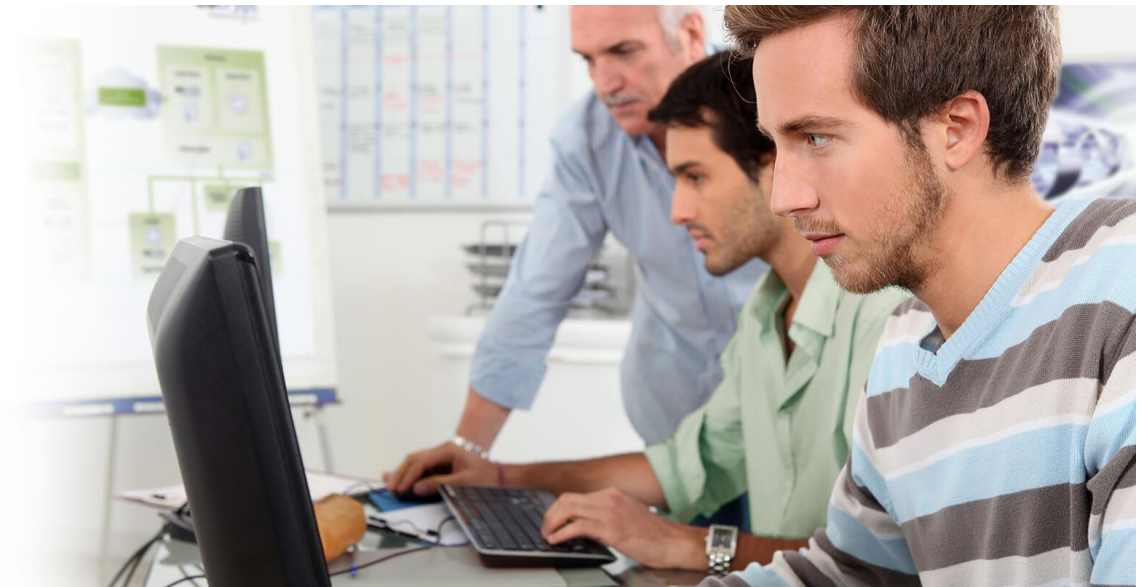
Web Hacking

Date	①July 3rd (Tue) - 4th (Wed) 9:00~17:00 ②July 5th (Thu) - 6th (Fri) 9:00~17:00
Venue	UDX CONFERENCE 6F (Akihabara)
Organizer	NANO OPT Media, Inc



Web Hacking

OVERVIEW

This is an entry-level web Application Security-testing class and is a recommended pre-requisite for our Advanced Web Hacking class. This class familiarises the attendees with the basics of Web and Application hacking. A number of tools and techniques will be taught during the 2 day class. If you would like to step into the world of ethical hacking / pen testing with a focus on web applications, then this is the right class for you.

-Class Details

This class familiarises the attendees with a wealth of tools and techniques needed to breach the security of web applications. The class starts from the very basic, and gradually builds up to a level where attendees can not only use the tools and techniques to hack various components involved in Web Application hacking, but also walk away with a solid understanding of the concepts on which these tools are based. The class also covers the industry standards such as OWASP Top 10, PCI DSS and contains numerous real life examples to help the attendees understand the true impact of these vulnerabilities.

Day 1

Information Gathering, Profiling and Cross-Site Scripting

- Understanding HTTP Protocol
- Identifying the Attack Surface
- Username Enumeration
- Information Disclosure
- Issues with SSL/TLS
- Cross-Site Scripting
- Cross-Site Request Forgery

Day 2

Injection, Flaws, Files and Hacks

- SQL Injection
- XXE Attacks
- OS Code Injection
- Local/Remote File Include
- Cryptographic Weakness
- Business Logic Flaws
- Insecure File Uploads

WHO SHOULD TAKE THIS COURSE

- System Administrators
- Web Developers
- SOC analysts
- Penetration Testers
- network engineers
- security enthusiasts
- anyone who wants to take their skills to the next level.

WHAT STUDENTS WILL BE PROVIDED WITH

・Access to a hacking lab not just during the course but for 30 days after the class too. This gives them plenty of time to practice the concepts taught in the class.

・Numerous scripts and tools will also be provided during the training, along with student hand-outs.

