

SECURE SOFTWARE APPLICATION

TVET CDACC UNIT CODE: SEC/OS/CS/CR/06/5/MA

UNIT DESCRIPTION

This unit covers the competencies required to secure software application. Competencies include Identifying software to be secured, establishing tools for application security assessment, perform application security assessment, hardening software application, monitoring application security performance and preparing of reports on software security.

ELEMENTS AND PERFORMANCE CRITERIA

ELEMENT	PERFORMANCE CRITERIA
These describe the key outcomes which make up workplace function.	These are assessable statements which specify the required level of performance for each of the elements. <i>(Bold and italicised terms are elaborated in the Range)</i>
1. Identify software to be secured	1.1 Organizational requirements and security policies are reviewed to determine software security needs. 1.2 Software applications (desktop, web, mobile, cloud-based) are identified for assessment. 1.3 Application functions, workflows, and user roles are analyzed to determine potential security risks. 1.4 Existing security controls and vulnerabilities in the software are documented. 1.5 Software components (databases, APIs, third-party libraries, integrations) are identified as part of the security scope. 1.6 Software to be secured is prioritized based on criticality, sensitivity of data handled, and business impact.
2. Establish tools for application security assessment	2.1 Security assessment requirements are identified in line with organizational policies and industry standards. 2.2 Appropriate security assessment tools (static analysis, dynamic analysis, penetration testing, vulnerability

	scanners, code review tools) are selected based on application type. 2.3 Open-source and commercial tools are evaluated for effectiveness, compatibility, and cost-efficiency. 2.4 Testing environments are set up to ensure safe execution of security assessment tools without disrupting production systems. 2.5 Security benchmarks and baselines (e.g., OWASP, NIST, ISO/IEC 27001) are established for tool configuration. 2.6 Selected tools are installed, configured, and validated to ensure accuracy of results. 2.7 Documentation of assessment tools, usage procedures, and configurations is prepared for future reference.
3. Perform application security assessment	3.1 Security assessment is planned in accordance with organizational policies and scope of the software application. 3.2 Static application security testing (SAST) is conducted to identify vulnerabilities in source code. 3.3 Dynamic application security testing (DAST) is performed to detect runtime vulnerabilities. 3.4 Penetration testing is carried out to simulate real-world attack scenarios. 3.5 Vulnerabilities related to authentication, authorization, input validation, and session management are identified and documented. 3.6 Third-party libraries, APIs, and integrations are tested for security weaknesses. 3.7 Assessment results are analyzed and prioritized based on severity, exploitability, and potential business impact. 3.8 A detailed vulnerability report is generated and

	submitted for corrective action.
4. Harden software application	4.1 Security vulnerabilities identified during assessment are prioritized and addressed according to severity. 4.2 Secure coding practices are applied to mitigate common threats such as SQL injection, cross-site scripting (XSS), buffer overflows, and insecure APIs. 4.3 Application configuration settings are reviewed and adjusted to enforce security best practices. 4.4 Strong authentication and authorization mechanisms are implemented to control user access. 4.5 Sensitive data is protected through encryption, hashing, and secure key management. 4.6 Application dependencies, libraries, and frameworks are updated and patched to eliminate known vulnerabilities. 4.7 Security hardening guidelines are applied to the application environment. 4.8 Hardened application is tested to verify that vulnerabilities have been mitigated and functionality is not compromised.
5. Monitor application security performance	5.1 Application security logs and audit trails are reviewed regularly to detect suspicious activities. 5.2 Security monitoring tools (e.g., SIEM, IDS/IPS, application firewalls) are configured to track application behaviour. 5.3 Key security metrics (failed login attempts, privilege escalations, abnormal traffic patterns) are analyzed to assess performance. 5.4 Vulnerability scans and penetration tests are scheduled periodically to evaluate ongoing security posture. 5.5 Alerts and notifications are generated to provide real-time response to potential threats.

	5.6 Incident response procedures are followed to address detected security breaches. 5.7 Monitoring results are documented and reported in line with organizational and compliance requirements. 5.8 Application security policies and controls are reviewed and updated based on monitoring outcomes.
6. Prepare a report on software security	6.1 Findings from security assessments, hardening activities, and monitoring are compiled into a comprehensive report. 6.2 Report includes identified vulnerabilities, corrective actions taken, and residual risks. 6.3 Security performance metrics and incident response outcomes are documented. 6.4 Compliance with organizational policies, legal, and regulatory standards is verified and included in the report. 6.5 Recommendations for continuous improvement and future security enhancements are outlined. 6.6 Report is formatted according to organizational templates and presented to relevant stakeholders. 6.7 Documentation is stored securely and updated regularly to reflect changes in the application's security posture.

