ITGLOBAL.COM
MANAGED IT. WORLDWIDE

Mobile applications' security testing

2021

ABOUT US

ITGLOBAL.COM Security is the global provider of Information Security Services

Part of ITGLOBAL.COM, International IT Service provider with in-depth expertise in the security area

Branches in The Netherlands, USA, Russia, Belarus, Kazakhstan

Clients from Europe, USA, Middle East, Central America, Russia

Team of highly skilled and certified specialists

Why to protect mobile applications?

01 A great number of applications processes and stores sensitive information of the customers (email, contacts, API tokens)

02 Mobile applications are forced to operate in non-trusted Wi-Fi networks

03 Each mobile platform has its own and variable requirements towards security: this, among the others, has to be considered by the developers

04 The majority of developers are not trained to develop secure applications

05 The number of mobile devices' users grew significantly within the last years, so mobile applications are becoming an integral part of daily life

Security risks based on our expertise statistics

82%

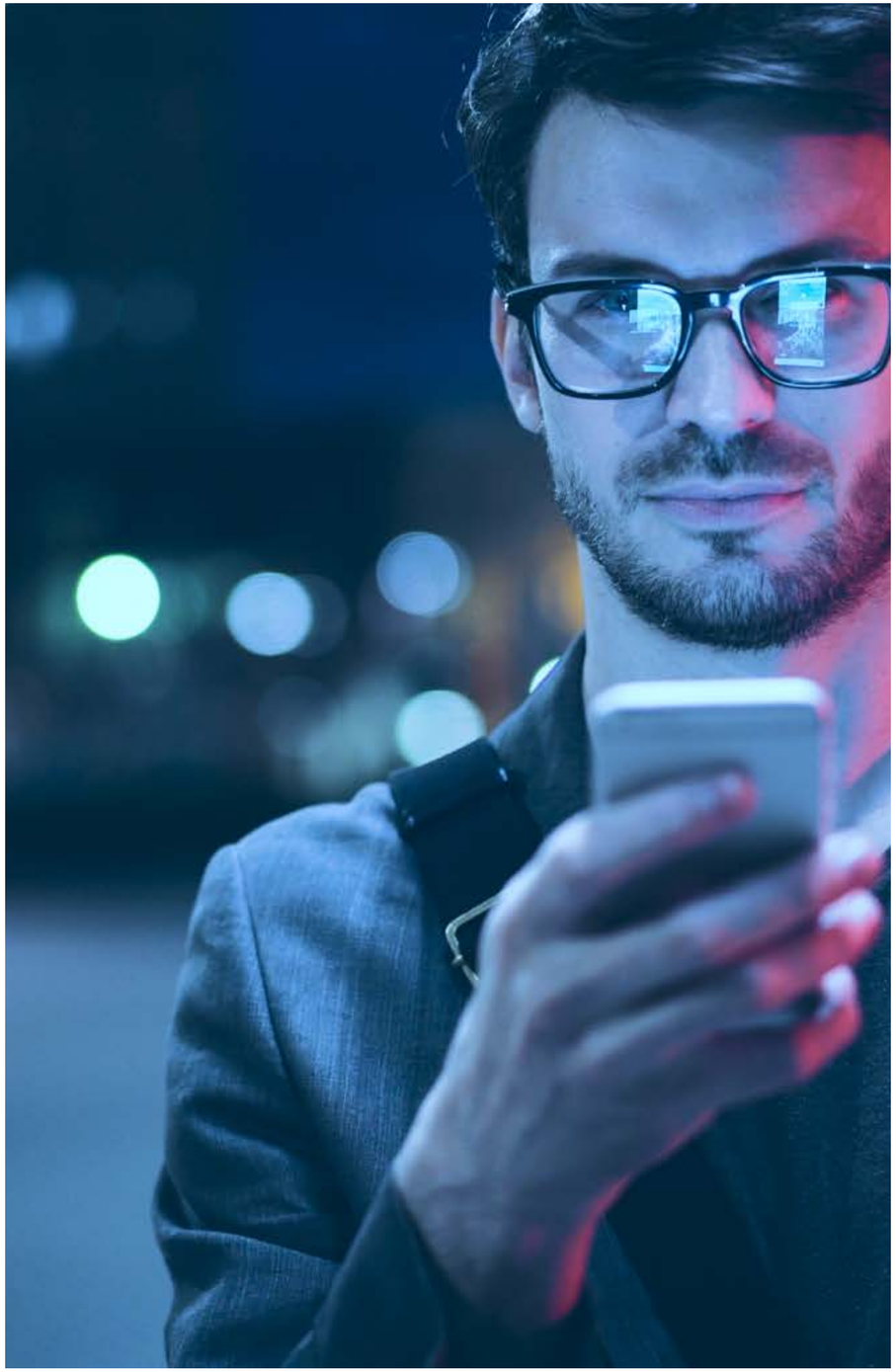
of tested retail applications have leaks of sensitive data

