Services on offer

Pentesting - General

Our company can handle most types of modern pentesting, we offer services for the following types of test:

- Network pentesting in accordance with PTES
- Website pentesting according to the OWASP top 10, including covered CWE items by top 10
- Website pentesting according to the CWE top 25 vulnerabilities
- Website pentesting according to the OWASP WSTG
- Organization pentesting according to OSSTMM, this sets a coverage level goal and actions to get there. The coverage is measured according to the OSSTMM standards.
- API pentesting in accordance with PTES and our internal methodology which delivers a document outlining exactly what has been covered and what not with a mention of the degree of coverage

CWE = Common Web Exploit

OSSTMM = Open Source Security Testing Methodology Manual

WSTG = Web Security Testing Guide

All pentests come with the following deliverables:

- Contract
- Test plan
- Test report
- Coverage report
- Debriefing powerpoint

Pentests have a periodic meeting attached to them if they take longer than 1 week in accordance with the client.

Consultancy services

- Security training of internal staff, being developers, architects or analysts
- Set up an internal automation framework for security testing
- SDLC investigation and improvement, including dev ops

SDLC = Software Development Life Cycle

Maturity assessments

We will asses the maturity of your web application according to industry standards. This can either be OWASP ASVS, OWASP SAMM or NIST 800-115. You will get a detailed report of actions you should undertake to advance to the next level of maturity when it comes to your software and where it is still lacking according to these standards.

Industries we specialize in

We currently have experience in:

- Web 3.0 pentesting
- Crypto currency exchanges
- Medical sector/Hospitals/Doctors
- Food delivery
- Banking
- Public transport
- HR/CRM applications