RANGE

This section provides work environments and conditions to which the performance criteria apply. It allows for different work environments and situations that will affect performance.

Variable	Range
Software applications for assessment may include but not limited to:	• Database applications • Web applications • Mobile applications • Cloud-based applications

Software components may include but not limited to:	• Databases • APIs • Third-party libraries • System integrations
Security assessment requirements may be based on but not limited to:	• Organizational policies • Security standards • Compliance regulations
Assessment tools may include but not limited to:	• Open-source tools • Commercial tools • Automated scanners • Manual testing utilities
Security benchmarks and baselines may include but not limited to:	• OWASP • NIST • ISO/IEC 27001 • Industry-specific standards
Assessment activities may include but not limited to:	• Development of assessment plan • Vulnerability scanning • Penetration testing • Risk documentation
Security monitoring tools may include but not limited to:	• SIEM • IDS/IPS • Firewalls • Log management systems
Monitoring activities may include but not limited to:	• Scheduled vulnerability scans • Continuous penetration testing • Tracking application behaviour
Compliance verification may include but not limited to:	• Organizational policies • Legal standards • Regulatory requirements • Industry-specific compliance frameworks

REQUIRED KNOWLEDGE AND UNDERSTANDING

The individual needs to demonstrate knowledge and understanding of:

- Recognizing and classifying different types of applications (desktop, web, mobile, cloud).
- Analyzing application functions, workflows, and user roles to assess risks.
- Identifying security assessment requirements aligned with policies and industry standards.
- Installing, configuring, and validating tools for accurate results.
- Performing penetration testing to simulate real-world attacks.
- Producing a detailed vulnerability report for corrective action.
- Applying secure coding practices to mitigate common threats (SQLi, XSS, buffer overflow, insecure APIs).
- Reviewing logs and audit trails for suspicious activities.
- Documenting vulnerabilities, corrective actions, and residual risks.

FOUNDATION SKILLS

The individual needs to demonstrate the following additional skills:

- Communications (verbal and written);
- Proficient in Digital Literacy;
- Time management;
- Analytical
- Problem solving;
- Planning;
- Decision making;
- Report writing;

EVIDENCE GUIDE

This provides advice on assessment and must be read in conjunction with the performance criteria, required skills and understanding and range.

1. Critical Aspects of Competency	Assessment requires evidence that the candidate: 1.1 List of software applications (desktop, web, mobile, cloud-based) was identified for security assessment. 1.2 Application functions, workflows, and user roles were analyzed and documented to highlight potential risks. 1.3 Software components such as databases, APIs, third-party
-----------------------------------	--

	libraries, and integrations were identified as part of the security scope. 1.4 Security assessment requirements were identified and documented in line with organizational policies and standards. 1.5 Evaluation of open-source and commercial tools was documented with considerations of effectiveness, compatibility, and cost-efficiency. 1.6 Security benchmarks and baselines (OWASP, NIST, ISO/IEC 27001) were established and documented for tool configuration. 1.7 Security assessment plan was developed and documented in line with organizational policies and defined scope. 1.8 Penetration testing findings were documented to demonstrate simulated attack scenarios. 1.9 Prioritized list of vulnerabilities was addressed and documented according to severity levels. 1.10 Secure coding practices were applied and documented to mitigate common threats such as SQL injection, XSS, and buffer overflows. 1.11 Security hardening guidelines were applied to the application environment and documented. 1.12 Security monitoring tools (SIEM, IDS/IPS, firewalls) were configured and documented to track application behavior. 1.13 Scheduled vulnerability scans and penetration tests were performed and documented to maintain security posture. 1.14 Monitoring results were documented and reported according to organizational and compliance requirements. 1.15 Findings from assessments, hardening, and monitoring were compiled and documented into a comprehensive report. 1.16 Security performance metrics and incident response outcomes were recorded and documented. 1.17 Compliance with organizational policies, legal, and regulatory standards was verified and included in the report.
--	---

2. Resource Implications for competent certification	The following resources should be provided: 2.1 Access to relevant workplace where assessment can take place 2.2 Appropriately simulated environment where assessment can take place 2.3 Materials relevant to the proposed activity or tasks
3. Methods of Assessment	Competency may be assessed through: 3.1 Oral questioning 3.2 Practical demonstration 3.3 Observation
4. Context of Assessment	Competency may be assessed individually in the actual workplace or through simulated work environment
5. Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended.