Sistematik

Penetration Testing Audit - Givearn

Start Date: 2023-08-03
End Date: 2023-09-08
Company: Sistematik OÜ
Website: https://sistematik.eu
Auditor: Reha Esen CEH, CISA

The following areas have been examined as part of the application security tests:

- Overview of the primary use scenarios.
- Manual analysis of the communication between the client (browser & mobile applications) and the back-end server, with an emphasis on OWASP Top 10.
- General security of the application server, such as vulnerability check of components.

The following issues have been excluded from the scope:

- DDoS (Distributed Denial of Service) tests and other types of load tests.
- Security assessment of the communication between the client browser and the 3rd party servers/APIs

Open Findings

Upon conclusion of the penetration assessment, all detected security vulnerabilities have been effectively addressed and validated. Currently, there are no open findings, underscoring the security posture of the Givearn mobile application.

Disclaimer

Although the tester has employed his best effort to this security test, by nature of security testing, no claim can be made to identify every security vulnerability. With this regard, this report is not an exhaustive list of all security weaknesses, but reflects the tester's expertise, experience, and risk perception.

Approval Date: 2023-09-08

Reha

(signature)

Reha Esen

	Risk Level	Typical Attributes	Explanation
MANDATORY	Urgent	**Most** Users Impacted **Low** Attack Complexity **No** Special Privileges Required **No** User Interaction Required	⚠ Data assets are either unguarded or can be compromised in mass, using publicly available tools/methods. Usual consequences are loss of confidentiality, integrity, or availability of all or most of the data, loss of system resources, such as critical source code or configuration information Access to source code, DB backup files, unauthenticated API interfaces, anonymous FTP services or OS access interfaces are typical examples.
	Critical	**Most/Some** Users Impacted **Medium/High** Attack Complexity **No/Some** Special Privileges Required **No** User Interaction Required	⛔ Data assets can either be fully compromised by highly qualified techniques or can only be partially compromised (such as attack vectors that target individual users) using publicly available tools/methods. XSS (Reflected, Stored and DOM- based), blind SQL injection, second-order SQL injection, SSRF, as well as other advanced attacks to gain unauthorized access to data, DB, APIs or OS can be the examples of this risk level.
	High	**Some** Users Impacted **No/Some** Special Privileges Required **Some** User Interaction Required	⚠ Vulnerabilities that have limited impact in terms of number of end-users, or cannot cause damage beyond limited data security issues, or a limited privilege escalation (less than administrative access) are considered as high risk. Additionally, vulnerabilities permitting escalation of privileges to administrative level, which can either be executed locally (by authorized individuals), or in combination with other attack techniques, are also considered here.
OPTIONAL	Medium	**Low/No** Direct Impact **No/Some** Special Privileges Required	ℹ Vulnerabilities that may not cause any direct form of data security issues, or attack types with a lower probability of harm for the data being processed/stored in the application, are categorized here. These vulnerabilities typically can be used for launching other attacks or may be used in combination with other attacks.
	Low	**No** Direct Impact	👉 This risk level is used for areas where the test subject is not well-aligned with the security best-practices.

Kill-Chain	☠ An attacker may combine multiple lower risk ("Optional") vulnerabilities and create a high-impact scenario. Such scenarios are marked with the "Kill-Chain" symbol and have a total risk level of "High", "Critical" or "Urgent".