TABLE IX: Mapping Proposed Vulnerabilities to Actual Vulnerabilities

Proposed Vulnerabilities	Book Mgt System			Cloud Native Eshop			Spring Boot			Knowledge Base			Tools			Identified Vlun.
	SNYK	Trivy	OWASP	SNYK	Trivy	OWASP	SNYK	Trivy	OWASP	SNYK	Trivy	OWASP	SNYK	Trivy	OWASP	
V_1: Exposed API Endpoints without Authentication.	4	0	0	1	0	0	2	0	0	0	0	1	7	0	1	8
V_2: Accidental Exposure of Sensitive API Endpoints.	6	0	0	0	0	0	1	0	0	0	0	0	7	0	0	7
V_3: Unknown/ Untrusted APIs.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_4: Weak authentication mechanisms for APIs.	5	0	0	2	1	0	2	0	0	0	0	1	9	1	1	11
V_5: Insecure data serialization.	0	0	0	0	0	0	0	0	1	0	0	1	0	0	2	2
V_6: Misconfiguration of API gateways.	4	0	0	1	0	0	0	0	0	0	0	1	5	0	1	6
V_7: Service Registration Poisoning.	3	0	0	1	0	0	2	1	0	0	0	0	6	1	0	7
V_8: Unauthorized Access to Service Discovery.	2	0	0	1	0	0	2	1	0	0	0	0	5	1	0	6
V_9: Unavailability of Service Registration Validation.	0	0	0	0	0	0	0	0	2	3	0	0	3	0	2	5
V_{10}: Unauthorized Service Deregistration.	2	0	0	1	0	0	3	1	0	0	0	0	6	1	0	7
V_{11}: Reuse of Previous Service Requests.	3	0	0	0	0	0	0	0	0	0	0	0	3	0	0	3
V_{12}: Legitimate Service Spoofing.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{13}: Insufficient Network Segmentation.	0	0	0	0	0	0	1	0	1	0	0	0	1	0	1	2
V_{14}: Improper Service Mesh Implementation.	0	0	0	0	0	0	1	0	2	0	0	0	1	0	2	3
V_{15}: Misconfigured Network Access Controls.	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
V_{16}: Incorrect Firewall Configuration.	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2	2
V_{17}: No Internet Traffic Encryption.	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2	2
V_{18}: Using Default Network Configurations.	4	0	0	0	0	0	0	0	0	0	0	0	4	0	0	4
V_{19}: Using Weak or Deprecated Algorithms.	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2	2
V_{20}: Lack of End-to-End Encryption.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{21}: Sensitive Data Exposure via Metadata.	6	0	0	0	0	0	0	0	0	0	0	0	6	0	0	6
V_{22}: Improper Encryption Key Management.	5	0	0	0	0	0	0	0	0	0	0	0	5	0	0	5
V_{23}: Improper Validation of Certificates.	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
V_{24}: Hardcoded Encryption Keys.	8	0	0	0	0	0	0	0	0	0	0	0	8	0	0	8
V_{25}: No Proper Rate Limiting.	11	1	1	2	0	0	3	0	2	3	0	0	19	1	3	23
V_{26}: Improper Handling of Suspicious.	3	0	0	2	0	0	1	2	2	6	0	0	12	2	2	16
V_{27}: Lack of Individualized Rate Limiting.	7	2	0	2	0	0	1	4	4	9	0	1	19	6	5	30
V_{28}: Improper Configuration of Rate Limits.	5	1	0	3	3	1	1	0	2	12	0	1	21	4	4	29
V_{29}: Targeted API Abuse.	4	0	0	3	0	0	1	0	4	6	0	1	14	0	5	19
V_{30}: Weak or Non-existent Database Encryption.	9	5	0	3	1	0	3	2	1	9	1	0	24	9	1	34
V_{31}: Inadequate Database Hardening.	10	3	1	3	1	0	10	2	1	9	2	0	32	8	2	42
V_{32}: Using Default Database Credentials.	15	6	3	5	2	1	17	7	6	18	1	2	55	16	12	83
V_{33}: Exposure of Sensitive Data via Error Messages.	6	0	0	0	0	0	4	0	0	2	0	0	12	0	0	12
V_{34}: Non-existent Data Integrity Checks.	2	2	1	1	0	0	5	0	1	10	0	1	18	2	3	23
V_{35}: SQL Injection.	5	0	0	5	1	0	0	1	0	16	0	1	26	2	1	29
V_{36}: Cross-Site Scripting (XSS).	57	5	2	0	0	0	21	15	6	1	0	2	79	20	10	109
V_{37}: Command Injection.	33	2	2	5	0	3	14	8	10	19	3	1	71	13	16	100
V_{38}: Insecure Deserialization of Data.	3	0	0	0	0	0	0	1	0	0	0	0	3	1	0	4
V_{39}: User Inputs Directly Accessing Objects.	16	2	1	1	0	1	1	0	3	7	1	3	25	3	8	36
V_{40}: Granting Higher than Required Level of Access.	13	1	1	1	0	0	4	2	0	0	0	0	18	3	1	22
V_{41}: Credential Hardcoding in Source Code.	1	0	0	2	0	0	0	0	0	0	0	0	3	0	0	3
V_{42}: Granted Privilege Exploitation.	11	1	0	0	0	0	1	2	0	0	0	0	12	3	0	15
