MOBILE PENETRATION TESTING



Cybersecurity service BDO in Ukraine powered by ImmuniWeb®

Why it is important to keep your mobile application secure?

→ As unsecure apps could bring much financial & reputable losses for its users

So, if your company or business have...

- Mobile application of small size & complexity*
- with one or two endpoints
 (e.g. APIs or web services) and one user role

*however, we have solutions for each size & complexity if needed

...than the best solution would be to:

- ▶ DETECT OWASP Mobile Top 10 weaknesses in your iOS or Android mobile app and discover SANS Top 25 vulnerabilities in the endpoints
- ▶ REVIEW whether your mobile app privacy, compliance and encryption mechanisms conform to industry best practices

How we grant full security assessment of your mobile application?

→ Through performing of tech advanced penetration testing

What is it & how it works?

Using advanced solution by ImmuniWeb® MobileSuite we leverage Machine Learning technology to accelerate and enhance mobile penetration testing. Every mobile penetration test is equipped with a contractual zero false positives SLA and a money-back guarantee if there is even a single false positive.









Testing methodologies cover:

- ► OWASP Mobile Security Testing Guide (MSTG)
- ▶ NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- ▶ PCI DSS Information Supplement: Penetration Testing Guidance
- ► MITRE ATT&CK® Matrices for Mobile and Enterprise
- ► FedRAMP Penetration Test Guidance
- ▶ ISACA's How to Audit GDPR

How your mobile application benefits from using our service?

→ By completion of full tech review on vulnerabilities with further testing at no cost

What you get under guaranteed results?

- Detected business logic and authentication bypass vulnerabilities

- Export vulnerability data from interactive dashboard to PDF or directly into SIEM or bug tracking system for faster remediation

Unlimited patch verification assessments after the penetration test, so your software developers can easily validate whether all the findings have been properly patched

Reporting standards used:

- ▶ OWASP Application Security Verification Standard (ASVS v4.0.2) Mapping
- ► Common Vulnerabilities and Exposures (CVE) Compatible
- Common Weakness Enumeration (CWE) Compatible
- Common Vulnerability Scoring System (CVSS v3.1)

Interested?

Contact us:



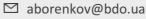






ANDRII BORENKOV

Director BDO Consulting



+380 50 380 96 01



BDO in Ukraine





