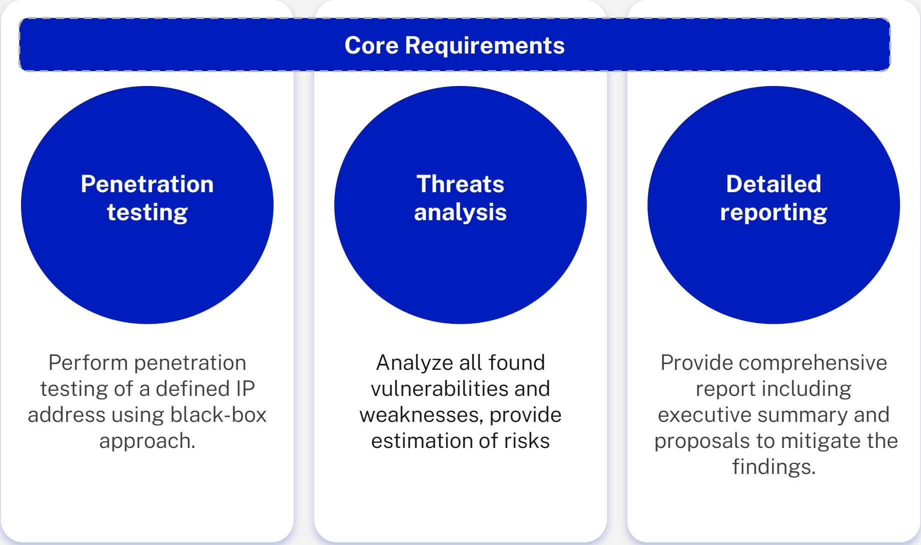
Why us?

CIKLUM

You're seeking a partner to help with **penetration testing** aiming at early vulnerabilities detection and thus, minimizing risks related to cyberattacks.



Core Requirements

Penetration testing

Perform penetration testing of a defined IP address using black-box approach.

Threats analysis

Analyze all found vulnerabilities and weaknesses, provide estimation of risks

Detailed reporting

Provide comprehensive report including executive summary and proposals to mitigate the findings.

60+ projects performed

DevSecOps Award, 2021 (finalist)

We believe that we are best placed to partner with you because:

1. We have **deep technical expertise** and can prove team's proficiency in the latest cybersecurity technologies, tools, and methodologies like OWASP or ISO 27001.
2. We specialize in **proactive threat intelligence**, showcasing our capability to anticipate emerging threats through consistent monitoring the threat landscape and analyzing novel attack vectors.
3. We employ a comprehensive **risk management** approach that focuses on identifying, prioritizing, and effectively mitigating risks, ensuring minimal impact from potential security incidents on our clients' operations.