67%

of tested travel applications have leaks of sensitive data

82%

of tested financial applications have leaks of sensitive data



What is (and what for) a mobile application pentest?

01 Possibility to uncover vulnerability in mobile application's cyber security – before an indruder can get a use of it

02 Specifically important for applications which process confidential data

03 (It) ensures that protection means embedded into a mobile application are valid and efficient

04 Testing can be performed on both IOS and Android applications

05 Risks of non-secure approaches to development are eliminated

Which applications can we test?

Native apps

developed initially for mobile devices under specific platforms, for example, Android or IOS

Web apps

they work just like native apps, but are available via a web browser of your mobile device. Web apps are developed using HTML5, CSS, JavaScript, Ruby and similar programming languages, which are used for work in the Internet.

Hybrid apps

these web apps look like native apps. They may have an icon on your screen, a flexible design, high performance and even the option to work offline. But in essence these are native-looking web apps.

What is the scope of mobile applications' pentest?

Source code examination

Source code examination helps to uncover main issues of a code – the ones that might not reveal themselves in a user interface.

API security evaluation

API is used to operate a mobile application. API is tested for business logic compliance and OWASP Top 10.

Servers' security evaluation

API and applications are placed on public servers. The servers has to pass standard tests on existence of vulnerabilities.

Stages of work

Reconnaissance

- OSINT
- Application's architecture exposure

Evaluation and Analysis

- Static analysis
- Local files' analysis
- Network and web traffic analysis
- Reverse engineering
- Inter-process interaction analysis
- Dynamic analysis

