



Xcode Intensif Training
Ethical Web hacking &
Security ~ Advanced



Ethical Web hacking ~ Advanced

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

Ethical web hacking & Security ~ Advanced

No	Session	Objective
Performing Basic System Management Tasks		
1	Session 1	<ul style="list-style-type: none"> - 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

		<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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 - Mengetahui POST dan GET - Memahami Get Method & post method - Manipulasi input pada post method untuk CSS (Cascading Style Sheets) Injection

		<ul style="list-style-type: none"> - Contoh pengamanan agar tidak terkena serangan CSS (Cascading Style Sheets) Injection - 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
	<p>Session 3</p>	<ul style="list-style-type: none"> - 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

		<ul style="list-style-type: none"> - 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
	<p>Session 4</p>	<ul style="list-style-type: none"> - SQL Injection union (MANUAL) - BLIND SQL Injection (MANUAL) - TIME BASED SQL Injection (MANUAL) - SQL Injection untuk BYPASS WAF (ADVANCED)

		<ul style="list-style-type: none"> - 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 - Tabel kebenaran gerbang "AND" dan "OR" - Variasi SQL Injection pada 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 variabel)
	<p>Session 5</p>	<p>Websploit untuk scan PMA</p> <ul style="list-style-type: none"> - PhpMyAdmin Exploitation Advanced - Ngeroot Linux - Contoh alur mendapatkan password user dengan akses root dari hasil eksploitasi web yang vulnerable <p>Pengamanan</p> <ul style="list-style-type: none"> - Teknik melakukan banned otomatis pada ip target yang melakukan scanning menggunakan NMAP dengan option seperti misal -sV dan -A

	<ul style="list-style-type: none">- 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)- Pengamanan brute force untuk wordpress- Membangun honeypot web untuk wordpress- Instalasi dan konfigurasi WAF (A web application firewall)- Cara agar SQL Injection khusus bypass WAF tidak mampu bypass WAF- Pengujian XSS, RFI & 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 <p>Pengawasan</p> <ul style="list-style-type: none">- Log web server- Log IDS (Intrusion detection system) pada Snort (Linux)- Log WAF (A web application firewall)
--	---