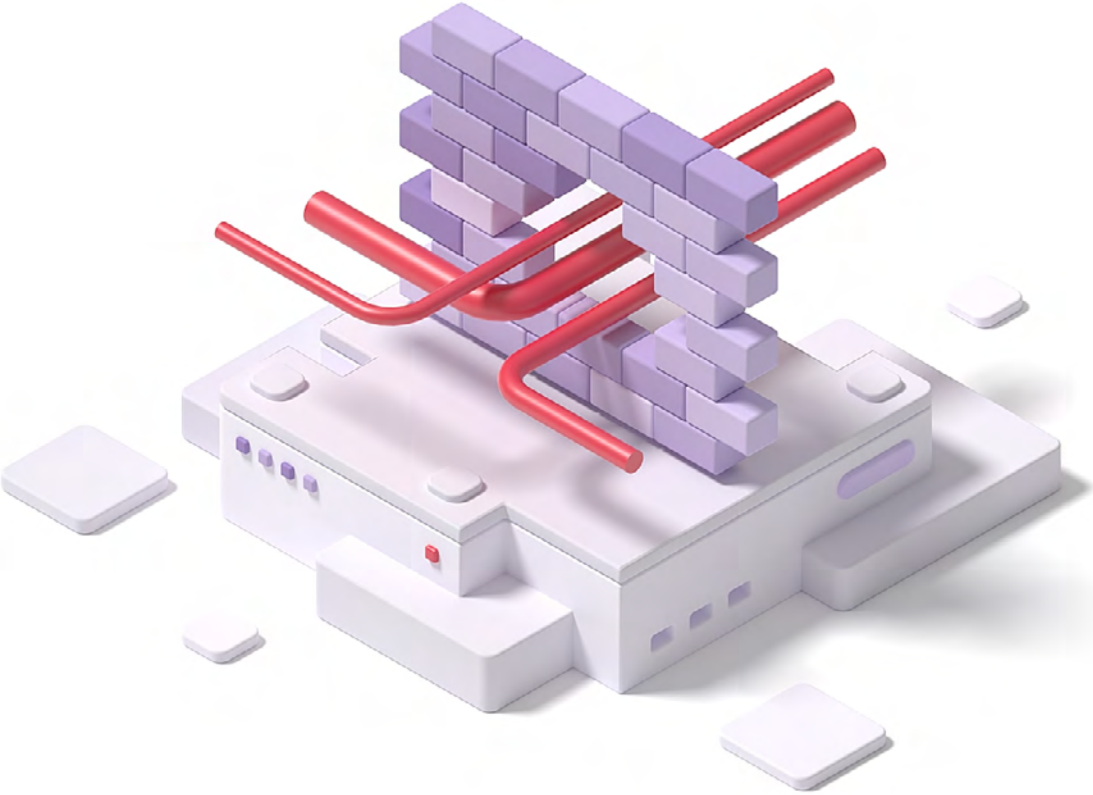
WebSec

WebSec Penetration Testing Whitepaper

Let us in to keep them out

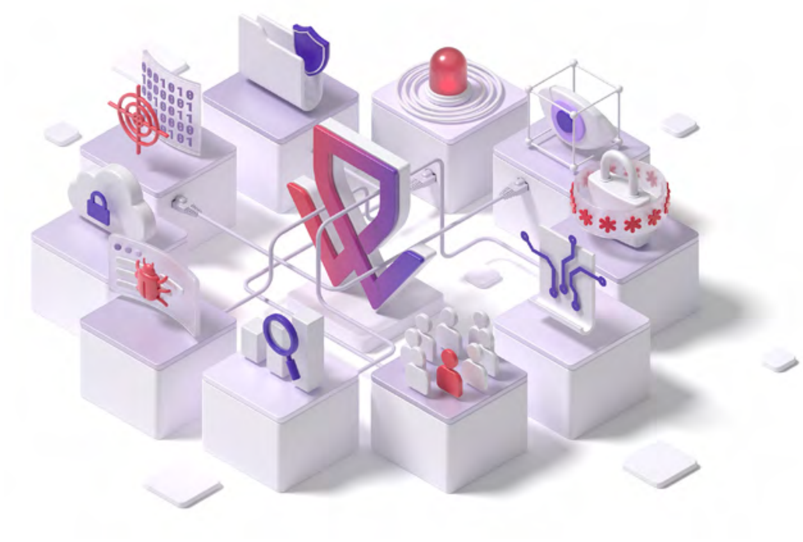


Vulnerability Assessment / Penetration Testing (VAPT)

Cybersecurity is a critical concern for all organizations. The ever-evolving threat landscape makes it challenging for businesses to secure their data. That's where our specialized service comes in. We offer proactive security services to check for system vulnerabilities.

