CWIL ACADEMY · COURSE CATALOGUE 2026–27

CW-RF

CWIL RedForge™

Offensive Security & Validation Programme

FLAGSHIP FORGE™ · OFFENSIVE

Authorised security testing, threat-informed validation and responsible reporting.

Aligned with NIST SP 800-115 · PTES · OWASP WSTG · ENISA ECSF

ABOUT THIS COURSE

Offensive Security treats testing as a bounded service that helps an owner make better decisions. The outline emphasises scope, evidence, safety controls, and remediation communication rather than unsupervised attack technique.

WHO IT IS FOR

Security testers, application and infrastructure engineers, and defenders who need to understand authorised adversary simulation.

PREREQUISITES

Working knowledge of TCP/IP, common application components, access control, and basic scripting concepts is recommended.

SYLLABUS, MODULE BY MODULE

01	Rules of engagement, consent & scope
02	Authorised asset discovery
03	Threat modelling & test selection
04	Evidence collection & impact reasoning
05	Communicating findings to owners
06	Retesting & responsible disclosure

LEARNING OUTCOMES

- Draft a bounded test plan with explicit authorisation and stop conditions
- Prioritise test questions using threat models and business context

- Record reproducible, non-destructive evidence without exposing sensitive data
- Write actionable findings that support remediation and safe retesting

LABS

Practice takes place in disposable, synthetic environments with deliberately simplified scenarios. Learners review supplied evidence and use benign validation exercises; the outline excludes exploit instructions, weaponisation, evasion, and activity against systems they do not own.

ASSESSMENT

Assessment is a scoped engagement plan, evidence register, and remediation report reviewed against authorisation, safety, reasoning, and communication criteria.

Register for CW-RF

Fees and batch dates are confirmed on enquiry. Remote, instructor-led, open across India.

cwil.in/register?course=cw-rf · info@cwil.in

IMPORTANT NOTICE

CWIL programmes are aligned with the frameworks listed and are not issued, endorsed or accredited by NIST, ISO, ENISA or any other standards body. CWIL credential and Forge™ programme names are trademarks of Cyber Warfare Intelligence Lab (OPC) Private Limited.