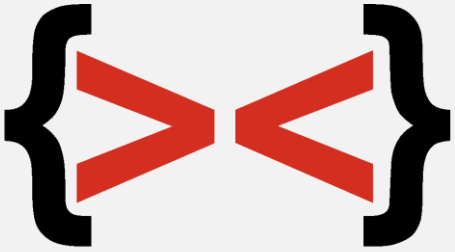
2020



Xcode Private Training

Advanced ethical web hacking & security

XCODE

Advanced Ethical Web hacking & security

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

Jumlah pertemuan : 6x pertemuan

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 - Mendeteksi jenis hash secara otomatis dan contoh melakukan cracking dari situs cracking hash - Contoh crack hash MD5 / SHA1 / lainnya dengan Hashcat

		- Mengenal web hacking - Scan untuk mendeteksi nama web server yang digunakan serta versinya, sistem operasi apa yang digunakan, jika menggunakan PHP maka menggunakan PHP versi berapa, jika menggunakan CMS maka apa nama CMS yang digunakan, jika CMS wordpress maka versi berapa wordpressnya dan sebagainya - TOR di Windows dan di linux dengan implementasinya tidak hanya di browser tapi juga di shell linux / terminal linux - Whois - Reverse domain - Google hacking - Mencari situs sesuai kriteria dengan cepat pada bing (Menampilkan semua yang dicari dalam 1 halaman) - Mencari halaman login admin (Secara otomatis mencari halaman web login admin berdasarkan dengan mencoba-coba nama-nama file halaman login admin yang umum) - Teknik-teknik bypass cloudflare - Dirbuster - Dirhunt - Dirsearch
2	Session 2	- Scan lebih dalam untuk mendapatkan versi pada suatu CMS, untuk kasus tidak terdeteksi jika menggunakan salah satu tool dari bawaan kali linux

		- Scanning Sub domain - 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 - Eksploitasi heartbleed - Buffer Overflow - HTTP Fuzzing - EIP - Pattern create & pattern offset - Menghindari proteksi pada module - JMP ESP - Proof of concept pada exploit - Memahami Get Method & post method - Cross-site scripting (XSS) - Pengamanan XSS dari sisi pemrograman - Scanning celah XSS di linux - Variasi teknik-teknik injeksi pada target dengan celah

		XSS - Eksploitasi XSS persistent untuk menggunakan akun target tanpa password login (Mengambil cookie dari target), masukkan ke browser lalu akses account target - Bypass filter upload image dengan Burp Suite - Pengamanan upload dengan .htaccess - Variasi teknik-teknik bypass filter upload
3	Session 3	- Cross-Site Request Forgery (CSRF) - Remote File Inclusion Contoh alur mendapatkan akses root dari hasil eksploitasi web yang vulnerable Crack password dengan john the ripper Menambah user dan menjadikan user menjadi admin Mengambil username dan password linux dari memory (Target : Ubuntu Desktop) Menyisipkan backdoor upload ke file php dan memasang backdoor php shell - WPscan - Scanning celah RFI di linux - Remote shell target dengan celah RFI - Bind Shell & Reverse shell - Ngeroot Linux - Contoh pengamanan terhadap serangan Remote File

		Inclusion dari sisi pemrograman - Contoh pengamanan terhadap serangan Remote File Inclusion dari sisi konfigurasi PHP.INI - Local File Inclusion - LFI untuk mendapatkan akses PHPMyadmin pada kasus celah pada plugin wordpress - Scanning celah LFI di linux - 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 - Cara mendapatkan akses shell dari LFI dengan reverse shell - WPScan - WPScan for brute force (Advanced) ~ Username Enumeration + crack password (Wordlist) - PHP Shell Development (Membuat PHP Shell sendiri dari awal untuk RFI) - Command Injection dan teknik-teknik variasinya - IDOR (Insecure Direct Object Reference) - Scanning SQL Injection - SQL Injection union - Havij di Windows

		- SQLMAP di Linux hingga crack hash password login dengan brute force - SQLMAP di Linux untuk masuk ke akses phpmyadmin - Contoh pengamanan SQL Injection dari sisi pemrograman
4	Session 4	- SQL Injection - bypass login wp - PHP upload & logger Login - BLIND SQL Injection - TIME BASED SQL Injection - 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) - SQL Injection untuk BYPASS WAF (ADVANCED) - Cara agar teknik SQL Injection khusus bypass WAF tidak mampu bypass WAF (Linux) - Pengujian pengamanan maksimal pada WAF untuk serangan XSS, RFI & SQL Injection (Termasuk serangan SQL Injection untuk bypass WAF) - Brute force dengan Burp Suite - Hacking untuk mendapatkan akses shell dengan memanfaatkan celah shellsock - 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) Websploit untuk scan PMA - PHPMyAdmin Exploitation
5	Session 5	Pengamanan - Teknik melakukan banned otomatis pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A (Linux) - Firewall UFW untuk mengatasi serangan bind shell - Firewall UFW untuk blokir ip - Blokir semua ip client kecuali ip client tertentu pada port service tertentu (kasusnya misal seperti website hanya bisa dibuka ip tertentu atau juga bisa misal untuk akses ssh hanya bisa diakses ip tertentu, tapi untuk web bisa diakses semua ip yang terhubung) - Pengamanan web server dari PHP Shell (Pengujian sebelum diamankan dan setelah diamankan) (Linux) - Eksploitasi PHP 7 (bypass disable_function & open_basedir) serta pengamanannya) - Periksa celah kernel linux dan update kernel (Mengamankan kernel dari rooting exploit yang sebelum berhasil di rooting) - Menonaktifkan Directory Listing (Linux) - Menyembunyikan halaman login wordpress

		- Mengganti url default URL pada PHPMyadmin (Linux) - PHPMyadmin Honeypot (Di linux) - Deteksi PHP Shell secara otomatis - Teknik melakukan banned pada ip attacker secara otomatis yang melakukan serangan brute force pada SSH (Linux) - Instalasi dan konfigurasi WAF (A web application firewall) (Linux)
6	Session 6	- Pertahanan dengan cloudflare - Setting name servers di domain dengan name server dari cloudflare - Set SSL / TLS encryption mode is Full (Strict) - pengamanan dengan cloudflare origin CA certificate on the server - Under Attack Mode di cloudflare - Setting virtualhost di web server - 2 Teknik bypass ip cloudflare disertai pengamanannya - Teknik agar web tidak bisa diakses lewat ip - Log pada web server jika diakses lewat domain / subdomain