इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

Digital India
Power To Empower

NIC National Informatics Centre



TRAINING SESSION ON:
SECURE WEB APPLICATION DEVELOPMENT & BEST PRACTICES

07th - 09th October-2026







Regional Application Security & Audit Division
National Informatics Centre
Bhubaneswar

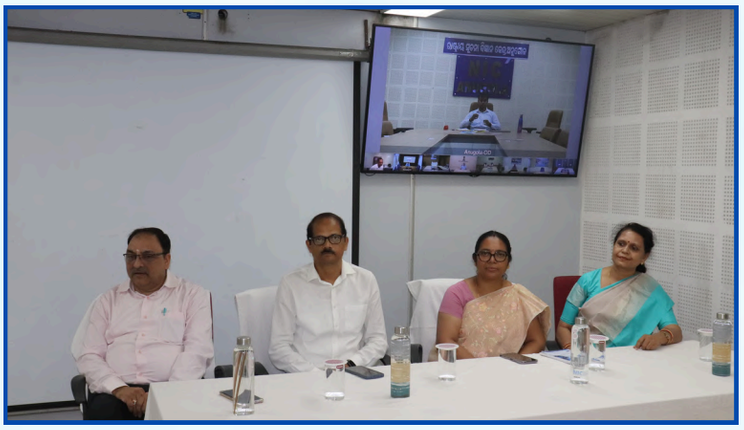
TRAINING SESSION ON :
SECURE WEB APPLICATION DEVELOPMENT & BEST PRACTICES

As part of the observance of Cyber Security Awareness month 2026, a three-day technical session on “Secure Web Application Development & Best Practices” was organized for officials and developers of NIC Odisha State Centre by the Regional Application Security & Audit Division, NIC Bhubaneswar, with the support of the Training Division, NIC Odisha, from 7th to 9th October 2026. Each session was conducted for two hours, with approximately 70 officials, including developers, participating in the programme.













TRAINING SESSION ON : SECURE WEB APPLICATION DEVELOPMENT & BEST PRACTICES

Delivering the Inaugural Address, Dr. A. K. Hota, SIO NIC Odisha, highlighted the significance of Cyber Security Awareness month and the 2026 cybersecurity theme, “Don’t Make It Easy for Them.” He emphasized that developers, as architects of applications, play a crucial role in safeguarding digital assets and stressed the importance of implementing security best practices at the early stages of the application development lifecycle.





In his address, Shri Jageswar Sahu, ASIO NIC Odisha, highlighted the importance of integrating security best practices into the application development lifecycle and emphasized the need for developers to carefully review audit reports and implement appropriate corrective measures. He further explained how even minor coding errors can compromise the application, potentially leading to security breaches and adversely affecting the credibility and reputation of the organization.

Welcoming the dignitaries and participants, Ms. Sasmeeta Sabat, HOD, Regional Application Security & Audit Division, outlined the objectives of the three-day technical session. She highlighted that three expert speakers would cover basic yet critical web application security issues based on OWASP guidelines. She also emphasized that security should be treated as a continuous process throughout the application lifecycle rather than an afterthought.



Shri Rajesh Mishra, DDG & HOG, Application Security Audit Division NIC HQ, joined the programme virtually and appreciated the initiative of conducting such technical training sessions for developers. He emphasized that these trainings would strengthen developers’ understanding of application security and help facilitate more efficient and effective security audits.

TRAINING SESSION ON :
SECURE WEB APPLICATION DEVELOPMENT & BEST PRACTICES

Day 1 commenced with a technical session by Ms. Sasmeeta Sabat, Scientist-E & HOD, Regional Application Security & Audit Division, on “Authentication and Authorization Techniques and Best Practices,” supported by practical demonstrations. She explained the importance of robust user authentication, secure access control, role-based permissions, and proper session management in web applications. The demonstrations highlighted common security weaknesses and emphasized implementing appropriate controls to prevent unauthorized access and privilege escalation.





Day 2 featured a technical session by Shri Rahul Kumar Sinha, Scientist-C & Deputy Director (IT), on “Vulnerable and Outdated Components, Insecure HTTP Security Headers, and Security Misconfigurations.” The session included practical demonstrations, different case studies, and recommendations on security best practices to help developers identify and mitigate common web application vulnerabilities.

Day 3 featured a technical session by Ms. Sanjukta Pradhan, Scientist-D & Joint Director (IT), on “Error Handling, Input Validation & Security Logging & Monitoring.” She covered different error-handling methods, whitelisting and blacklisting approaches & importance of logging, their security implications with practical demo, and best practices to prevent invalid inputs and avoid exposing sensitive information through error messages.





TRAINING SESSION ON :
SECURE WEB APPLICATION DEVELOPMENT & BEST PRACTICES

The concluding session featured an interactive quiz in the presence of the SIO, ASIO, and HOD-Training Division. Each speaker posed 10 multiple-choice questions to the participants, explaining the correct answers and their rationale. The session encouraged active participation and group discussions, and a small token of appreciation was presented to each participant.









