

## SECURE SOFTWARE APPLICATION

**ISCED UNIT CODE:** 0612554 06A

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

### Relationship to Occupational Standards

This unit addresses the unit of competency: Secure Software Application

**Duration of Unit:** 150 hours

### Unit Description

This unit covers the competencies required to secure software application. It involves 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.

### Summary of Learning Outcomes

| Learning Outcomes                                      | Durations (Hours) |
|--------------------------------------------------------|-------------------|
| 1. Identify software to be secured                     | 20                |
| 2. Establish tools for application security assessment | 20                |
| 3. Perform application security assessment             | 30                |
| 4. Harden software application                         | 30                |
| 5. Monitor application security performance            | 30                |
| 6. Prepare a report on software security               | 20                |
| <b>Total Hours</b>                                     | <b>150</b>        |

## Learning Outcomes, Content and Suggested Assessment Methods

| Learning Outcome                                       | Content                                                                                                                                                                                                                                                                                                                                                                                               | Suggested Assessment Methods                                                                                                                    |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Identify software to be secured                     | 1.1 Meaning of Terms<br>1.2 Types of software<br>1.3 Classification of software and their application<br>1.4 Factors influencing software selection<br>1.5 Identify Software That Needs Security<br>1.6 Identify existing list of installed software<br>1.7 Check software security updates<br>1.8 Research CVE Vulnerabilities for listed software                                                   | <ul style="list-style-type: none"> <li>• Observation</li> <li>• Written tests</li> <li>• Oral questioning</li> <li>• Practical tests</li> </ul> |
| 2. Establish tools for application security assessment | 2.1 Types of tools used in software application security assessment<br>2.2 Assessing software application<br>2.2.1 Input Validation<br>2.2.2 Session Management<br>2.2.3 Error Handling<br>2.3 OWASP Security Knowledge framework (SKF) Threat Modelling<br>2.4 Perform common vulnerabilities.<br>2.5 Asses the security posture of a web application<br>2.6 Conduct security assessment using tools | <ul style="list-style-type: none"> <li>• Observation</li> <li>• Written tests</li> <li>• Oral questioning</li> <li>• Practical tests</li> </ul> |
| 3. Perform application security assessment             | 3.1 Introduction to application security<br>3.2 Phases of application security assessment<br>3.3 Reconnaissance and information                                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>• Observation</li> <li>• Written tests</li> <li>• Oral questioning</li> <li>• Practical tests</li> </ul> |

| Learning Outcome               | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Suggested Assessment Methods                                                                                                                    |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | gathering<br>3.3.1 Passive information gathering<br>3.3.2 Active information gathering<br>3.4 Threat modelling<br>3.4.1 STRIDE model<br>3.4.2 PASTA model<br>3.5 Vulnerability Assessment<br>3.5.1 Manual Testing<br>3.5.2 Automated Scanning Tools<br>3.6 Exploitation and verification<br>3.7 Best Practices                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                 |
| 4. Harden software application | 4.1 Introduction to Software Hardening<br>4.2 Basic security principles for software applications.<br>4.3 Software configuration<br>4.4 Common threats to applications.<br>4.5 Software Vulnerabilities<br>4.5.1 Injection Attacks (SQL Injection, Command Injection).<br>4.5.2 Broken Authentication and Session Management.<br>4.5.3 Cross-Site Scripting (XSS).<br>4.5.4 Insecure Deserialization.<br>4.5.5 Misconfigured Security Headers.<br>4.6 Security measures in software application<br>4.7 Hardening techniques<br>4.7.1 Secure coding practices<br>4.7.2 Applying least privilege principle<br>4.7.3 Secure configuration of software | <ul style="list-style-type: none"> <li>• Observation</li> <li>• Written tests</li> <li>• Oral questioning</li> <li>• Practical tests</li> </ul> |