Exploitation

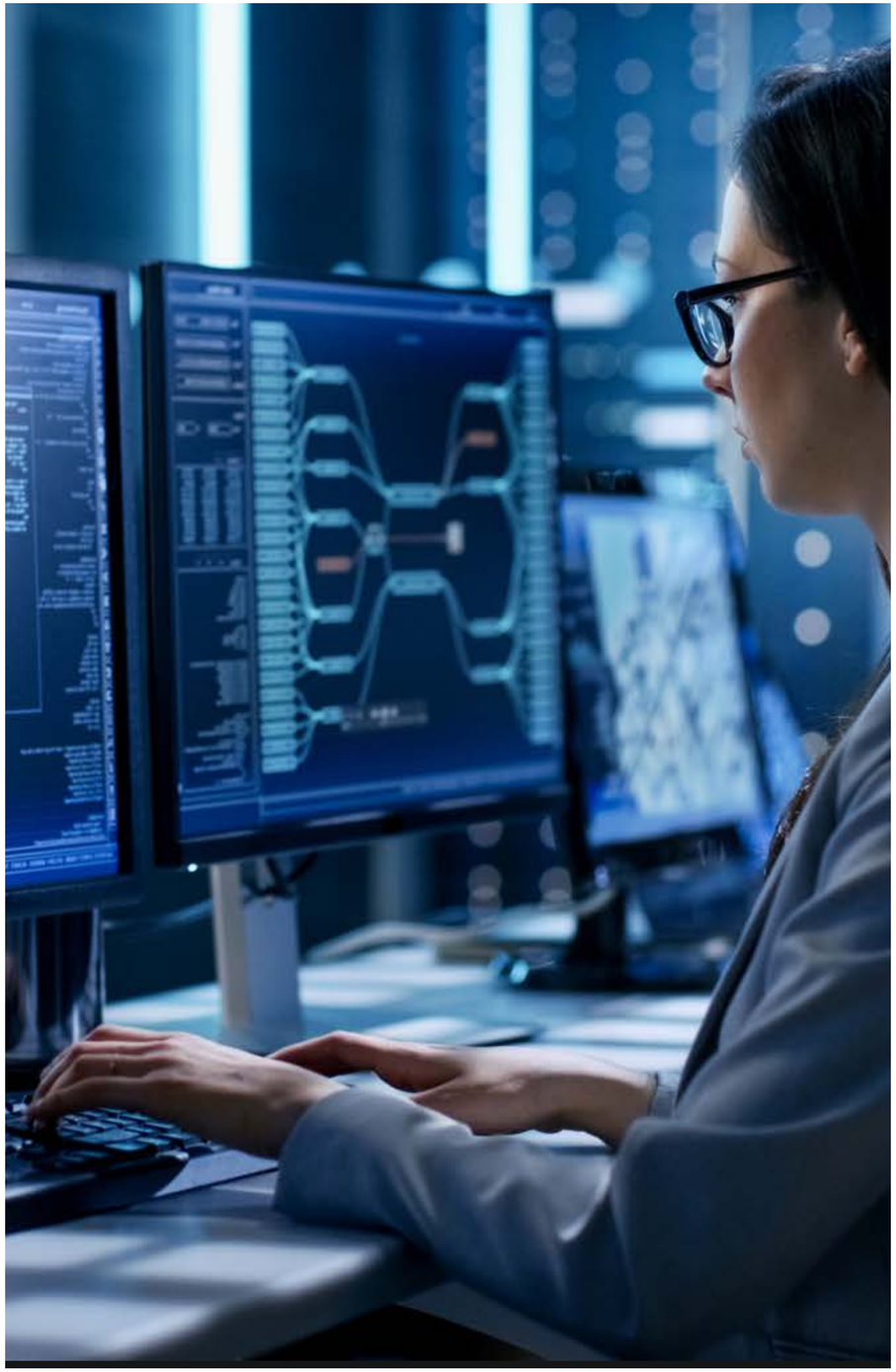
- Exploitation of found vulnerabilities
- Elevation of privilege
- Manipulation of input and transferred parameters

Reporting

- Evaluation of found vulnerabilities' risks
- Compliation of a report and provision of recommendations

