SkillsDA®
Center for advance training

Individuals at this job are responsible for vulnerability assessment for applications, performing source code review, testing the source code, suggesting remediation actions, perform hardening and monitor organization's traffic and logs for threats.

NSQF - 7 Level

Job Family in Cyber Security
QP Name: SSC/Q0903
Analyst Application Security

SkillsDA®
Center for advance training

Certification Students will be awarded once after successfully completing the Course duration

Analyst Application Security - SFNOS 0909

Vulnerability Assessment for AppSec

Analyst Application Security - SFNOS 0910

Application Hardening and deployment configuration for minumum AppSec Vulnerabilities

Analyst Application Security - SFNOS 0911

Application Monitoring and Mitigation Strategies for AppSec

Total Theory Hours	36 Hours
Total Practical Hours	120 Hours
Total Course Duration	156 Hours

Each Course Fee	₹5000 + GST
Total Course Fee	₹15000 + GST

www.skillsda.com

futureskills®
A NASSCOM initiative

SkillsDA®
Center for advance training

futureskills®
A NASSCOM initiative

COURSE NAME

VULNERABILITY ASSESSMENT FOR APPSEC

SFNOS 0909

THEORY

- Explore heterogeneous potential threats
- Multi-dimensional application penetration testing | Conduct manual and automated penetration testing
- Evaluate factor-based criticality of information | Identify the application type/category w.r.t factors | Identify and Isolate root causes of vulnerabilities
- Different testing methods for applications
- Gather information via manual documentation review | Gather web-based information via automated tools
- Establish the application life cycle | Review application security design and architecture | Manual source code vulnerability assessment | Evaluate the vulnerabilities from root cause to solution mechanisms | Categorize vulnerabilities for weakness and sensitivity. | Requirements for securing application life cycle | Automate static, dynamic and interactive testing results
- Collate application security controls | Assess application vulnerability | Validate data for failed false positives | Develop an application tracker | Step-by-step audit trail for information classification | Secure data collection and storage procedures
- Industry ready application capabilities
- Application patching life cycle

Course Theory Duration - 13.5 Hours
Course Practical Duration – 38 Hours

Course Overall Duration – 51.5 Hours

Duration of quizzes/knowledge check - 140 minutes
No. of Quizzes/knowledge checks - 7
Total no. of questions/Knowledge checks - 20
No. of quiz attempts given to user - 3 attempts

Criteria for for awarding E-Certificate
80% course completion and Scoring 70% in Knowledge check

COURSE Fee:

₹ 5000 + GST

Access Duration

6 Months

Pre Requisites for learners: Learners should have an understanding of how the web works, and the basics web technologies and web development languages

PRACTICALS

LAB MANUAL

Intrusion detection techniques - Penetration testing methods - Risk assessment and treatment methods - Application testing methods - Information gathering techniques Vulnerability management techniques - Identifying sourcecode vulnerability - Code security using SonarQube - Web security using Apptrana - Web app testing using Wapiti and Skipfish - Web application security scanning using Netsparker - Code analysis using Spotbugs and Deepscan - Web security scan using OWASP ZAP - Test planning using JAMA - Security analysis requirement using security use cases

TOOLS/TECHNIQUES

Snort - Ollydbg - Splunk - Ekram system - Metasploit - Firebug - Nessus - Hyena Acunetix WVS - Superscan - Angry IP scanner - Nmap - Nessus - PILAR RM - CIS Controls - RM - ActivTrak Monitoring - IDA Pro - HTTP RAT - Acunetix - Cyber Triage - PSTools - GFI LanGuard - Power Spy - PILAR RM

SkillsDA®
Center for advance training

futureskills®
A NASSCOM initiative

COURSE NAME

APPLICATION HARDENING AND DEPLOYMENT CONFIGURATION FOR MINUMUM APPSEC VULNERABILITIES

SFNOS 0910

THEORY

- Identify & secure web servers and web | Review all applications for valid credentials | Review systems and applications to reduce the chance of exploitation | Apply access controls to applications and databases | Ensure patches for all web servers, web applications and databases
- Ensure STIGs for compliance with best practices | Review logs for web attacks and identify signs of compromise
- Implement defences such as firewalls & load balancer | Ensure that all applications connect with least privilege | Limit and monitor file creation in network | Configure application securely for minimum exposure and weaknesses | Secure applications via application testing, code review, WAF, etc.
- Check platforms for reported vulnerabilities and available patches
- Work on the established guidelines for security configuration and hardening | Establish mechanism and measures to ensure patches on all application assets
- Define security baseline for malware protection | Make business users aware of application vulnerability and patch requirements | Define strategy for management of patches and updates
- Identify a patch management life cycle process | Integrate patch management with the IT infrastructure management | Ensure that infrastructures are reengineered for patch management requirements
- Research best practices in hardening applications | Document the outcome of the tools and solutions