V_{43}: Race Condition Exploitation.	1	0	0	1	0	0	0	0	0	0	0	1	2	0	1	3
V_{44}: Improper Data Transaction Management.	1	0	0	2	1	0	1	0	0	0	0	2	4	1	2	7
V_{45}: Insecure Data Synchronization.	0	0	0	0	0	1	4	1	0	6	0	2	10	1	3	14
V_{46}: Concurrent Data Access Mismanagement.	3	0	0	0	0	1	0	1	1	4	1	0	7	2	2	11
V_{47}: Lack of Regular Backups.	5	0	0	0	0	0	4	3	0	4	0	0	13	3	0	16
V_{48}: Insecure Backup Storage.	2	0	0	0	0	0	1	0	0	7	1	0	10	1	0	11
V_{49}: Lack of Backup Validation.	1	0	0	1	0	1	3	2	0	4	1	0	9	3	1	13
V_{50}: Improper Disposal of Outdated Backups.	1	0	0	0	0	0	0	1	1	1	0	0	2	1	1	4
V_{51}: Insecure/Weak Authentication.	9	0	0	0	0	0	2	1	1	3	0	0	14	1	1	16
V_{52}: Enumeration of Accounts.	1	0	0	0	0	0	1	0	0	4	0	0	6	0	0	6
V_{53}: Continued Usage of Breached Credentials.	1	0	0	0	0	0	2	0	0	3	0	0	6	0	0	6
V_{54}: Identity Federation Misconfiguration.	6	0	0	0	0	0	1	0	0	11	0	0	18	0	0	18
V_{55}: Provision of Higher Privileges.	30	2	1	0	0	0	10	7	0	0	0	0	40	9	1	50
V_{56}: Improper Token Invalidation.	0	0	0	1	0	0	0	1	0	10	1	0	11	2	0	13
V_{57}: Insecure Access Token Storage.	10	0	0	0	0	0	2	1	0	1	0	0	13	1	0	14
V_{58}: Embedded Static Credentials.	7	0	0	0	0	0	2	1	1	1	0	0	10	1	1	12
V_{59}: Reuse of Passwords.	6	1	1	0	0	0	3	3	0	1	1	0	10	5	1	16
V_{60}: Vulnerable Password Recovery Process.	1	0	0	0	0	0	1	1	0	3	0	0	5	1	0	6
V_{61}: MFA not Used/Enforced.	3	0	0	0	0	0	2	1	0	6	0	0	11	1	0	12
V_{62}: Phishing Attacks on Users.	1	0	0	1	0	0	1	1	1	5	0	1	8	1	2	11
V_{63}: Unenforced Access Controls.	8	0	0	0	1	0	3	0	0	5	0	0	16	1	0	17
V_{64}: Human Error in Granting Access.	3	0	0	0	0	0	1	1	1	5	0	0	9	1	1	11
V_{65}: Insecure Direct Object Reference.	28	1	1	6	1	0	9	6	5	10	1	0	53	9	6	68
V_{66}: Vulnerable APIs Having Higher Control.	3	1	1	2	0	0	4	1	0	5	0	1	14	2	2	18
V_{67}: Session Hijacking.	3	2	0	0	0	0	4	0	1	13	0	1	20	2	2	24
V_{68}: Cross-Site Request Forgery.	7	2	0	1	0	0	2	3	0	7	0	1	17	5	1	23
V_{69}: Session Control Exploitation.	4	2	0	1	0	0	4	4	1	4	1	0	13	7	1	21
V_{70}: Improper Session Expiry.	6	1	1	0	0	0	2	3	1	7	0	0	15	4	2	21
V_{71}: Container Misconfigurations.	0	0	0	1	0	0	0	0	1	6	0	0	7	0	1	8
V_{72}: Improper Container Isolation.	0	0	0	2	0	0	0	0	1	6	0	0	8	0	1	9
V_{73}: Direct Storage of Sensitive Data on Container Image.	4	0	0	0	0	0	1	0	1	9	0	0	14	0	1	15
V_{74}: Outdated/Insecure Container Image Usage.	0	0	0	0	1	0	0	0	3	3	1	0	3	2	3	8
V_{75}: Misconfiguration of Orchestration Dashboards.	0	0	0	1	0	0	0	0	1	4	0	2	5	0	3	8
V_{76}: Orchestration Tools Having Unrestricted API Access.	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
V_{77}: Poor Definition of RBAC.	11	0	0	0	0	0	4	1	0	0	0	0	15	1	0	16
V_{78}: Vulnerabilities in Orchestration Tools.	4	0	0	2	0	0	1	0	1	7	0	0	14	0	1	15
V_{79}: Insecure Service Configuration.	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
V_{80}: Service Deployments with no Configuration Validation.	3	0	0	0	0	0	0	0	0	0	0	0	3	0	0	3
V_{81}: Embedded Passwords/Tokens in Configuration Files.	7	1	0	0	0	0	1	1	0	0	0	0	8	2	0	10
V_{82}: Insecure Configuration File Validation.	9	0	0	1	0	0	1	4	2	6	1	0	17	5	2	24
V_{83}: Adding Components with Known Vulnerabilities.	3	0	0	0	0	0	2	3	0	4	0	1	9	3	1	13
V_{84}: Outdated/Unmaintained Dependency Usage.	2	0	0	1	0	0	0	1	2	3	1	0	6	2	2	10
V_{85}: Insufficient Scanning of Dependencies.	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
V_{86}: No Transitive Dependency Validation.	7	0	0	0	0	0	3	4	0	0	0	0	10	4	0	14
