Curriculum Vitae of Dr.-Ing. Mario Heiderich

Contact Data

Address	Bielefelder Str. 14 10709 Berlin
Date of Birth	8th of July, 1981
Born in	Marburg a. d. Lahn
Nationality	German
E-Mail	mario@cure53.de

Education and Civilian Service

2000	University Admission, Christian Rauch Schule, Bad Arolsen.
2000–2001	Civilian Service Deutsches Rotes Kreuz, Wolfhagen.

Academic Experience

2001–2005	Academic Studies and *Graduate Engineer in Media Informatics*, University of Applied Sciences, Friedberg.
2010–2012	PhD Candidate at Prof. Dr. Jörg Schwenk, Chair for Network and Data Security, Ruhr-University Bochum, Germany.
June 2012	Successfully completed PhD studies at the Chair for Network and Data Security, Ruhr-University Bochum, Germany.
since Jun 2012	Post-Doc at the Chair for Network and Data Security, Ruhr-University Bochum, Germany.

Professional Experience

2004	University Intern, Editworks GmbH, Marburg a. d. Lahn.
2005–2007	Developer, DocCheck Medical Services GmbH, Cologne.
2007–2009	Security Developer, Ormigo GmbH, Cologne.
2009–2011	Technical Lead / CTO, Business In Inc., New York, USA / Cologne.
2011–2014	Security Researcher, Microsoft, Redmond, USA.
2011–2019	Security Researcher, Chair for Network and Data Security, Ruhr-University Bochum.
2011–2019	Penetrationtester, Deutsche Post AG, Bonn / Berlin.
since Jun. 2007	Founder and Director Cure53, Penetration Testing Firm, Berlin.

since Jan. 2019 External Lecturer, Chair for Network and Data Security, Ruhr-University Bochum.

Academic Publications

1. DOMPurify: Client-Side Protection Against XSS and Markup Injection, Heiderich, Mario and Späth, Christopher and Schwenk, Jörg, European Symposium on Research in Computer Security, 2017

2. How Private is Your Private Cloud
? – Security Analysis of Cloud Control Interfaces, Dennis Felsch, Mario Heiderich, Frederic Schulz, Jörg Schwenk - ACM CCSW 2015 in conjunction with the ACM Conference on Computer and Communications Security (CCS) October 16, 2015, The Denver Marriot City Center, Denver, Colorado, USA.

3. Waiting for CSP – Securing Legacy Web Applications with JSAgents, Mario Heiderich, Marcus Niemietz, Jörg Schwenk - Waiting for CSP — Securing Legacy Web Applications with JSAgents, ESORICS 2015, 20th European Symposium on Research in Computer Security

4. Scriptless Timing Attacks on Web Browser Privacy, Bin Liang, Wei You, Liangkun Liu, Wenchang Shi, Mario Heiderich - 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks

5. Scriptless attacks: Stealing more pie without touching the sill, Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, Jörg Schwenk - Journal of Computer Security, Volume 22, Number 4 / 2014, Web Application Security - Web @ 25

6. mXSS Attacks – Attacking well-secured Web-Applications by using innerHTML Mutations, Mario Heiderich, Jörg Schwenk, Tilman Frosch, Jonas Magazinius, Edward Z. Yang - 20th ACM Conference on Computer and Communications Security (CCS), Berlin, Germany, November 2013

7. SS-FP: Browser Fingerprinting using HTML Parser Quirks, Erwan Abgrall, Yves Le Traon, Martin Monperrus, Sylvain Gombault, Mario Heiderich, Alain Ribault

8. Scriptless Attacks – Stealing the Pie Without Touching the Sill, Mario Heiderich, Marcus Niemietz, Felix Schuster, Thorsten Holz, Jörg Schwenk - 19th ACM Conference on Computer and Communications Security (CCS), Raleigh, NC, October 2012

9. On the Fragility and Limitations of Current Browser-provided Clickjacking Protection Schemes, Sebastian Lekies, Mario Heiderich, Dennis Appelt, Thorsten Holz, Martin Johns - 6th USENIX Workshop on Offensive Technologies (WOOT), Bellevue, WA, August 2012

10. Crouching Tiger – Hidden Payload: Security Risks of Scalable Vectors Graphics, Mario Heiderich, Tilman Frosch, Meiko Jensen, Thorsten Holz - 18th ACM Conference on Computer and Communications Security (CCS), October 2011

11. All Your Clouds are Belong to us – Security Analysis of Cloud Management Interfaces, Juraj Somorovsky, Mario Heiderich, Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono - 18th ACM Cloud Computing Security Workshop (CCSW), October 2011

12. IceShield: Detection and Mitigation of Malicious Websites with a Frozen DOM, Mario Heiderich, Tilman Frosch, Thorsten Holz - 14th International Symposium on Recent Advances in Intrusion Detection (RAID), September 2011

13. The Bug that made me President – A Browser- and Web-Security Case Study on Helios Voting, Mario Heiderich, Tilman Frosch, Marcus Niemietz, Jörg Schwenk - 3rd International Conference on E-Voting and Identity (VoteID 2011), September 2011

