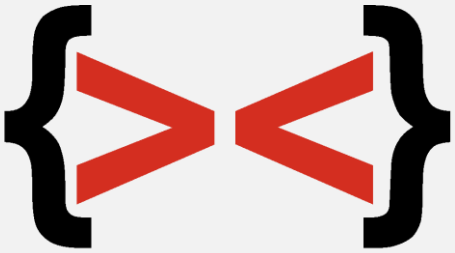
2018



Xcode Intensif Training

Advanced ethical web hacking & security

XCODE

Advanced Ethical Web hacking & security

Pembelajaran teknik-teknik web hacking secara ethical dan keamanannya secara advanced

Waktu Training: 5 hari

Objectives : Dengan Menyelesaikan training ini diharapkan peserta bisa melakukan teknik-teknik web hacking dan pengamanannya secara advanced

XCODE

Advanced Ethical web hacking & Security

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	- Ethical Hacking - Pengenalan web dan database (HTML, PHP, MySQL) - Form, action, metode post, input type text dan submit, koneksi database, mysqli_connect, mysqli_query, pengkondisian & mysql_num_rows, create database, use, create table, insert, select, alter, update, drop dan dasar managemen user pada MySQL. - Dasar Kriptopgrafi - Mengenal encode / decode (base64), disertai prakteknya dengan python - Mengenal salah satu enkripsi & dekripsinya pada kriptografi simetris, disertai prakteknya dengan python - Mengenal enkripsi & dekripsinya pada kriptografi asimetris (public key & private key), disertai prakteknya dengan python - Mengenal fungsi hash disertai prakteknya untuk membangun hashnya dengan python dan cara crack nya dengan menggunakan wordlist - Mengenal web hacking - Reverse domain - Google hacking

		- Google hacking dengan cepat (Menampilkan semua yang dicari dalam 1 halaman dan tidak terkena captcha google) - Dirbuster - Dirhunt - CMS Scan - Scanning Sub domain - Mendeteksi jenis hash secara otomatis dan contoh melakukan cracking dari situs-situs cracking hash - Mendeteksi Web Application Firewall pada website - Scanning IP, port, service, OS dll - Dasar hacking (Web Server) - Denial of Server web server - Denial of Service ip public - Teknik untuk meminimalisir serangan ke server dan pengamanannya secara umum - Salah satu pengamanan dari DoS pada web server
2	Session 2	- Eksploitasi heartbleed - Buffer Overflow - Fuzzing http (head/put/get/post) - EIP - Pattern create & pattern offset

		- Menghindari proteksi pada module - JMP ESP - Proof of concept pada exploit - Mengenal POST dan GET - Memahami Get Method & post method - Cross-site scripting (XSS) - Pengamanan XSS dari sisi pemrograman - Scanning XSS - di linux dan windows - Eksploitasi XSS non persistent untuk remote target melalui client side attack (browser ~ metasploit framework) - Variasi teknik-teknik injeksi pada target dengan celah XSS - Eksploitasi XSS persistent untuk menggunakan account target tanpa password login (Mengambil cookie dari target), masukkan ke browser lalu akses account target - Bypass filter upload image dengan tamper data - Pengamanan upload dengan .htaccess - Variasi teknik-teknik bypass filter upload
	Session 3	- Cross-Site Request Forgery (CSRF) - Local File Inclusion - LFI untuk mendapatkan akses PHPMyadmin pada kasus celah pada plugin wordpress

		- LFI untuk mendapatkan username pada linux - Contoh pengamanan LFI dari sisi programming - Contoh pengamanan LFI dari sisi konfigurasi PHP.INI - Variasi teknik-teknik injeksi pada target dengan celah LFI - WPScan - WPScan for brute force (Advanced) ~ Username Enumeration + crack password (Wordlist) - Admin login scanner - Scanning SQL Injection - di Linux dan Windows - Remote File Inclusion - Scanning RFI - di linux dan windows - PHP Shell Development (Membuat PHP Shell sendiri dari awal untuk RFI) - Remote shell target dengan celah RFI - Bind Shell & Reverse shell - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi pemrograman - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi konfigurasi PHP.INI - Command Injection dan teknik-teknik variasinya
	Session 4	- SQL Injection union - BLIND SQL Injection

		- TIME BASED SQL Injection - SQL Injection untuk BYPASS WAF (ADVANCED) - Contoh pengamanan SQL Injection dari sisi pemrograman - SQL Injection - bypass login wp - PHP upload & logger Login - Havij di Windows - SQLMAP di Linux - SQL Injection pada web halaman login - Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (pengecekan dengan input password) - Contoh pengamanan pada web login dari SQL Injection dari sisi pemrograman (Filter pada input variablel) - Hacking wordpress secara default pada versi tertentu, bukan pada celah dari plugin atau themes (Mengganti isi content) - Hacking Joomla secara default pada versi-versi tertentu (Mengakses shell linux secara langsung dengan reverse shell)
	Session 5	Websploit untuk scan PMA - PHPMyAdmin Exploitation - Ngeroot Linux

		- Contoh alur mendapatkan password user dengan akses root dari hasil eksploitasi web yang vulnerable Pengamanan - Teknik melakukan banned otomatis pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan –A - Firewall UFW untuk mengatasi serangan bind shell - Firewall UFW untuk blokir ip - Pengamanan web server dari PHP Shell (Pengujian sebelum diamankan dan setelah diamankan) - Periksa celah kernel dan update kernel (Mengamankan kernel dari rooting exploit yang sebelum berhasil di rooting) - Mengganti url default URL pada PHPMyadmin - Instalasi dan konfigurasi WAF (A web application firewall) - Cara agar SQL Injection khusus bypass WAF tidak mampu bypass WAF - Pengujian XSS dan SQL Injection (Termasuk SQL Injection yang ditujukan untuk bypass WAF) - Teknik melakukan banned secara otomatis pada ip target yang melakukan scanning otomatis atau cek celah pada variabel secara manual pada web yang diamankan Pengawasan - Log web server - Log WAF (A web application firewall)

		- Instalasi dan konfigurasi Snort untuk IDS - Log IDS (Intrusion detection system) pada Snort (Linux)