| Learning Outcome                            | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Suggested Assessment Methods                                                                                                                    |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             | <p>components</p> <p>4.7.4 Secure deployment and monitoring</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                 |
| 5. Monitor application security performance | <p>5.1 Factors to consider in monitoring of application security performance</p> <p>5.2 Implementation of monitoring solutions</p> <p>5.3 Logs management and monitoring</p> <p>5.4 Key Metrics to Monitor</p> <p>5.4.1 Failed Login Attempts</p> <p>5.4.2 Unusual API Requests</p> <p>5.4.3 Changes in Application Files</p> <p>5.5 Web applications logs and log management tools</p> <p>5.5.1 Apache/Nginx logs -Access error and Security logs for web server Monitoring</p> <p>5.5.2 IIS logs</p> <p>5.5.3 ELK Stark</p> <p>5.6 Advanced monitoring tools and techniques.</p> <p>5.6.1 Security Information and Event Management (SIEM) tools</p> <p>5.6.2 Web application firewall (WAF) and security monitoring.</p> <p>5.6.3 Threat hunting with AI and Machine learning</p> | <ul style="list-style-type: none"> <li>• Observation</li> <li>• Written tests</li> <li>• Oral questioning</li> <li>• Practical tests</li> </ul> |
| 6. Prepare a report on software security    | <p>6.1 Application summary</p> <p>6.1.1 Overview of the application</p> <p>6.1.2 Security goals</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• Observation</li> <li>• Written tests</li> <li>• Oral questioning</li> </ul>                            |

| Learning Outcome | Content                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Suggested Assessment Methods                                        |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
|                  | 6.1.3 Key findings<br>6.2 Methodology<br>6.2.1 Assessment approach<br>6.2.2 Tools used<br>6.2.3 Testing environment<br>6.3 Vulnerabilities and Risks<br>6.3.1 Identified vulnerabilities<br>6.3.2 Severity and impact<br>6.3.3 Risk rating methodology<br>6.4 Security Controls<br>6.4.1 Existing security measures<br>6.4.2 Effectiveness<br>6.5 Recommendations<br>6.5.1 Security improvements<br>6.5.2 Best practices<br>6.5.3 Remediation timeline<br>6.6 Conclusion<br>6.7 Appendices<br>6.7.1 Detailed findings<br>6.7.2 References | <ul style="list-style-type: none"> <li>• Practical tests</li> </ul> |

### Suggested Methods of Instructions

- In Instructor led facilitation of theory
- Demonstration by trainer
- Practical work by trainee
- Viewing of related videos
- Group discussions

**Recommended Resources for 25 trainees.**

| <b>S/No.</b> | <b>Category/Item</b>                            | <b>Description/<br/>Specifications</b> | <b>Quantity</b> | <b>Recommended<br/>Ratio<br/>(Trainee: Item)</b> |
|--------------|-------------------------------------------------|----------------------------------------|-----------------|--------------------------------------------------|
| <b>A</b>     | <b>Learning Materials</b>                       |                                        |                 |                                                  |
| 1.           | Textbooks                                       |                                        | 13 pcs          | 13:1                                             |
| 2.           | Installation manuals                            |                                        | 5pcs            | 5:1                                              |
| 3.           | Charts                                          |                                        |                 |                                                  |
| 4.           | PowerPoint presentations                        | For trainer's<br>use                   |                 |                                                  |
| <b>B</b>     | <b>Learning Facilities &amp; infrastructure</b> |                                        |                 |                                                  |
| 5.           | Lecture/theory room                             |                                        | 1               | 25:1                                             |
| 6.           | Computer Laboratory                             |                                        | 1               | 25:1                                             |
| 7.           | Internet Connection                             |                                        |                 |                                                  |
| <b>C</b>     | <b>Consumable materials</b>                     |                                        |                 |                                                  |
| 8.           | Printing papers                                 |                                        | 1 ream          | 1:20                                             |
| 9.           | Toners                                          |                                        | 2 pcs           | 13:1                                             |
| 10.          | Assorted colour of whiteboard<br>markers        |                                        |                 |                                                  |
| <b>D</b>     | <b>Tools and Equipment</b>                      |                                        |                 |                                                  |
| 11.          | Computers/Smartphones                           |                                        | 25 pcs          | 1:1                                              |
| 12.          | Projector                                       |                                        | 1 pc            | 25:1                                             |
| 13.          | VMware/Oracle virtual box                       |                                        | 25 pc           | 1:1                                              |
| 14.          | Kali Linux or Parrot OS                         |                                        | 25 pc           | 1:1                                              |