Our team has extensive experience in various roles, from developers to IT admins and security specialists, so we can test systems from different angles to find all the weak points.

Our Penetration Testing services are tailored to meet the specific needs of each organization we work with. You can trust us to keep your information systems safe.



Our Services

At WebSec, we offer a wide range of cutting-edge penetration testing services to help secure your organization's critical assets.
Types of penetration testing that we do:

☑ Web Application Pentesting

The web application pentesting helps identify security flaws in your web-based software and applications, ensuring that your customer data and business information remains safe from cyberattacks.

☑ Mobile Application Pentesting

This service guarantees the security of your mobile apps, enabling you to provide your users with a seamless and secure experience.

☑ Infrastructure Pentesting

Our infrastructure pentesting service evaluates your organization's network infrastructure, including servers, firewalls, and routers, to identify potential weaknesses and vulnerabilities.

☑ Network Pentesting & Segmentation Testing

This service helps identify security flaws in your organization's network and segments, enabling you to implement more effective security measures.

☑ IoT Pentesting

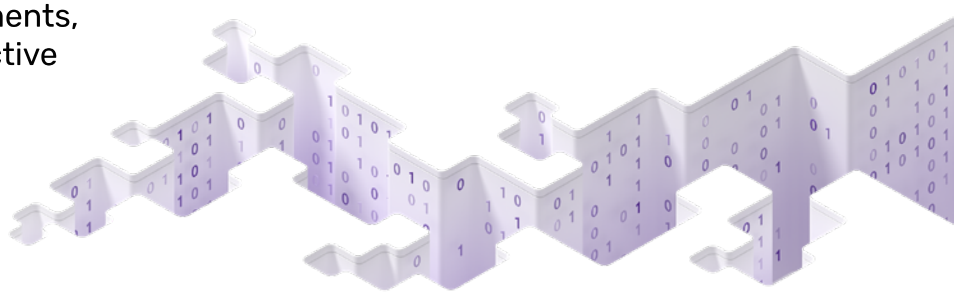
This is designed to test the security of Internet of Things (IoT) devices, ensuring that your smart devices and networks are secure and safe from cyber threats.

☑ SCADA / ICS Pentesting

Our ICS Pentesting service evaluates that the industrial control systems have been tested and configured in accordance with best ICS security practice and that there are no known or unknown vulnerabilities present in either the ICS hardware or software.

☑ API / Endpoint Pentesting

This pentesting service is designed to identify potential vulnerabilities and weaknesses in your organization's APIs and endpoints, ensuring that your data is secure and protected.



Compliance Pentests

At WebSec, we understand the importance of compliance and regulatory requirements in today's digital landscape. That's why we offer a range of compliance pentesting services to help you meet industry-specific standards and regulations.

Our team of experienced security experts uses the latest techniques and tools to deliver comprehensive compliance pentesting services. Trust us to help you meet regulatory requirements, protect sensitive data, and ensure the security of your organization's critical assets.

NEN-7510 Pentest (For Medical Institutes)

We offer NEN-7510 pentesting services to ensure that your organization meets healthcare data's highest information security standards.

ISO 27001 Pentest (For Quality Assurance)

Our ISO 27001 pentesting services help you evaluate your information security management system and ensure compliance with international standards.

BIO Pentest (For Dutch Government Institutes)

This helps you comply with the Baseline Government Information Security (BIO) requirements, ensuring your sensitive data remains safe and secure.

PCI-DSS Pentest (For Financial Institutes)

We offer PCI-DSS pentesting services to evaluate your organization's compliance with the Payment Card Industry Data Security Standard (PCI-DSS) and ensure the safety of your customers' financial data.

