TechNova Security Solutions

SECURITY ASSESSMENT

2024-002 - DefectDojo Environment Analysis

21/08/2025

VERSION 1.0

TechNova Security Solutions | Global Security Department
Tech Boulevard 123, Denver, Colorado

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

TechNova Security Solutions conducted a comprehensive security assessment of the DefectDojo environment between August 17-21, 2025. This assessment analyzed the vulnerability management platform and its associated applications to identify security risks and provide actionable recommendations.

1.1 Scope

1.1.1 Systems

Product Name	Platform	Lifecycle	Business Criticality
Donkey Kong	Web	Production	High
Donkey Kong Jr.	Web	Production	High
Donkey Kong II	IoT	Retirement	Medium
Donkey Kong Hockey	Desktop	Retirement	High
Donkey Kong Circus	Web	Production	Medium

1.1.2 Testing Methods

The assessment utilized multiple security testing approaches:

- **Static Application Security Testing (SAST)** - Semgrep analysis
- **Software Composition Analysis (SCA)** - Snyk and BlackDuck scans
- **Container Security** - Trivy vulnerability scanning
- **Web Application Testing** - Burp GraphQL API analysis

1.1.3 Assessment Period

Assessment conducted over 40 hours between August 17-21, 2025, covering all critical production systems and security controls.

1.2 Result Summary

2,571
TOTAL FINDINGS

669
CRITICAL VULNERABILITIES

903
HIGH VULNERABILITIES

999
MEDIUM/LOW VULNERABILITIES

Severity	Count	Percentage	Status
CRITICAL	669	26.0%	Open
HIGH	903	35.1%	Open
MEDIUM	999	38.9%	Open

1.3 Estimated Risk

Overall Security Risk Assessment

6.6 / 10

HIGH RISK

The risk score of 6.6 indicates a **High Risk** security posture requiring immediate attention. This score is calculated based on the weighted severity distribution of identified vulnerabilities, with critical and high-severity findings comprising 61.1% of all detected issues.

1.4 Suggested Measures

Immediate Actions (0-30 days)

- **Critical Priority:** Address all 669 critical vulnerabilities immediately
- **Security Team Assembly:** Establish dedicated remediation team with daily standups
- **Emergency Patching:** Implement emergency patch deployment process
- **Access Controls:** Review and tighten authentication mechanisms

Short-term Actions (30-90 days)

- **High Severity Remediation:** Systematic approach to 903 high-severity findings
- **Security Controls Enhancement:** Implement additional defensive measures
- **Automated Scanning:** Establish continuous security monitoring
- **Developer Training:** Security awareness and secure coding practices

Long-term Strategy (90+ days)

- **Security Architecture Review:** Comprehensive security design assessment
- **DevSecOps Integration:** Security-first development lifecycle
- **Regular Assessments:** Quarterly security testing program
- **Compliance Framework:** Industry standard adherence (NIST, ISO 27001)

2 VULNERABILITY DETAILS

congregation.fact.comfort-jewelry

Critical

CWE: CWE-545

File: /weaeR/RGaRn/UrfuYthingdds.bak

Line: 924

Risk Level: Medium

Description: Critical vulnerability involving improper validation of security parameters. Code analysis reveals potential for privilege escalation through manipulation of security controls.

Code Snippet:

```
for _, v := range arr {fmt.Println(v)}
```

Remediation

- Implement proper input validation and sanitization
- Use secure cryptographic implementations: `javax.crypto.Cipher.getInstance("AES/GCM/NoPadding")`
- Apply principle of least privilege to affected components

orchard.permission.happiness-jealousy

High

CWE: CWE-14

File: /OHnetpairmpa.flv

Line: 734

Risk Level: Medium

Description: Compiler removal of code to clear buffers creates potential for information disclosure. Sensitive data may remain in memory after intended clearing operations.

Remediation

- Implement secure memory clearing functions that cannot be optimized away
- Use volatile qualifiers for security-critical buffer operations
- Consider platform-specific secure memory clearing APIs

2.1 Top Common Weakness Enumerations (CWE)

CWE ID	Description	Frequency	Risk Impact
CWE-393	Return of Wrong Status Code	High	Medium
CWE-449	UI Performs Wrong Action	High	Medium
CWE-394	Unexpected Status Code or Return Value	Medium	Medium
CWE-14	Compiler Removal of Code to Clear Buffers	Medium	High
CWE-519	Compromised Credentials	Low	Critical

3 METHODOLOGY OVERVIEW

The security assessment methodology employed by TechNova Security Solutions follows industry best practices and standards including:

3.1 Framework Alignment

- **OWASP Top 10:** Web application security testing guidelines
- **NIST Cybersecurity Framework:** Risk assessment and management
- **SANS Testing Methodology:** Systematic vulnerability identification
- **DefectDojo Integration:** Vulnerability management lifecycle

3.2 Testing Tools and Techniques

4 SCANNING TECHNOLOGIES	**19** TEST CONFIGURATIONS
5 PRODUCTS ASSESSED	**100%** COVERAGE ACHIEVED

3.3 Quality Assurance

All findings undergo rigorous validation including:

- Automated verification through multiple scanning engines
- Manual validation of critical and high-severity findings
- False positive analysis and risk contextualization

- Business impact assessment for prioritization