CYPRO AB

Web & Mobile App Penetration Testing

Predict   **Detect**   Protect   Respond   Recover
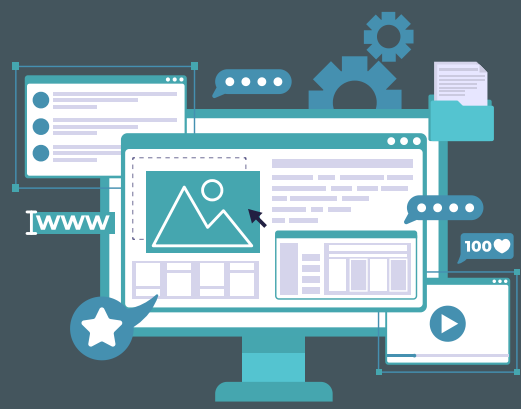
WEB APPLICATION PENTEST

Our expert follows ISO27001 standards and are well-equipped with latest cyber security certificates. Web Application Penetration Testing is a controlled and methodical assessment of your web-based applications to identify vulnerabilities and potential security loopholes. Our highly skilled and experienced Red Team experts simulate real-world cyber attacks to evaluate the strength and resilience of your web applications.

WHAT ARE THE BENEFITS?

- **Identifying Vulnerabilities:** both common and obscure security vulnerabilities that could be exploited by malicious actors.

- **Preventing Data Breaches:** which helps safeguard your organization's reputation, customer trust, and prevents potential legal and financial consequences.

- **NIS2 Web Compliance Requirements:** by performing these compliance tests such as PCI DSS, HIPAA, and GDPR, mandate regular security assessments, including penetration testing.

- **Enhancing Incident Response:** Pentest can helps aid your understanding of the attack vectors and swiftly mitigating the breach, reducing potential damage and downtime.

- **Protecting Business Continuity:** you ensure the continuous and uninterrupted operation of your your web applications, minimizing the risk of business impact.

- **Gaining Stakeholder Confidence:** by regularly conducting web application penetration tests.

COMPREHENSIVE TESTING PROCESS

Our process begins with an in-depth analysis of your web application's attack surface, aiming to simulate historical, innovative, and advanced intrusion methods, including:

- **Data Gathering**
- **System Identification**
- **Vulnerability assessment**
- **Exploitation**

We offer a robust Penetration Testing service designed to replicate the tactics, techniques, and procedures used by malicious actors. This includes:

- Comprehensive meetings with your development and security teams

- Access to relevant documentation for a deep understanding of your architecture and potential threat vectors

- Access your web application to identify all intentional and unintentional exposures

ABOUT US

Cypro AB will help you to comply with directives as NIS2 and standards as ISO 27001 with the mission to stay compliant and secure over time. Our top-tier global security assessment team includes experts specializing in red teaming and information security offers unparalleled insight into potential vulnerabilities.

A state-of-the-art Security Operations Center (SOC) enables us to deliver the highest level of security services, actively monitoring and responding to possible threats.

CONTACT US

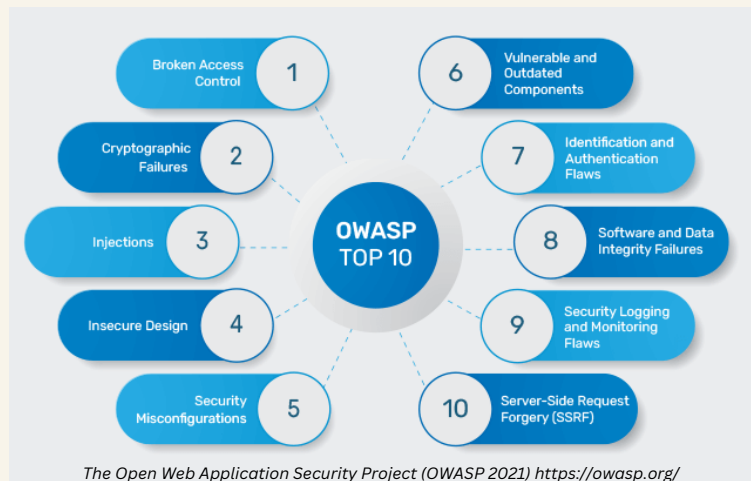contact@cypro.se
https://www.cypro.se

METHODOLOGY

Cypro System assessment methodology includes structured review processes based on recognized "best-in-class" practices as defined by such methodologies as MITRE, the Open Web Application Security Project OTG (OWASP). OWASP OTG refers to the OWASP Testing Guide Project, which is a comprehensive resource developed by the Open Web Application Security Project.