CoronaCheck-app Pentest (For Dutch Covid test centers/labs)

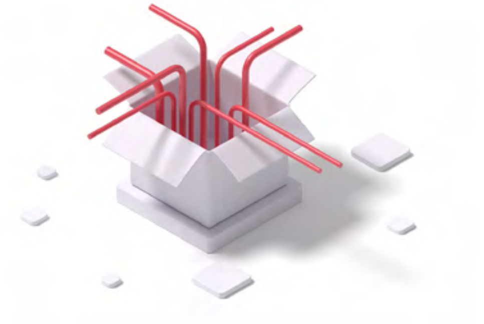
This is to help you meet the strict requirements for securing sensitive personal health information.

Pentest Approaches

We know that each organization has unique needs when it comes to penetration testing. That's why we offer a range of pentest approaches to fit the specific requirements.

White Box

Our White Box approach is perfect for organizations that want to evaluate their systems or applications comprehensively. With full knowledge and access to the source code, our security experts can accurately identify potential vulnerabilities and weaknesses in your systems.



Grey Box

For those who want a balance between comprehensive testing and real-world conditions, our Grey Box approach offers a solution. With little prior knowledge about your systems or applications, we can simulate a real-world attack scenario and identify potential security flaws in your organization's infrastructure.

Black Box

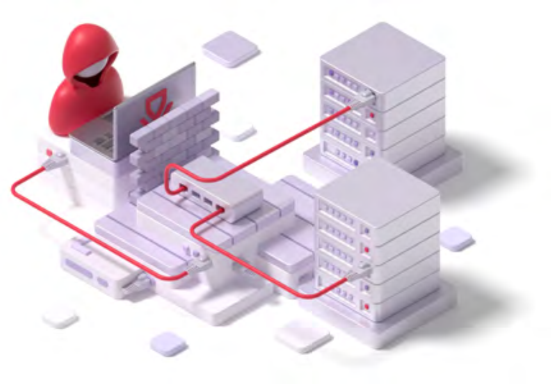
If you want to test your organization's ability to detect and respond to attacks, our Black Box approach is the perfect solution. With no prior knowledge about your systems or applications, we can simulate a real-world attack scenario and identify potential security flaws, allowing you to improve your security posture and better protect your critical assets.

Pentesting Areas

Identifying vulnerabilities and securing an organization’s critical assets requires a clear understanding of penetration testing areas.

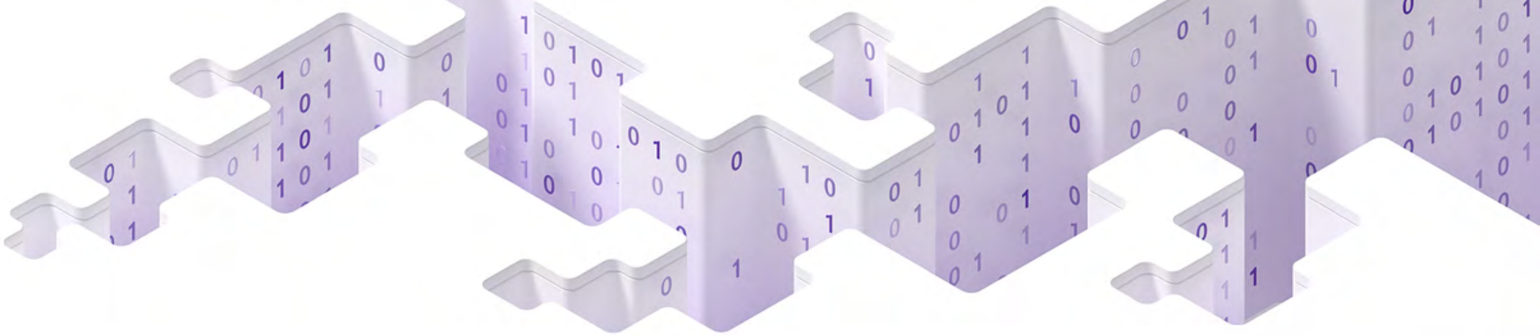
External Pentest

Our External Pentest approach allows us to remotely test your organization’s external-facing systems, applications, and networks. We perform this testing directly on your target IP address or domain, identifying potential vulnerabilities and weaknesses attackers could exploit.



Internal Pentest

For organizations with complex internal systems and networks, our Internal Pentest approach is the perfect solution. Our experienced security experts can perform this testing remotely through VPN or physically on location, identifying potential vulnerabilities and weaknesses in your internal infrastructure.



