



THE XSS RAT · CERTIFICATION

Issued by Wesley Thijs · ratcerts.com

PROFESSIONAL

CNWPP

CERTIFIED NETWORK AND WEB APP PENTESTING PROFESSIONAL

This certifies that

Ariful Islam Anik

has demonstrated practical competence in network and web application penetration testing,
planning, executing and reporting a full engagement under examination conditions.

DATE OF AWARD

12 April 2026

ISSUED BY

The XSS Rat



CERTIFICATE ID

DA55-DBBD-4E39-081D

VERIFY AT

ratcerts.com/verify?code=DA55-DBBD-4E39-081D

Wesley Thijs · Founder & Lead Examiner
OSCP · CNWPP · CAPIE · CWAP



THE XSS RAT · CERTIFICATION

Issued by Wesley Thijs · ratcerts.com

SYLLABUS · PAGE 2 OF 3

CNWPP - What was taught

CERTIFIED NETWORK AND WEB APP PENTESTING PROFESSIONAL

HOW IT WAS EXAMINED

Full simulated engagement: scoping, NDA, test plan, network and web testing, final report, and a verbal exam with the examiner.

Chapter 1 · Defining what a pentest is

- Pentest methodologies overview
- Scoping a pentest
- The NDA and letter of engagement
- Deliverables: test plan, test report, notice of engagement
- How to handle a client
- The debriefing

Chapter 2 · Network scanning & exploits

- How we do a pentest
- Nmap and port scanning
- FTP and SMB enumeration and attacks
- Exploit-DB
- Wireshark, Zenmap, Nikto

Chapter 3 · Web exploits, part 1

- Fuzzing
- Burp Suite Community
- CSRF
- JWT attacks
- Open redirects
- SSRF (with labs)

Chapter 4 · Web exploits, part 2

- IDOR and broken access control in depth
- Business logic flaws
- CAPTCHA bypasses
- XPath injection
- Insecure deserialisation
- XSS: the art of exploitation



THE XSS RAT · CERTIFICATION

Issued by Wesley Thijs · ratcerts.com

SYLLABUS · PAGE 3 OF 3

CNWPP - What was taught

CERTIFIED NETWORK AND WEB APP PENTESTING PROFESSIONAL

CONTINUED

Chapter 5 · Methodologies

- Main-app methodology
- Broad-scope methodology
- Active Directory hacking overview

Chapter 6 · Vulnerability scanners & tools

- Vulnerability scanners
- Out-of-band servers
- Postman
- Scanning with OWASP ZAP

Chapter 7 · OWASP Top 10

- OWASP Top 10 (web), every category with demo
- OWASP API Top 10, every category with labs

Chapter 8 · The pentesting methodologies

- OSSTMM and the RAV calculation
- OWASP testing methodology
- PTES: pre-engagement and intelligence gathering
- Defining your full test from A to Z

Chapter 9 · Checklists

- FTP, SSH, SMB and HTTP enumeration
- OWASP WSTG checklist
- WebSocket testing
- Dangerous HTTP methods, directory brute forcing, content discovery

Chapter 10 · Simulated pentest

- Tying it all together in one attack
- Scoping meeting simulation
- Test plan template and final report