TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Advanced Pwning & Fixing of Node.js & Electron apps, shells, injections and fun!

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: TR20_HMTS and save an additional 5% of the current valid rate of any package!

Overview

This course is the culmination of years of experience gained via practical penetration testing of JavaScript applications as well as countless hours spent doing research. We have structured this course around the OWASP Security Testing Guide and relevant items of the OWASP Application Security Verification Standard (ASVS), so this course covers and goes beyond the OWASP Top Ten, the course additionally includes specific attack vectors against Electron and Node.js apps. This course provides participants with actionable skills that can be applied immediately from day 1.

Please note our courses are 90% hands-on, we do not lecture students with boring bullet points and theories, instead we give you practical challenges and help you solve them, teaching you how to troubleshoot common issues and get the most out of this training. As we try to keep both new and advanced students happy, the course is very comprehensive and we have not met any student able to complete all challenges during the class, therefore training continues after the course through our frequently updated training portal, for which you keep lifetime access, as well as unlimited email support.

ERNW Insight GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
BIC: GENODE61HD3

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
Ust-ID DE 304 445 827
IBAN: DE84 6729 0100 0067 1236 03

Managing Director:
Kerstin Schröter

Each day starts with a brief introduction to the JavaScript platform (i.e. Node.js, Electron) for that day and then continues with a look at static analysis, moves on to dynamic checks finishing off with a nice CTF session to test the skills gained.

Day 1: Focused specifically on Node.js. We start with understanding the platform and then deep dive into static and dynamic analysis of the applications at hand. This day is packed with hands on exercises and CTF-style challenges.

Day 2: Focused on Electron: We start with understanding Electron and various security considerations. We then focus on static and dynamic analysis of the applications at hand. The day is filled with hands on exercises ending with a CTF for more practical fun.

Prerequisites

This course has no prerequisites as it is designed to accommodate students with different skills:

- Advanced students will enjoy comprehensive labs, extra miles and CTF challenges.
- Less experienced students complete what they can during the class and can continue at their own pace from home using the training portal.

This said, the more you learn about the following ahead of the course, the more you will get out of the course:

- Linux command line basics;
- Node.js basics;
- Electron basics.

Requirements

A laptop with the following specifications:

- Ability to connect to wireless and wired networks;
- Ability to read PDF files ;
- Administrative rights: USB allowed, the ability to deactivate AV, firewall, install tools;
- Knowledge of the BIOS password, in case VT is disabled;
- Minimum 8GB of RAM (recommended: 16GB+);
- 60GB+ of free disk space (to copy a lab VM and other goodies);
- VirtualBox 6.0 or greater, including the “VirtualBox Extension Pack”.

Attendees will be provided with:

- **Lifetime access** to training portal with all course materials;
- **Unlimited access** to future updates and step-by-step **video recordings**;
- **Unlimited email support**, if you need help while you practice at home later;
- Interesting vulnerable apps to practice;
- Digital copies of all training material;
- Custom Build Lab VMs;
- Purpose Build Vulnerable Test apps;
- Source code for test apps.

Who should attend this training?

This course is for beginners, intermediate and advanced level students. While beginners are introduced to the nuances of Node.js and Electron app security from scratch, intermediate and advanced level learners get to perfect both their knowledge and skills on the subject. Extra mile challenges are available in every module to help more advanced students polish their skills. The course is crafted in a way that regardless of your skill level you will significantly improve your JavaScript security skills.

- If you are new and cannot complete the labs during the class, that is OK, as you keep training portal access, you will learn a lot in the class but can continue from home with the training portal.
- If you are more advanced in JavaScript security you can try to complete the labs in full and then take the CTF challenges we have for each day, you will likely also attempt to complete some exercises from home later.

About the Trainers:

Anirudh Anand is a security researcher with a primary focus on Web and Mobile Application Security. He is currently working as a Senior Security Engineer at CRED and also Security Trainer at 7asecurity. He has been submitting bugs and contributing to security tools for over 7 years. In his free time, he participates in CTF competitions along with team bi0s (#1 security team in India according to CTF time). His bounties involve vulnerabilities in Google, Microsoft, LinkedIn, Zendesk, Sendgrid, Gitlab, Gratipay and Flipboard.
Anirudh also has contributed to several OWASP projects with notable contributions being in OWTF and Hackademic Challenges Project. He has presented/trained in a multitude of conferences including c0c0n 2019, BlackHat Arsenal 2019, BlackHat Europe Arsenal 2018, HITB Dubai 2018, Offzone Moscow 2018, Ground Zero Summit Delhi 2015 and Xorconf 2015.

Abraham Aranguren is the CEO of 7ASecurity, a company specializing in penetration testing of web/mobile apps, infrastructure, code reviews and training. Former senior penetration tester / team lead at Cure53 and Version 1. Creator of “Practical Web Defense” - a hands-on eLearn Security attack / defense course, OWASP OWTF project leader, an OWASP flagship project, Major degree and Diploma in Computer Science, some certs: CISSP, OSCP, GWEB, OSWP, CPTS, CEH, MCSE:Security, MCSA:Security, Security+. As a shell scripting fan trained by unix dinosaurs, Abraham wears a proud manly beard. He writes on Twitter as @7asecurity @7a_ @owtfp or Blog. Multiple presentations, pentest reports and recordings can be found on Publications.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR20_HMTS
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hmtrainingsolutions.com
+49 6022 5089999 / www.hmtrainingsolutions.com