Our Pentesting Process

1. Intake
2. Pentestwaiver & Contract
3. Planning
4. Pentesting
5. Reporting
6. Aftercare

At WebSec, we believe in a systematic and comprehensive approach to penetration testing. Hence our complete pentesting process;

1. Intake: We start with an intake meeting to understand your organization's unique needs and specific requirements for the pentesting project.

2. Pentest Waiver & Contract: We ensure legal compliance and transparency by providing a pentest waiver and contract that outlines the project's scope, timeline, and expected deliverables.

3. Planning: We create a detailed pentesting plan that identifies potential vulnerabilities, testing methods, and timeline to ensure the most efficient use of resources.

4. Pentesting: Our experienced team of ethical hackers will test using the latest tools and techniques to identify potential security flaws.

5. Reporting: We provide a comprehensive and detailed report of the pentesting results, including an analysis of identified vulnerabilities and recommended remediation strategies.

6. Aftercare: Our commitment to you doesn't end with completing the pentesting project. We provide aftercare services, including ongoing monitoring and support, to secure your organization's critical assets.

We prioritize your organization's security and work tirelessly to identify and address potential vulnerabilities. Trust us to provide a reliable, transparent, and effective pentesting process.

How can we guarantee the quality of our pentests?

To ensure the quality of our testing and reporting, we utilize several security frameworks and standards in all of our tests, including:

OWASP: We follow the OWASP standards, including the ASVS, WSTG, and TOP 10, to ensure a comprehensive approach to identifying vulnerabilities.

PTES Standard: We adhere to the Penetration Testing Execution Standard (PTES) to ensure consistency and completeness in our testing methodology.

CCV PENTEST: The CCV PENTEST Trustmark verifies us as a global penetration testing service provider. This certificate validates our compliance with NEN- AND- ISO/IEC 17065 standards and ensures our provision of seamless pentesting services.

We pride ourselves on our experienced and certified team of security specialists. Our specialists are OSCP certified, with 2 to 5 years of experience in penetration testing or a related field.

CCV
CYBER PENTEST

Comprehensive Penetration Testing Deliverables by WebSec: Ensuring System Integrity and Enhancing Cybersecurity Awareness

At WebSec, our commitment to cybersecurity extends beyond conventional penetration testing. We provide a comprehensive suite of deliverables designed to certify and enhance the security resilience of your systems. Below is an overview of our main deliverables, along with additional options available to further bolster your cybersecurity posture:

Main Deliverables:

Technical Report

A detailed analysis of the penetration testing outcomes, including identified vulnerabilities and recommended remediations.

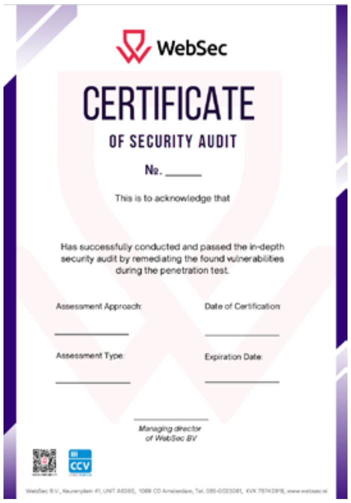
Management Report

High-level summary tailored for executive understanding, focusing on strategic insights and risk management implications.

Optional Deliverables:

VAPT (Vulnerability Assessment and Penetration Testing) Certification

An official certification recognizing the successful completion of rigorous testing and the attainment of security benchmarks.



WebSec

CERTIFICATE

OF SECURITY AUDIT

№. ______

This is to acknowledge that

Has successfully conducted and passed the in-depth security audit by remediating the found vulnerabilities during the penetration test.

Assessment Approach: ______

Date of Certification: ______

Assessment Type: ______

Expiration Date: ______

Managing director
of WebSec BV

WebSec B.V., Keurenplein 41, UNIT A6260, 1069 CD Amsterdam, Tel. 085-0023061, KVK 78742919, www.websec.nl

Digital Badge

A symbol / Trust Mark of cybersecurity diligence, this digital emblem can be displayed on your digital platforms to signify your commitment to robust security practices.

SECURED BY WEBSEC.NL
SECURED BY WEBSEC.NL
SECURED BY WEBSEC.NL