itdesign

itdesign GmbH · Friedrichstraße 12 · 72072 Tübingen · Deutschland

Tübingen, February 7, 2020

Penetration Test 2019

Dear Reader,

We conducted our yearly penetration test in December 2019 with very convincing results. No major leaks were detected, and all other findings have been corrected.

Our penetration test partner for the test was CODE WHITE FINEST HACKING **, one of the leading PEN-test companies in Germany for thorough testing of applications and IT environments.**

They provided the following short statement regarding the test:

> *itdesign GmbH contracted an offensive cybersecurity company specialized in providing realistic attacker simulations to perform a holistic but non-exhaustive application penetration test against the Meisterplan web application. The main goal was to identify vulnerabilities that could harm the company, customers or even allow an anonymous attacker to breach perimeter into internal networks ranges of itdesign GmbH via the Internet.*
>
> *The test has been carried out from a black-box perspective, that is, neither source code nor other detailed information was given beforehand. At a later stage of the engagement, itdesign GmbH provided a set of API endpoints in order to facilitate the process of API endpoint enumeration.*
>
> *Ultimately it was not possible to compromise the overall security of the application under test or gain access to sensitive data within the time frame of 5 days allocated to the assessment.*

itdesign GmbH
Friedrichstraße 12
72072 Tübingen
Deutschland
Tel. +49 7071 3667-60
Fax +49 7071 3667-89
Web www.itdesign.de
E-Mail info@itdesign.de

Geschäftsführer
Christoph Adamczyk, Dr. Christoph Hirnle,
Johannes Koppenhöfer, Dr. Jörg Leute
Sitz der Gesellschaft
72072 Tübingen, Deutschland
Registergericht
Amtsgericht Stuttgart HRB 382021
USt.Id.Nr. DE203913579

Bankverbindungen
VR Bank Tübingen eG
IBAN DE39 6406 1854 0066 4020 00 · Swift-Code GENODES1STW
Commerzbank Tübingen
IBAN DE95 6414 0036 0890 0730 00 · Swift-Code COBADEFF641
Kreissparkasse Tübingen
IBAN DE47 6415 0020 0001 4665 19 · Swift-Code SOLADES1TUB

Nevertheless, some minor issues have been identified:
** the logon mechanism did not successfully prevent so called 'password-spraying' attacks which try to leverage the usage of weak passwords.*
** under certain circumstances the reporting functionality, which provided read access to a PostgreSQL database, might lead to a privilege escalation giving an attacker administrative rights to the affected Meisterplan instance.*

After reporting these findings, both issues have been successfully mitigated by itdesign GmbH in close cooperation with the testing provider.

The response time of technical as well as management staff was typically short. itdesign GmbH were friendly and open minded throughout the whole assessment including feedback sessions. Security related topics have been well understood and subsequently acted upon with a mature mindset.

The detailed report may be shared under a confidentiality agreement and upon request.

Sincerely,

Dr. Tobias Hüttner , CIO

itdesign GmbH
Friedrichstraße 12
72072 Tübingen
Deutschland
Tel. +49 7071 3667-60
Fax +49 7071 3667-89
Web www.itdesign.de
E-Mail info@itdesign.de

Geschäftsführer
Johannes Koppenhöfer, Dr. Jörg Leute
Sitz der Gesellschaft
72072 Tübingen, Deutschland
Registergericht
Amtsgericht Stuttgart HRB 382021
USt.Id.Nr. DE203913579

Bankverbindungen
Volksbank Tübingen
IBAN DE33 6419 0110 0066 4020 00 · Swift-Code GENODES1TUE
Commerzbank Tübingen
IBAN DE95 6414 0036 0890 0730 00 · Swift-Code COBADEFF641
Kreissparkasse Tübingen
IBAN DE47 6415 0020 0001 4665 19 · Swift-Code SOLADES1TUB