PENETRATION TESTING

Executive *summary.*

DontBeHacked s. r. o. — accounting and payroll system. Testing period 1 – 7 April 2026.

CLIENT	PERIOD	TESTER	REPORT DATE
DontBeHacked s. r. o.	1 – 7 Apr 2026	Nabu technologies	8 April 2026

Critical exposure *identified.*

CRITICAL SEVERITY

During testing we identified a vulnerability that allows an attacker from the internet to obtain access to **payroll and personal data of all customers of the DontBeHacked system** — including national identification numbers, payslips and bank accounts. Exploitation requires only an ordinary trial account and freely available tooling.

In total we identified **7 security findings** — one critical, two high, two medium and two informational.

1	2	2	2
CRITICAL	**HIGH**	**MEDIUM**	**INFORMATIONAL**
Existential threat	Serious, recoverable damage	Significant exposure	Hygiene observations

What this means for *your company.*

The most severe finding concerns the way the DontBeHacked system verifies access to its application programming interface. An attacker can read data of all customers without any login credentials.

Personal data breach

Access to names, national identification numbers, addresses and bank accounts. Scope: **~ 85,000 employees** across all customers.

Payroll data breach

Complete payslips, salary components, contributions and tax records. GDPR Art. 9, Slovak Act No. 18/2018 Coll.

Regulatory consequences

Fine from the Slovak Office for Personal Data Protection of up to **4 % of annual turnover** under GDPR Art. 83. Mandatory notification of data subjects.

Reputational risk

DontBeHacked customers entrust the system with the most sensitive data of their employees. A public breach would equate to a loss of trust and customer churn.

List of identified *issues.*

Seven confirmed findings ranked by severity. Technical detail, reproduction steps and remediation recommendations are provided in a separate **technical report** intended for the development team.

F-01	CRITICAL	Unauthorised access to payroll data of all customers via API without authorisation	**CONFIRMED**
F-02	HIGH	Vulnerable library allowing remote code execution on the application server	**CONFIRMED**
F-03	HIGH	Cloud storage access keys embedded directly into the mobile application	**CONFIRMED**
F-04	MEDIUM	Administrative interface accessible from any IP address without network restriction	**CONFIRMED**
F-05	MEDIUM	Missing limit on the number of login attempts (rate limiting)	**CONFIRMED**
F-06	INFO	Outdated versions of supporting libraries with published patches, with no known exploit in the context of the application	OBSERVATION
F-07	INFO	Missing security HTTP headers on the web portal	OBSERVATION

Critical, high and medium severity findings are billable; informational observations are included in the report at no charge. Under the contract, billing is **exclusively for the most severe finding** — F-01.

Recommended *priorities.*

01

F-01 — Unauthorised access to API

Deploy authorisation checks on the payroll endpoints. Estimated effort: 1 – 2 working days.

WITHIN 48 HOURS

02

F-03 — Access keys in the mobile application

Rotate keys, replace with server-generated SAS tokens with limited validity. Review access logs for the past 90 days.

WITHIN 7 DAYS

03

F-02 — Vulnerable deserialisation

Change the JSON library configuration, or migrate to a secure alternative. Regression testing of the API.

NEXT RELEASE

04

F-04 and F-05 — Admin panel, rate limiting

Restrict the admin portal to the corporate VPN or an IP whitelist. Deploy rate limiting on the login endpoint (max 5 attempts / 15 min).

NEXT RELEASE

What was *tested.*

PARAMETER	VALUE
Assets	Web portal (**app.dontbehacked.sk**), REST API (**api.dontbehacked.sk**), Android mobile application (v 4.2.1), administrative portal (**admin.dontbehacked.sk**), 38 identified subdomains.
Methodology	OWASP Testing Guide v4.2, PTES and NIST SP 800-115. Three phases: automated scanning, static analysis and manual testing. Findings were validated by expert review before being recorded in the report.
Limitations	Does not cover the internal network, physical security, social engineering or third-party systems. No destructive testing — evidence was gathered via non-destructive reproduction paths.

06 • NEXT STEPS

Recommended *schedule.*

#	STEP	DEADLINE
1	Closing consultation with the technical team and leadership (1 hour, remote)	Within 5 working days
2	Remediation of critical finding F-01	Within 48 hours
3	Window for any objections to the severity of findings	14 calendar days
4	Free re-verification of remediation (max. 3× per finding)	Within 60 days

Scope and validity disclaimer. This report describes findings identified during penetration testing in the period 1 – 7 April 2026 on the assets defined in section 05. Testing is a point-in-time assessment — it reflects the state of the systems at the time of execution; subsequent changes may introduce new vulnerabilities. The methodology covers the most common classes of vulnerabilities but is not exhaustive; the absence of a finding does not imply the absence of a vulnerability. This report does not constitute certification of compliance with security standards. We recommend regular repetition of testing at least every 6 months or after significant changes to the system.