The following also gives a high-level description and process of Cypro methodology used for performing Penetration Testing.

Cypro uses the OWASP OTG Top ten lists as a guide for the application penetration testing. The methodology is based on a set of tests that targets the OWASP Top ten vulnerabilities and based on OWASP OTG.

The Open Web Application Security Project (OWASP 2021) https://owasp.org/

WHAT YOU'LL RECEIVE

Preparations
Statement of work. Scope meeting to set the agreed scope of work, roles and responsibilities, walk through of methodology.

Performing the test
Conduct the test according to agreed process and methodologies.
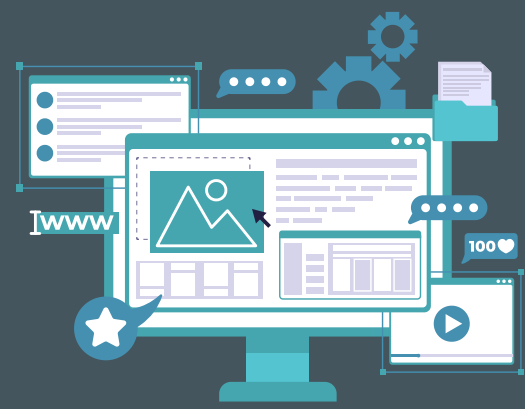
Reporting and follow up:
A detailed and reviewed security report. A report walk through containing executive summary, conclusions, recommendations, details on deliverables such as **CVE vulnerabilities, leaked usernames and passwords, malicious IP addresses, software used, similar domains, SSL Certificate Host Mismatch.**

READY TO BOOST YOUR CYBER SECURITY

Start by reaching out to your trusted Cypro customer contact or connecting with our experienced experts. Together, we embark on a transformative path to fortify your defenses, ensuring your valuable assets remain safe from harm.

CYPRO

Initiate Your Defense
Connect with Cypro's Experts Today!

CONTACT US

contact@cypro.se
https://www.cypro.se

CYPRO AB

Mobile Penetration Testing

Predict **Detect** **Protect** **Respond** **Recover**

MOBILE PENTEST

Our expert follows ISO27001 standards and are well-equipped with latest cyber security certificates. Mobile penetration testing is a security assessment conducted on mobile applications and devices to identify vulnerabilities and weaknesses that could be exploited by attackers. The ultimate goal is to provide actionable insights and recommendations for improving the security of mobile applications.

WHAT ARE THE BENEFITS?

- **Identifying Vulnerabilities:** uncover potential security flaws, vulnerabilities, and weaknesses in web and mobile applications.

- **Strengthening Security Posture:** conducting pentests making your web and mobile applications more resilient to cyber threats and attacks.

- **Safeguarding Sensitive Data:** pentes helps ensure that sensitive data, such as user credentials, personal information, and financial details.

- **Compliance and Regulations:** pentest assists organizations in meeting regulatory requirements and industry standards.

- **Reducing Financial Risks:** pentest helps mitigate the financial risks associated with potential data breaches, reputational damage, and legal liabilities.

- **Enhancing Customer Trust:** Regular pentest instills confidence in customers and stakeholders.

- **Improving Software Development:** Pentest feedback aids developers in understanding security best practices.

COMPREHENSIVE TESTING PROCESS

Our process begins with an in-depth analysis of your web application's attack surface, aiming to simulate historical, innovative, and advanced intrusion methods, including:

- **Data Gathering**
- **System Identification**
- **Vulnerability assessment**
- **Exploitation**

We offer a robust Penetration Testing service designed to replicate the tactics, techniques, and procedures used by malicious actors.

Our skilled Red Team employ a variety of techniques to probe for vulnerabilities, leaving no stone unturned. This includes examining the web application's front-end, back-end, APIs, and other potential attack surfaces.

ABOUT US

Cypro AB will help you to comply with directives as NIS2 and standards as ISO 27001 with the mission to stay compliant and secure over time. Our team of top-tier professionals includes GSAT (Global Security Assessment Team) experts, specializing in the red team domain, offering unparalleled insight into potential vulnerabilities.

A state-of-the-art Security Operations Center (SOC) enables us to deliver the highest level of security services, actively monitoring and responding to threats around the clock.

CONTACT US

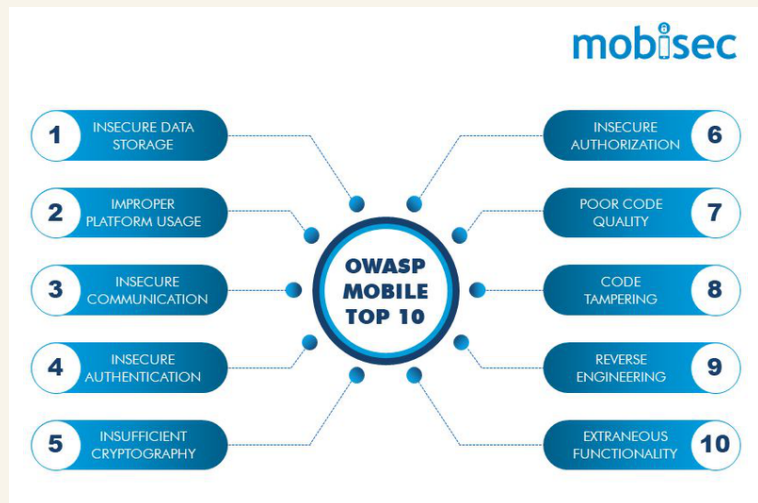contact@cypro.se
https://www.cypro.se

METHODOLOGY

Cypro System assessment methodology includes structured review processes based on recognized "best-in-class" practices as defined by such methodologies as MITRE, the Open Web Application Security Project OTG (OWASP). OWASP OTG refers to the OWASP Testing Guide Project, which is a comprehensive resource developed by the Open Web Application Security Project.

The following also gives a high-level description and process of Cypro methodology used for performing Penetration Testing.

Cypro uses the OWASP Top ten lists as a guide for the application penetration testing the methodology is based on a set of tests that targets the OWASP Top ten vulnerabilities and based on OWASP OTG.

mobisec

OWASP MOBILE TOP 10

1. INSECURE DATA STORAGE
2. IMPROPER PLATFORM USAGE
3. INSECURE COMMUNICATION
4. INSECURE AUTHENTICATION
5. INSUFFICIENT CRYPTOGRAPHY
6. INSECURE AUTHORIZATION
7. POOR CODE QUALITY
8. CODE TAMPERING
9. REVERSE ENGINEERING
10. EXTRANEOUS FUNCTIONALITY

WHAT YOU'LL RECEIVE

Preparations: Statement of work. Scope meeting to set the agreed scope of work, roles and responsibilities, walk through of methodology.

Performing the test: Conduct the test according to agreed process and methodologies.

Reporting and follow up: A detailed and reviewed security report. A report walk through containing executive summary, conclusions, recommendations, details on deliverables such as **CVE vulnerabilities, leaked usernames and passwords, malicious IP addresses, software used, similar domains, SSL Certificate Host Mismatch.**

READY FOR BOOST YOUR CYBER SECURITY

Start by reaching out to your trusted Cypro customer contact or connecting with our experienced experts. Together, we embark on a transformative path to fortify your defenses, ensuring your valuable assets remain safe from harm.

CYPRO

Initiate Your Defense
Connect with Cypro's Experts Today!

CONTACT US

contact@cypro.se
https://www.cypro.se