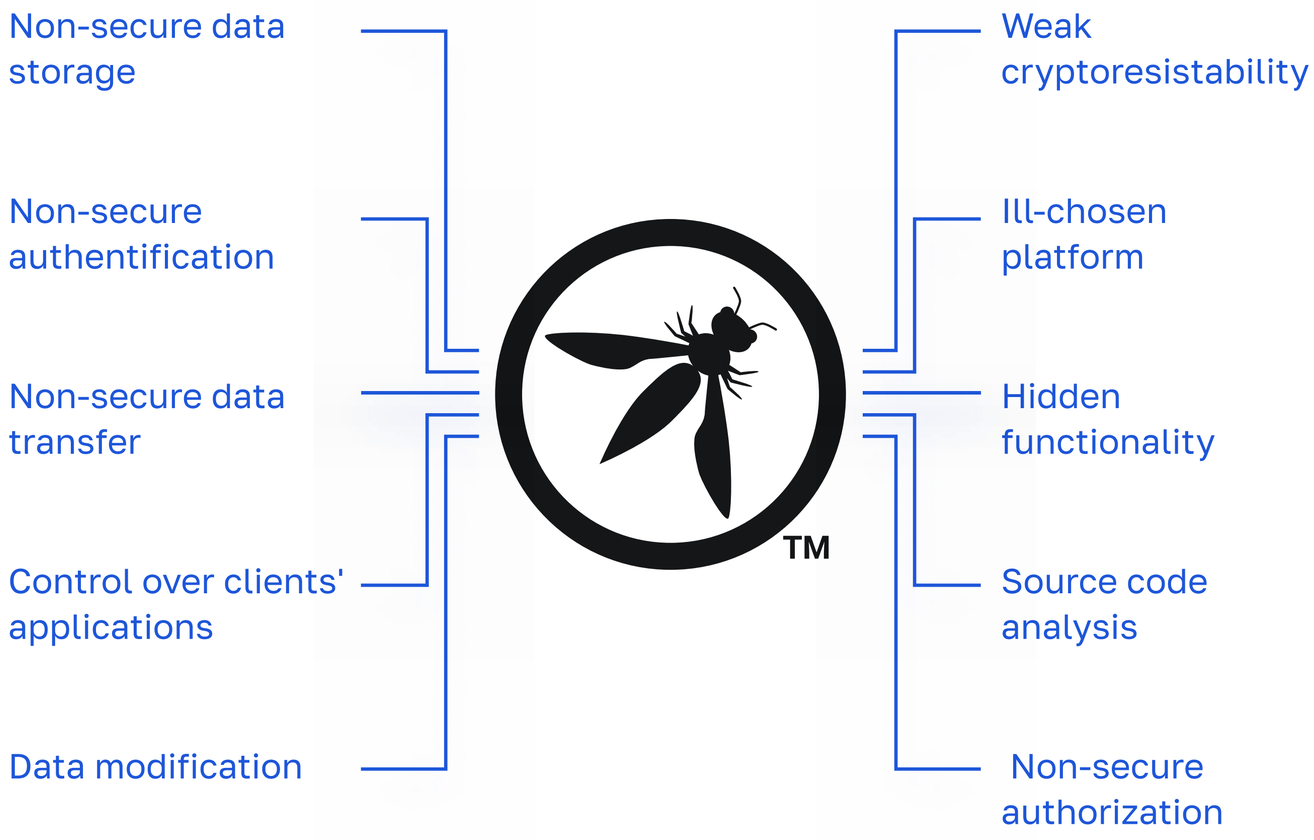
What we need from client to start?

- Initial information or servers accessible for tests
- Application in the exact shape in which it'll be placed into a store
- Source codes (if available)
- Paperwork (if available)
- Non-Obfuscated application

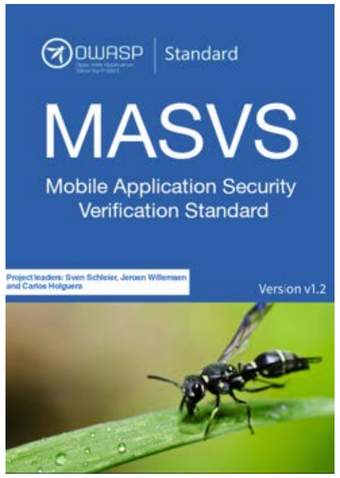


Main method we use

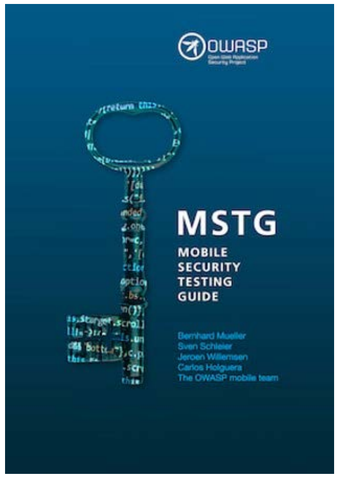
OWASP
MOBILE SECURITY
TOP 10



Additional standards and methods in use



Mobile App Security Verification Standards (MASVS)



Mobile Security testing Guide (MSTG)

Our own, experience-based and proven, Mobile Security Testing Checklist

Why us?