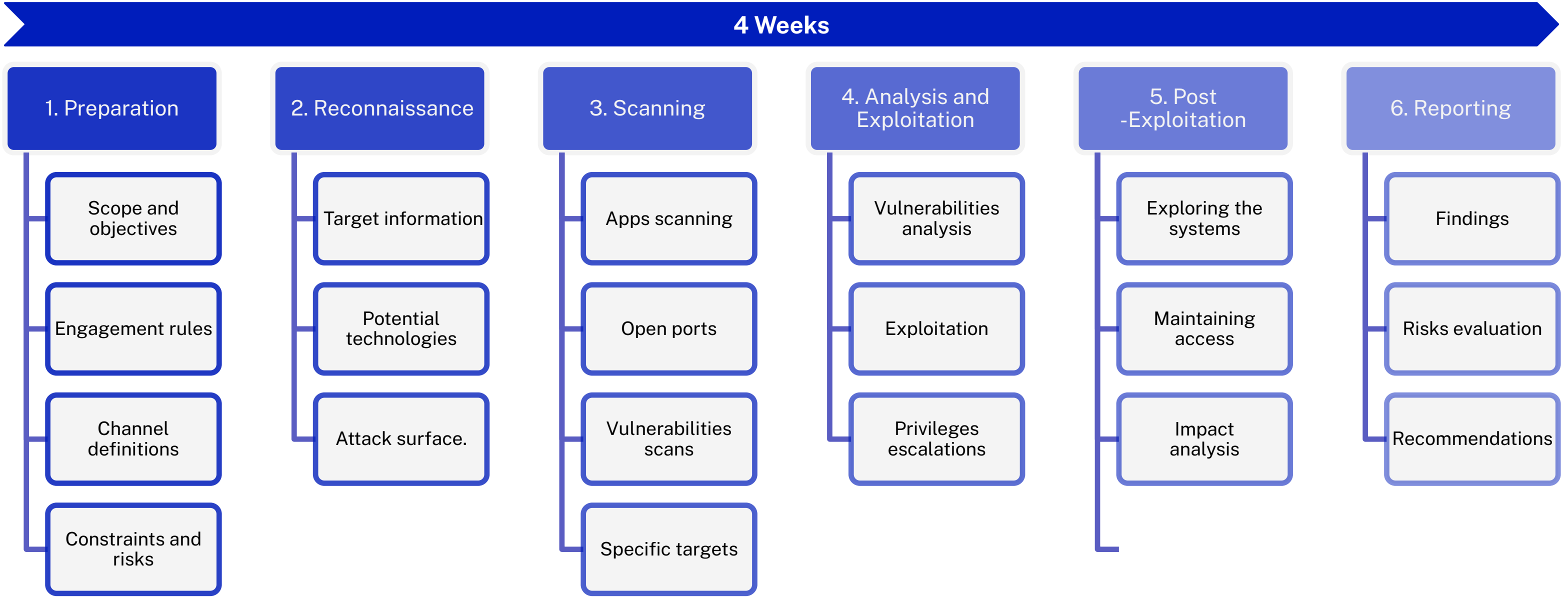
Typical scope

We would refine scope with you during the preparation phase, the typical scoping and outputs are outlined below.

- Tech stack identification (web servers, operating systems, programming languages, APIs).
- SQL injections (injecting malicious SQL queries).
- XSS - Cross-Site Scripting (injecting malicious scripts into input fields).
- XXE - XML External Entity (injecting malicious XML segments into input fields).
- Broken Authentication Testing (e.g. weak passwords or session management flaws).
- Sensitive Data Exposure Testing (handling the sensitive data such as user credentials, payment information, and personal information).
- Broken Access Control Testing (authorization concepts).
- Security Misconfigurations Testing (misconfigurations, default passwords or unnecessary services).
- Insecure Deserialization Testing (manipulating serialized objects sent to the application).
- Using Components with Known Vulnerabilities Testing.
- Insufficient Logging and Monitoring Testing (logging and monitoring mechanisms).
- IDOR - Insecure Direct Object References Testing (manipulating parameters in requests to access unauthorized data or functionality).
- CSRF - Cross-Site Request Forgery Testing (crafting malicious requests).

High level plan

CIKLUM



4 Weeks

1. Preparation
- Scope and objectives
- Engagement rules
- Channel definitions
- Constraints and risks

2. Reconnaissance
- Target information
- Potential technologies
- Attack surface.

3. Scanning
- Apps scanning
- Open ports
- Vulnerabilities scans
- Specific targets

4. Analysis and Exploitation
- Vulnerabilities analysis
- Exploitation
- Privileges escalations

5. Post -Exploitation
- Exploring the systems
- Maintaining access
- Impact analysis

6. Reporting
- Findings
- Risks evaluation
- Recommendations

Typical deliverables

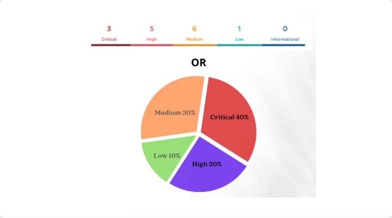
Penetration testing report comprising of:

- Detailed overview of the current status
- List of vulnerabilities found
- Risks and Severity evaluations
- Recommendations to improve

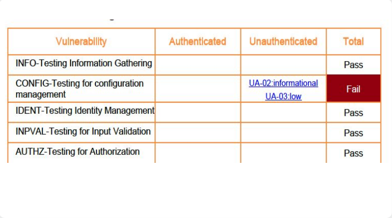
Value achieved:

- Vulnerabilities identification
- Overall security evaluation
- Overall risks reduction

Managerial summary

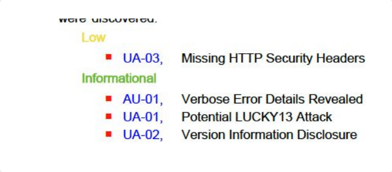


List of findings



Vulnerability	Authenticated	Unauthenticated	Total
INFO-Testing Information Gathering			Pass
CONFIG-Testing for configuration management		UA-02:informational UA-03:low	Fail
IDENT-Testing Identity Management			Pass
INPVAL-Testing for Input Validation			Pass
AUTHZ-Testing for Authorization			Pass

List of recommendations



were discovered.

Low

- UA-03, Missing HTTP Security Headers

Informational

- AU-01, Verbose Error Details Revealed
- UA-01, Potential LUCKY13 Attack
- UA-02, Version Information Disclosure