Course Theory Duration - 11.5 Hours
Course Practical Duration – 38 Hours

Course Overall Duration – 49.5 Hours

Duration of quizzes/knowledge check - 160 minutes
No. of Quizzes/knowledge checks - 8
Total no. of questions/Knowledge checks - 20
No. of quiz attempts given to user - 3 attempts

Criteria for for awarding E-Certificate
80% course completion and Scoring 70% in Knowledge check

COURSE Fee:

₹ 5000 + GST

Access Duration

6 Months

Pre Requisites for learners: Learners should have an understanding of how the web works, and the basics web technologies and web development languages

PRACTICALS

LAB MANUAL

Web application vulnerability scanning - Security breach prevention - Web application security techniques - Application vulnerability management techniques - Hardening techniques and standards - Application security and patch management - Managing patches and updates in web application - DAST techniques

TOOLS/TECHNIQUES

Manual - Arachni - Metasploit OWASP - Wireshark - Nmap - Manual - Nagios - pfsense OpenVAS - Metasploit - Snort - Nmap - OSSEC - Cryfs - Kali Linux - Skipfish - Oracle Traffic Director - Blackfire - Tideways - Splunk - Loggly - Papertrail - Netsparker - PCI Requirement - Fireeye - Open SSH - SolarWinds Patch Manager - Manageengine - WSUS RSI Secuirty - Appknox - Veracode - Netsparker

SkillsDA®
Center for advance training

futureskills®
A NASSCOM initiative

COURSE NAME

APPLICATION MONITORING AND MITIGATION STRATEGIES FOR APPSEC

SFNOS 0911

THEORY

- Verify the scope of application assets and system components | Use specified monitoring and data collection methods and tools
- Monitor application consoles using SIEM tool to detect security threats
- Define and establish operational processes for log management | Identify and capture all event logs via appropriate tools
- Ensure time stamping and synchronization of servers among all log sources | Maintain a tracker which captures inventory of Cyber security incidents related to applications | Work on the defined process for prioritization and handling of Cyber Security incidents | Raise incidents in Cyber Security Incident logging/reporting tools | Follow-up for taking actions on the incidents raised | Report the results of the monitoring, incident logging and closure activities using SOP
- Cyber Security incident/breach management plan to detect or report incidents | Assign the incident to the relevant persons following organizational procedures | Perform telemetry monitoring to identify security platform issues
- Characterize and analyse application traffic to identify anomalous activity and potential threats | Identify trends and patterns as per standard guidelines | Coordinate with computer network defense (CND) staff to validate network alerts | Perform event correlation to gain situational awareness and determine the threat potential | Categorize the priority of identified risks, their probability of occurrence and potential impact | Determine actions required to investigate and mitigate identified risks | Monitor external data sources and determine its impact on the enterprise
- Record and categorize the service request as per organizational policies | Prioritize the service request according to organizational guidelines | Obtain help or advice from specialist | Comply with relevant legislation, standards, policies and procedures

Course Theory Duration - 13 Hours
Course Practical Duration - 38 Hours

Course Overall Duration - 51 Hours

Duration of quizzes/knowledge check - 140 minutes
No. of Quizzes/knowledge checks - 7
No. of questions in each quiz/knowledge checks - 20
No. of quiz attempts given to user - 3 attempts

Criteria for awarding the E-certificate
80% course completion and Scoring 70% in Knowledge check

COURSE Fee:

₹ 5000 + GST

Access Duration

6 Months

Pre Requisites for learners: Learners should have an understanding of how the web works, and the basics web technologies and web development languages

PRACTICALS

LAB MANUAL

Incident handling and response techniques - Data collection and asset management - SIEM techniques - Managing logs using various applications - Cyber security incident management - Event correlation and risk prioritization - Network monitoring and management - Real time monitoring using various applications - Application performance monitoring

TOOLS/TECHNIQUES

Windows MBSA - Syslog server config - OSSIM - Splunk - Asset tracking - Event Log Explorer - Splunk - Snort IDS - Snort - Splunk Forwarder - dotDefender - Anti DDOS Guardian - Atom - Netcraft Toolbar - Wireshark - ntopng - Open Source Security Information Management - ELK Stack