Professional cetrification

- Offensive Security Certified Professional (OSCP)
- Certified Ethical Hacker (CEH)
- Web Application Pentester (CWAP)
- eLearnSecurity Mobile Application Penetration Tester (eMAPT)

What your company gets at the end?

A detailed report on performed pentest, with security issues in a mobile application and related services pinpointed, and recommendations on fixing provided

- Comprehension of vulnerabilities in a mobile application
- Comprehension of necessary actions for vulnerabilities' elimination

TABLE 3 1 – CONSOLIDATED PENTEST RESULTS

№	Objective	Is the objective achieved?
1.	Discovered incorrect server and network hardware configurations	✓
2.	Discovered incorrect software configurations	✓
3.	Managed to attack Company customers	✓
4.	Gained access to protected information	−
5.	Managed to remotely execute commands	−
6.	Gained access to the internal network	−
	Overall protection level of the Company infrastructure's external perimeter	+

● Yes ● No ● Medium

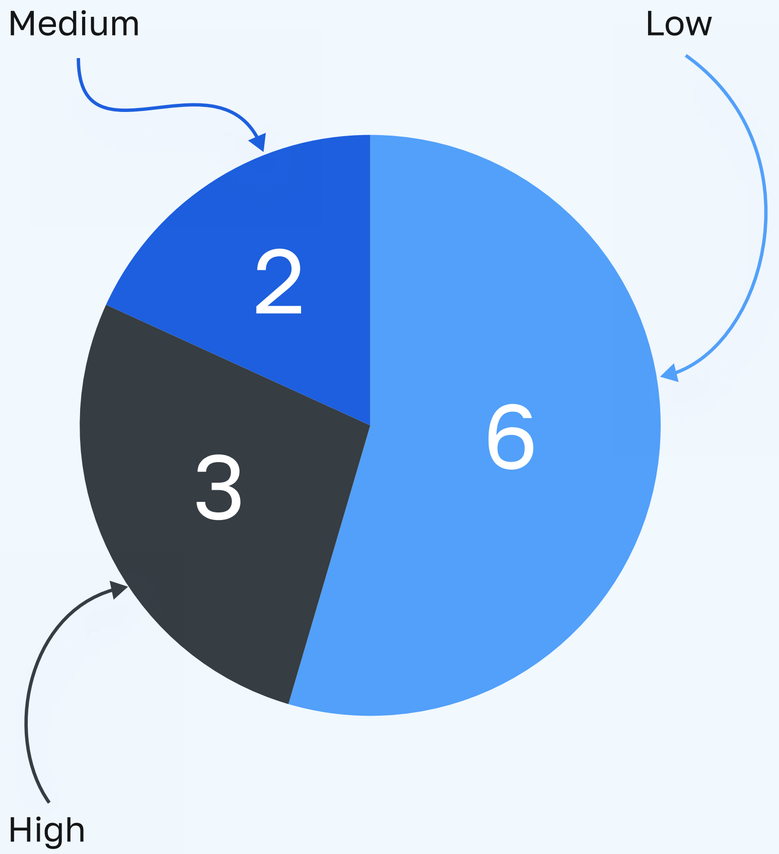
The penetration test revealed 11 vulnerabilities of various severity levels. Chart 3-1 shows the distribution of vulnerabilities by severity level.

WHAT YOUR COMPANY GETS AT THE END?

Summary

Distribution of vulnerabilities by severity level

CHART 3 1 – DISTRIBUTION
OF VULNERABILITIES BY SEVERITY LEVEL



Our clients


GAZPROM


открытие
Банк


QIWI
Кошелек


FINOM


Digital
Intelligence


CLARINS


Digital
Attitude
A Methodos Company


L'ORÉAL


MELON
FASHION GROUP


REDMOND


SOFTEQ


eyezon
LIVE VIDEO SHOPPING

What to do to start the security problem solving?

Questionnaire for penetration test service calculation

TEST DRIVE

Call us for a professional
open source FREE evaluation

PENTEST

Fill the questionnaire for pentest

Aleksandr Zubrikov
HEAD OF IT SECURITY

aleksandr.zubrikov@itglobal.com