Conference Talks

1. Keynote: An Infosec Timeline: Noteworthy Events From 1970 To 2050, OWASP AppSec 2010, Amsterdam, Netherlands

2. Keynote: How To Build Your Own Infosec Company, BSides 2018, Lisbon, Portugal

3. Keynote: XSS is Dead - We just don't get it, OWASP AppSec 2018, London, United Kingdom

4. My Sweet Innocence Exposed - Eleven Reasons why we will all miss you, "E", WarCon 2016, Warsaw, Poland

5. ToStaticHTML for Everyone! About DOMPurify, Security in the DOM, and Why We Really Need Both, USENIX Enigma 2016, San Francisco, USA

6. An Abusive Relationship with AngularJS – About the Security Adventures with the "Super-Hero" Framework, CodeBlue 2015, Tokyo, Japan

7. Copy & Pest – A case-study on the clipboard, blind trust and invisible cross-application XSS, OWASP AppSec EU 2015, Amsterdam, Netherlands

8. ECMAScript 6 from an Attacker's Perspective – Breaking Frameworks, Sandboxes, and everything else, nullcon 2015, Goa, India

9. In the DOM, no one can hear your scream, Mario Heiderich, border:none, Nuremberg, Germany / EnterJS, Cologne, Germany

10. JSMVCOMFG – To sternly look at JavaScript MVC and Templating Frameworks, Mario Heiderich, ZeroNights, Moscow, Russia / Bluehat 2013, Seattle, USA

11. The innerHTML Apocalypse – How mXSS attacks change everything we believed to know so far, Mario Heiderich, SyScan'13, Singapore
12. Got Your Nose – How Attackers steal your precious Files without using JavaScript, Mario Heiderich, HackInParis 2012, Paris, France
13. The Image that called me – Active Content Injection with SVG Files, Mario Heiderich, Bluehat 2011, Seattle, USA
14. Locking the Throne Room 2.0 – How ES5+ will change XSS and Client Side Security, Mario Heiderich, Bluehat 2011, Seattle, USA
15. Locking the Throne Room – ECMA Script 5, a frozen DOM and the eradication of XSS, Mario Heiderich, Hack In Paris 2011, Paris, France
16. Dev and Blind – Attacking the Weakest Link in IT Security, Mario Heiderich, Johannes Hofmann, CONFidence 2010 2.0, Prague, Czech Republic
17. The Presence and Future of Web Attacks – Multi-Layer Attacks and XSSQLI, Mario Heiderich, CONFidence 2010, Krakow, Poland
18. JavaScript from Hell – Advanced Client Side Injection Techniques of Tomorrow, Mario Heiderich, OWASP AppSec Germany 2009 Conference, Nuremberg, Germany
19. The Ultimate IDS Smackdown – How red vs. blue situations can influence more than one might assume, Mario Heiderich, Gareth Heyes, OWASP Chapter Meeting 2009, London, UK
20. I thought you were my friend – Malicious markup, browser issues and other obscurities, Mario Heiderich, CONFidence 2009, Krakow, Poland
21. PHPIDS – Monitoring Attack Surface Activity, Mario Heiderich, OWASP AppSec Europe 2008, Ghent, Belgium

Projects and Work

- Penetration-Testing for various international companies and organizations
- Penetration-Testing Team-Lead for 500+ Projects
- Further references can be requested by contacting mario@cure53.de

Further Activities

- Organizer of HackPra AllStars Conference in Hamburg, Germany, 2013, Amsterdam, Netherlands, 2015, Belfast, UK, 2017, Amsterdam, Netherlands, 2019

- Founder and Maintainer of the DOMPurify Project, https://github.com/cure53/DOMPurify
- Founder and Maintainer of the HTML5 Security Cheatsheet, https://html5sec.org/, https://github.com/cure53/H5SC
- Founder and Maintainer of the HTTP Leaks Project, https://github.com/cure53/HTTPLeaks
- Invited Speaker on international Conferences (CONFidence 2009, 2010, 2011, 2012; Hack In Paris 2011, 2012, 2013, 2014; SyScan'13; OWASP AppSec Research 2010, 2011, 2012, 2013; Microsoft Bluehat 2011, 2012, 2013; ZeroNights Moscow 2013; Insomni'Hack 2013, 2014; WASR Workshop 2013; various other conferences)
- Organizer HackPra University Lecture (2011, 2012, 2013) and HackPra Allstars Conference Track, Hamburg, Germany, August 2013
- Technical Advisor for Tangled Web, Deutsche Ausgabe, 2013
- Program Committee Member USENIX WOOT'12, '13 and '14, OWASP Germany, GreHack 2013
- Jury Member E-POSTBRIEF Security Cup, 2013
- Invited Participant Dagstuhl Seminar 12401, Web Application Security, Oct. 2012
- Co-Chair on international Web Application Security Summits (OWASP Summit, 2011, Portugal)
- Captain of Team RUB - Winner of the E-POSTBRIEF Security Cup, 2010
- Published Author (Sichere Webanwendungen: Das Praxisbuch, Galileo Press, 2008; Web Application Obfuscation, Syngress, 2010)
- Co-founder and Former Lead Developer PHPIDS, https://phpids.org/
- General Handsomeness and good hair (independently rated above average)