51] V_{21}: Sensitive Data Exposure via Metadata [3], [49] V_{22}: Improper Encryption Key Management [52], [51] V_{23}: Improper Validation of Certificates [53], [49] V_{24}: Hardcoded Encryption Keys [30], [49]
		Rate Limiting and Throttling	V_{25}: No Proper Rate Limiting [31], [42], [54] V_{26}: Improper Handling of Suspicious IPs [55], [54] V_{27}: Lack of Individualized Rate Limiting [54], [42] V_{28}: Improper Configuration of Rate Limits [54] V_{29}: Targeted API Abuse [25], [42]
	Data Security and Management	Data Storage and Encryption	V_{30}: Weak or Non-existent Database Encryption [56], [23] V_{31}: Inadequate Database Hardening [57], [58] V_{32}: Using Default Database Credentials [59], [23] V_{33}: Exposure of Sensitive Data via Error Messages [60], [58] V_{34}: Non-existent Data Integrity Checks [60], [23]
		Data Validation and Sanitization	V_{35}: SQL Injection [61], [58] V_{36}: Cross-Site Scripting (XSS) [61], [58] V_{37}: Command Injection [61], [62] V_{38}: Insecure Deserialization of Data [30], [58]
		Data Access Control	V_{39}: User Inputs Directly Accessing Objects [63], [64] V_{40}: Granting Higher than Required Level of Access [65] V_{41}: Credential Hardcoding in Source Code [33], [64] V_{42}: Granted Privilege Exploitation [66]
		Data Consistency and Integrity	V_{43}: Race Condition Exploitation [31], [46] V_{44}: Improper Data Transaction Management [63], [46] V_{45}: Insecure Data Synchronization [67] V_{46}: Concurrent Data Access Mismanagement [38], [46]
		Backup and recovery	V_{47}: Lack of Regular Backups [66], [58] V_{48}: Insecure Backup Storage [66], [58] V_{49}: Lack of Backup Validation [43], [58] V_{50}: Improper Disposal of Outdated Backups [68], [58]
	Identity Access Control	Identity and Access Management	V_{51}: Insecure/Weak Authentication [69] V_{52}: Enumeration of Accounts [3], [70] V_{53}: Continued Usage of Breached Credentials [70] V_{54}: Identity Federation Misconfiguration [70]
		Permission and Privilege Management	V_{55}: Provision of Higher Privileges [42], [58] V_{56}: Improper Token Invalidation [42] V_{57}: Insecure Access Token Storage [42], [58] V_{58}: Embedded Static Credentials [42]
		Identity/ Access Authentication	V_{59}: Reuse of Passwords [64] V_{60}: Vulnerable Password Recovery Process [64] V_{61}: MFA not Used/Enforced [64] V_{62}: Phishing Attacks on Users [5], [64]
		Authorization and Policy Enforcement	V_{63}: Unenforced Access Controls [64] V_{64}: Human Error in Granting Access [71], [5] V_{65}: Insecure Direct Object Reference [72] V_{66}: Vulnerable APIs Having Higher Control [64]
		Session Management	V_{67}: Session Hijacking [42], [69] V_{68}: Cross-Site Request Forgery [42], [62] V_{69}: Session Control Exploitation [42], [69] V_{70}: Improper Session Expiry [42], [69]
	Deployment and Orchestration	Containerization Security	V_{71}: Container Misconfigurations [30], [23] V_{72}: Improper Container Isolation [67], [23] V_{73}: Direct Storage of Sensitive Data on Container Image [53], [23] V_{74}: Outdated/Insecure Container Image Usage [73], [23]
		Orchestration Tools and Platforms	V_{75}: Misconfiguration of Orchestration Dashboards [74], [44] V_{76}: Orchestration Tools Having Unrestricted API Access [44], [61] V_{77}: Poor Definition of RBAC [75], [44] V_{78}: Vulnerabilities in Orchestration Tools [76], [44]
		Configuration Management	V_{79}: Insecure Service Configuration [74], [49] V_{80}: Service Deployments with no Configuration Validation [74], [49] V_{81}: Embedded Passwords/Tokens in Configuration Files [74], [49] V_{82}: Insecure Configuration File Validation [74], [49]
		Dependency Management	V_{83}: Adding Components with Known Vulnerabilities [49] V_{84}: Outdated/Unmaintained Dependency Usage [28], [49] V_{85}: Insufficient Scanning of Dependencies [55], [49] V_{86}: No Transitive Dependency Validation [49]
	Heterogeneity	Technology Stack Diversification	V_{87}: Inconsistent Security Practices [51] V_{88}: Issues Within Specific Libraries [51], [48] V_{89}: Misconfiguration of Different Platforms [51], [48] V_{90}: Patch Management Complexity [51]
		Interoperability and Compatibility	V_{91}: Legacy System Integration Vulnerabilities [36], [51] V_{92}: Mismatched Data Formats in Different Technologies [51] V_{93}: Service Mesh Configuration Errors [41], [51] V_{94}: Inconsistent Security at Integration Points [68], [51]
		Third-Party Services and Integrations	V_{95}: Compromised Supply Chain Attacks [31], [26] V_{96}: Third-Party Components Service Outages [64], [26] V_{97}: Insecure Third-Party Components [56], [26] V_{98}: No Proper Security Practices in Third-Party Components [51], [26]
		Specific Language and Framework Usage	V_{99}: Various Injection Vulnerabilities [3], [51] V_{100}: Improper XSS Prevention Implementation [5], [3], [51] V_{101}: Insecure Deserialization in components [3], [51] V_{102}: Flaws in Specific Frameworks [3], [51]
		Platform/ Infrastructure Diversification	V_{103}: Cloud Environment Misconfiguration [37], [77] V_{104}: Infrastructure Tools Misconfiguration [78], [77] V_{105}: Mismanagement of VMs [46], [77] V_{106}: Insufficient Network Security [5], [77]
	DevOps and CI/CD	CI/CD and automation	V_{107}: Lack of Integration Tool Security [68], [44] V_{108}: CI/CD Misconfigurations [79] V_{109}: Pipeline not having Security Controls [44], [80] V_{110}: Vulnerable Code Deployment [67], [44]
		Infrastructure as Code	V_{111}: Insecure IaC Scripts [81], [44] V_{112}: Automated Deployment of Misconfigured Infrastructure [24], [28] V_{113}: Secrets Hardcoded Within IaC Scripts [44] V_{114}: No Version Control for IaC [44]
		Secrets Management	V_{115}: Insufficient Storage and Rotation of Secrets [82], [36] V_{116}: No Centralized Secrets Management System [82], [36] V_{117}: Committing Secrets in Version Control [58], [78] V_{118}: Failure to Monitor Secrets Access Logs [82], [36]
		Testing and Analysis of the Pipeline	V_{119}: Not Having Enough Automated Testing [5], [58] V_{120}: Poor/no Manual Reviews of Security [3], [81], [58] V_{121}: Not Acting on Test Results [3], [58] V_{122}: Outdated Testing Tools Used [5], [58]
		DevSecOps Practices	V_{123}: No Proper Training Provided for Teams [44], [56] V_{124}: Not Considering Security in Early Phases of Development [44], [56] V_{125}: Inconsistent Security Practices Application [44], [56] V_{126}: Low/Poor Collaboration Levels of Security and DevOps [44], [56]