RADICALLY OPEN SECURITY

Executive Summary

TIMi SRL

V 1.1
Amsterdam, September 18th, 2023
Confidential

Document Properties

Client	TIMi SRL
Title	Executive Summary
Target	Azure Access PHP scripts
Version	1.1
Pentester	Marcus Bointon
Authors	Marcus Bointon, Stefan Vink
Reviewed by	Stefan Vink
Approved by	Melanie Rieback

Version control

Version	Date	Author	Description
0.1	September 6th, 2023	Marcus Bointon	Initial draft
0.2	September 12th, 2023	Stefan Vink	Review
1.0	September 12th, 2023	Marcus Bointon	1.0
1.1	September 18th, 2023	Marcus Bointon	Retest

Contact

For more information about this document and its contents please contact Radically Open Security B.V.

Name	Melanie Rieback
Address	Science Park 608 1098 XH Amsterdam The Netherlands
Phone	+31 (0)20 2621 255
Email	info@radicallyopensecurity.com

Table of Contents

1 Executive Summary

1.1 Introduction

Between September 6, 2023 and September 7, 2023, Radically Open Security B.V. carried out a first penetration test for TIMi SRL. Between September 15, 2023 and September 18, 2023, ROS carried out a retest (i.e. a second penetration test).

ROS performed a penetration test of three PHP scripts concerned with the management of Azure OAuth tokens with TIMi in order to assess the security of the scripts against SQL injection and other attacks. ROS analysed and ran the scripts and guide TIMi in attempting to find vulnerabilities, exploiting any such found to try and gain further access and elevated privileges.

1.2 Scope of work

The scope of the penetration test was limited to the following target:

- Azure Access PHP scripts (248 lines of PHP code before testing, 388 lines after adding many checks & re-code to improve security)

The scoped services are broken down as follows:

- Code audit: 0.5 days
- Reporting: 0.5 days
- Retest: 0.5 days
- Retest reporting: 0.5 days
- PM/Review: 0.5 days
- **Total effort: 2.5 days**

1.3 Timeline

The security audit took place between September 6, 2023 and September 7, 2023. The retest took place between September 15, 2023 and September 18, 2023.

2 Conclusion

During the first crystal-box penetration test we found 6 issues (no high severity findings were found).These findings have been shared and explained in a full report with the team at TIMi.

After TIMi had made amendments to the code following our recommendations, ROS conducted a retest (i.e. a second penetration test) to check that the mitigations were effective, and have not introduced new vulnerabilities.

We found that all the issues that we reported have been addressed appropriately, except one. The remaining issue is a low severity finding: it's that the SQLite database is not encrypted. **This is not itself a vulnerability**, because the database is now well-protected, but more a part of a defence in depth, should other measures fail. Consequently, **we consider the code to be sufficiently robust and free of vulnerabilities that would represent a significant threat** when using the scripts in the authentication operations for which they are intended.

There is still room for improvement in code quality and reliability, but we hope that our advice and recommendations will help raise awareness of security during development. Finally, we want to emphasize that security is a process – this audit is just a one-time snapshot. Security posture must be continuously evaluated and improved. Regular audits and ongoing improvements are essential in order to maintain control of your corporate information security. We hope that the pentest report (and the detailed explanations of our findings) will contribute meaningfully towards that end.

3 Future Work Recommendations

- **Regular security assessments**

  Security is an ongoing process and not a product, so we advise undertaking regular security assessments and penetration tests, ideally prior to every major release or every quarter.

- **Overhaul development environment and processes**

  We estimate that the coding conventions and coding styles can be improved. We advise TIMi to make better use of modern PHP features and tools to improve code quality, security, and reliability throughout the application.

4 About Us

Radically Open Security B.V. is the world's first not-for-profit computer security consultancy. We operate under an innovative new business model whereby we use a Dutch fiscal entity, called a “Fiscaal Fondswervende Instelling” (Fiscal Fund raising Institution), as a commercial front-end to send 90% of our profits, tax-free, to a not-for-profit foundation, Stichting NL net. The NLnet Foundation has supported open-source, digital rights, and Internet research for almost 20 years.

In contrast to other organizations, our profits do not benefit shareholders, investors, or founders. Our profits benefit society. As an organization without a profit-motive, we recruit top-name, ethical security experts and find like-minded customers that want to use their IT security budget as a "vote" to support socially responsible entrepreneurship. The rapid pace of our current growth reflects the positive response the market has to our idealistic philosophy and innovative business model.

Radically Open Security B.V. has a number of values that we describe as our “Core Principles.” These are:

- **No sketchy stuff**
  We don't build surveillance systems, hack activists, sell exploits to intelligence agencies, or anything of the sort. If a job is even remotely morally questionable, we simply won't do it.
- **Open-Source**
  Releasing ALL tools and frameworks we build as open source on GitHub (a link to our GitHub page can be found on our website).
- **Teach to fish**
  During engagements, we will not only share our results with your company, but also provide a step-by-step description of how to perform the same audit or procedure without us. We want to demystify what we're doing. It's not rocket science, and we genuinely want to help your company improve its security posture, even if it costs us repeat business.
- **IoCs for free**
  Releasing ALL collected threat intelligence (Indicators of Compromise) into an open-source database that everyone can freely use. (Sanitized in agreement with customers.)
- **Zero days**
  We don't sell zero-days - we responsibly disclose them!

For more information about Radically Open Security B.V., we refer you to our website: www.radicallyopensecurity.com.

5 Disclaimer

It is important to understand the limits of ROS's services. ROS does not (and cannot) give guarantees that something is secure. ROS, instead, has an obligation to make reasonable efforts (in Dutch: "*inspanningsverplichting*") to perform the agreed services.

Appendix 1 Testing team

Marcus Bointon	Marcus has a BSc in Computer Science and Digital Electronics from King's College London, and an MSc in interactive computer system design from Loughborough University of Technology. He maintains PHPMailer (a top-10 PHP project on GitHub), is a regular contributor to innumerable open-source projects, and he wrote the HTML5 specification for email addresses. He's the chief architect of the smartmessages.net email marketing system, lead developer for clubzero.co, and has worked with ROS since 2016, mainly as a technical writer & editor. You'll often find Marcus speaking at developer conferences on web development, email, devops, privacy, data protection, and security.
Melanie Rieback	Melanie Rieback is a former Asst. Prof. of Computer Science from the VU, who is also the co-founder/CEO of Radically Open Security.