Following the success of NotSoSecure’s Black Hat with Basic Infrastructure, Basic Web and Advanced Infrastructure Hacking, we have proudly brought out this very Advanced Web Hacking training written and delivered by NotSoSecure Group and world-famous Mario Heiderich. Available for private groups onsite, we have brought the very best of our combined expertise together to challenge our respective clients and to push the boundaries of knowledge further in our industry.

This fast-paced class, gives attendees an insight into advanced AppSec topics. Broken down into 3 days of Server Side Flaws and 2 days of Client Side Flaws, the team has built a state of the art hacklab and recreated security vulnerabilities based on real life Pen Tests and real bug bounties seen in the wild. Written with and delivered by NotSoSecure Group in association with Mario Heiderich: Mario, a “security researcher” is from Berlin; leads the small yet exquisite pen-test company called Cure53 and pesters peaceful attendees on various 5th tier conferences with his hastily assembled powerpoint-slides...

**Advanced Web Hacking** – Black Belt Edition, is available for private groups. Delivered as on-site training around the world particularly in the UK, EU and USA for numbers up to 16 students. A list of on-site pre-requisites is available upon request.

Server Side flaws (3 days)
These vulnerabilities affected well-known software/websites and span across multiple technologies (e.g., .NET framework to Node.js applications). The vulnerabilities selected for the class either typically go undetected by modern scanners or the exploitation techniques are not so well known.

**SQL Injection**
- 2nd order injection
- NoSQL injection
- Out-of-Band exploitation
- WAF bypass techniques

**XXE Injection**
- Blind XXE injection
- Case Study of recent XXE bugs
- XXE to Code Execution

**Serialization Flaws**
- PHP object injection
- Java serialisation flaws
- Case study of recent serialisation flaws

**HTTP Parameter Pollution (HPP)**
- Detecting HPP in application
- Case study of recent HPP bugs

**Business Logic Flaws**
- Mass Assignment bugs
- OS code injection
- Crypto attacks

Client Side Flaws - Exploiting Websites using offensive HTML, SVG, CSS, and other Browser-Evil (2 days)
The focus of this aspect of the training is on the offensive and dangerous parts of HTML, JSON and related technologies, the nasty and undocumented stuff, dozens of new attack techniques brought to the laboratory of horrors of those maintaining the HTML5 Security Cheat Sheet. We will learn how to attack any web-application with either unknown legacy features or the half-baked results coming to your browser from the labs of W3C, WHATWG and the ES6 mailing lists. Whether you want to attack modern web applications or shiny browser extensions and Chrome Packaged Apps - we have that covered.

A bit of knowledge on HTML and JavaScript is required here, but rookies and rocket scientists will be satisfied equally. HTML is a living standard. And so is this class. Course material will be provided on-site and via access to a private Github repo so all attendees will receive updated material even months after the actual training.

Starting with;
- Client Side Flaws: The very Basics
- HTTP / Encoding
- Character Sets
- CSRF and detail
- Cross Site-Scripting
- DOM Clobbering
- Drag&Drop / Copy&Paste
- DOMXSS

Moving on to;
- HTML5 Attacks & Vectors
- SVG
- XML
- Mutation XSS / mXSS
- Scriptless Attacks
- SOP Bypasses
- Filter Bypasses
- Optimizing your Payload

Note: Whoever works with or against the security of modern web applications will enjoy and benefit from this class. This is not a beginner class and attendees are expected to have a good prior understanding of the OWASP top 10 issues to gain maximum value from the class. Further to this, the class does not cover all AppSec topics and focuses only on advanced identification and exploitation techniques of the vulnerabilities shown on the right.