・A certificate of attendance

TRAINER

Sam Sanoop

Security Consultant

Conferences

BSides London
Steelcon,
MWRIcon

Open-Source Projects

DVWS

Damn Vulnerable Web Services is a vulnerable web application written in PHP that can be used to learn real world web service vulnerabilities.

Background

Sam is an information security enthusiast with interest in web application security. Sam holds a Bachelor of Science (BSc) degree in Computer Security with Forensics from Sheffield Hallam University, and international certifications such as Offensive Security Certified Professional (OSCP) and CREST Registered Penetration Tester (CRT).
Sam used to regularly partake in bug bounty programs as a student and has reported multiple vulnerabilities through HackerOne as well as directly to companies such as Magix, Checkpoint, OLX and Bosch. After graduating, he has worked with various well know security companies in United Kingdom including CQrity and MWR InfoSecurity before joining NotSoSecure as a Security Consultant. Sam has a well-rounded skill set, although he prefers to tackle challenges associated with web application security. His current research is focused on web application front-end framework security.

What he does for NotSoSecure

Sam works as a Security Consultant and delivers a multitude of security assessments covering web application security, code reviews and network security. Within NotSoSecure's team of Information Security specialists, he works primarily on web application security projects and is one of the trainer for NotSoSecure's Basic Web Hacking training course. Sam undertakes a variety of security-consulting services including penetration testing applications and infrastructure to clients within a variety of industries while working closely with them, establishing fruitful professional relationships.

Prices *Including 2days lunch

1st Early bird discount : JPY 195,000 Deadline :May 25th, 2018

2nd Early bird discount : JPY 235,000 Deadline :June 22th, 2018

Regular : JPY 275,000 (All prices are not including tax)

WHAT STUDENTS SHOULD BRING

The only requirement for this class is that you must bring your own laptop and have admin/root access on it.

During the class, we will give you VPN access to our state-of-art hacklab which is hosted in our datacenter in UK. Once you are connected to the lab, you will find all the relevant tools/VMs there.

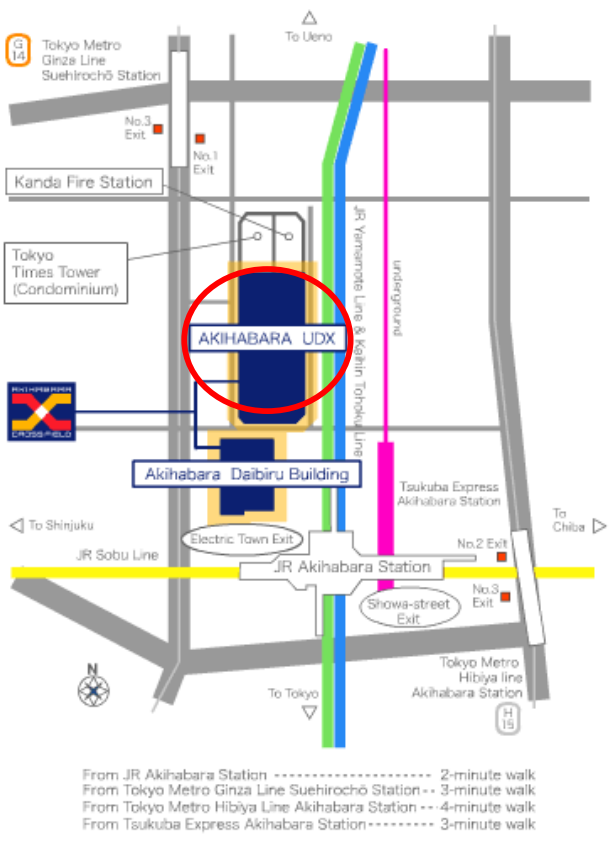
We also provide a dedicated Kali VM to each attendee on the hacklab. So, you don't need to bring any VMs with you. All you need is admin access to install the VPN client and once connected, you are good to go!

STUDENT REQUIREMENTS

Bring your own laptop and have admin/root access on it.

Also, note that we will use an wireless network for this class.

ACCESS



Inquiry
CSET Show Management Office
(NANO OPT Media,Inc.)
TEL : +81-3-6258-0590
FAX : +81-3-6258-0598
Email: contact@f2ff.jp