V_{87}: Inconsistent Security Practices.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{88}: Issues Within Specific Libraries.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{89}: Misconfiguration of Different Platforms.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{90}: Patch Management Complexity.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{91}: Legacy System Integration Vulnerabilities.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{92}: Mismatched Data Formats in Different Technologies.	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1
V_{93}: Service Mesh Configuration Errors.	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1
V_{94}: Inconsistent Security at Integration Points.	4	1	1	0	0	0	4	2	0	0	0	0	8	3	1	12
V_{95}: Compromised Supply Chain Attacks.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{96}: Third-Party Components Service Outages.	6	0	0	0	0	0	3	2	0	0	0	0	9	2	0	11
V_{97}: Insecure Third-Party Components.	6	0	0	0	0	0	0	3	0	0	0	0	6	3	0	9
V_{98}: No Proper Security Practices in Third-Party Components.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{99}: Various Injection Vulnerabilities.	48	4	6	8	1	1	16	12	15	32	2	3	104	19	25	148
V_{100}: Improper XSS Prevention Implementation.	0	0	0	12	3	2	0	0	14	36	1	0	48	4	16	68
V_{101}: Insecure Deserialization in components.	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1
V_{102}: Flaws in Specific Frameworks.	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2	2
V_{103}: Cloud Environment Misconfiguration.	0	0	0	2	0	1	0	0	1	1	0	0	3	0	2	5
V_{104}: Infrastructure Tools Misconfiguration.	0	0	0	1	0	0	0	0	1	0	0	0	1	0	1	2
V_{105}: Mismanagement of VMs.	0	0	0	1	0	0	0	0	1	2	0	0	3	0	1	4
V_{106}: Insufficient Network Security.	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2	2
V_{107}: Lack of Integration Tool Security.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{108}: CI/CD Misconfigurations.	0	0	0	1	0	0	0	0	1	1	0	0	2	0	1	3
V_{109}: Pipeline not having Security Controls.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1.0
V_{110}: Vulnerable Code Deployment.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{111}: Insecure IaC Scripts.	1	0	0	1	0	0	0	0	1	2	0	0	4	0	1	5
V_{112}: Automated Deployment of Misconfigured Infrastructure.	0	0	0	1	0	0	0	0	2	3	0	1	4	0	3	7
V_{113}: Secrets Hardcoded Within IaC Scripts.	6	0	0	0	0	0	1	0	0	0	0	0	7	0	0	7
V_{114}: No Version Control for IaC.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{115}: Insufficient Storage and Rotation of Secrets.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{116}: No Centralized Secrets Management System.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{117}: Committing Secrets in Version Control.	5	0	0	0	0	0	1	0	0	0	0	0	6	0	0	6
V_{118}: Failure to Monitor Secrets Access Logs.	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2	2
V_{119}: Not Having Enough Automated Testing.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{120}: Poor/no Manual Reviews of Security.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{121}: Not Acting on Test Results.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{122}: Outdated Testing Tools Used.	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1
V_{123}: No Proper Training Provided for Teams.	0	0	0	0	0	1	0	0	0	1	0	0	1	0	1	2
V_{124}: Not Considering Security in Early Phases of Development.	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1
V_{125}: Inconsistent Security Practices Application.	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1
V_{126}: Low/Poor Collaboration Levels of Security and DevOps.	0	0	0	0	0	1	0	0	0	1	0	0	1	0	1	2
Total Vulnerability Counts	545	49	24	96	17	15	208	127	142	390	21	33	1239	214	214	**1667**
		618			**128**			**477**			**444**			**1667**		