CYBER SECURITY : WEB EXPLOITATION AND DEFENSE

TECH-STACK: PENETRATION TESTING, WEBSITE HACKING, BRUTEFORCE, SQL INJECTION, RED LIMITER, CROSS-SITE SCRIPTING (XSS) ,DIRECTORY TRAVERSAL, SENSITIVE INFORMATION DISCLOSURE, ACCESS CONTROL,FILE UPLOAD, AUTHENTICATION & AUTHORIZATION, INCIDENT RESPONSE

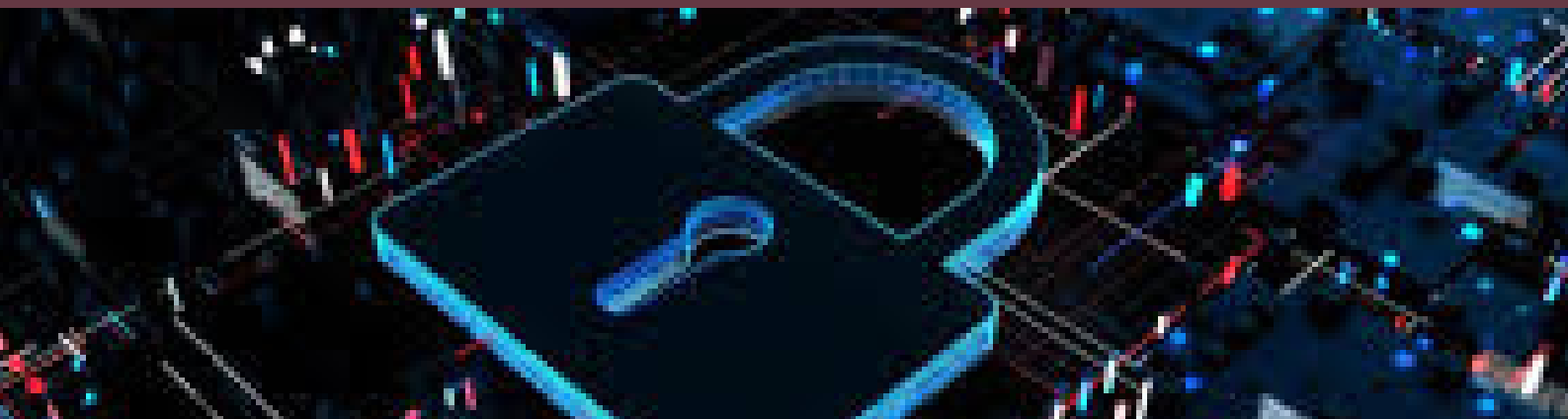
M-Knows Consulting

CYBER SECURITY

Web Security Bootcamp: Exploitation and Defense adalah sebuah program pelatihan intensif yang dirancang untuk memberikan pemahaman mendalam tentang keamanan web, dengan fokus pada teknik eksploitasi dan pertahanan. Bootcamp ini bertujuan untuk melatih peserta dalam mengidentifikasi kerentanan pada aplikasi web, memahami cara kerja serangan, dan mengimplementasikan langkah-langkah perlindungan yang efektif.

Bootcamp ini dirancang untuk para profesional keamanan, pengembang web, dan siapa pun yang ingin memperdalam pemahaman mereka tentang dunia keamanan web yang kompleks. Dalam lingkungan pelatihan yang intensif dan interaktif, peserta akan dihadapkan pada simulasi dunia nyata dari serangan dan pertahanan keamanan web.

Selama bootcamp, peserta akan menjelajahi kasus-kasus nyata tentang serangan terkenal pada aplikasi web, menggali metode pengeksploitasian yang digunakan oleh penyerang, dan menyelami detil teknis dari celah keamanan. Ini akan memberi mereka wawasan mendalam tentang bagaimana serangan terjadi, mengapa kerentanan dapat dieksploitasi, dan bagaimana dampaknya terhadap sistem dan data yang terlibat.



CYBER SECURITY

Selama bootcamp, peserta akan menjelajahi kasus-kasus nyata tentang serangan terkenal pada aplikasi web, menggali metode pengeksploitasian yang digunakan oleh penyerang, dan menyelami detil teknis dari celah keamanan. Ini akan memberi mereka wawasan mendalam tentang bagaimana serangan terjadi, mengapa kerentanan dapat dieksploitasi, dan bagaimana dampaknya terhadap sistem dan data yang terlibat.

Bootcamp ini memberikan penekanan khusus pada etika keamanan siber. Peserta diberikan ilmu tentang bagaimana melaporkan kerentanan secara bertanggung jawab, serta berkontribusi dalam menghadirkan lingkungan internet yang lebih aman dan terlindungi.

"Cyber Security Bootcamp: Web Exploitation and Defense" adalah kesempatan peserta untuk menjalani peran ganda sebagai penyerang dan penjaga, memberi ilmu mendalam tentang dunia cyber security yang terus berkembang dan kompleks khususnya keamanan web.

Silabus Pelatihan

Sesi 1: Pengenalan Keamanan Website

1. Pengenalan keamanan web dan pentingnya melindungi aplikasi online.
2. Model ancaman umum terhadap aplikasi web.
3. Prinsip dasar keamanan web: kerentanan dan serangan umum.
4. Pengenalan alat-alat yang digunakan dalam pengujian keamanan web.
5. Penugasan 1: Meriset Tools terbaru dan kasus terkini web security breach.

Sesi 2: Keamanan Hypertext Transfer Protocol (HTTP)

1. Pengenalan keamanan web dan pentingnya melindungi aplikasi online.
2. Pengertian dasar tentang protokol HTTP (Hypertext Transfer Protocol).
3. Verbs HTTP: GET, POST, PUT, DELETE, dan metode lainnya.
4. Pengenalan ke header HTTP dan bagaimana informasi dikirimkan antara klien dan server.
5. Penugasan 2: Mengerjakan soal mengenai fungsi Hypertext Transfer Protocol (HTTP) dalam website aplikasi.

Sesi 3: Melakukan Setup Environment pada device peserta

1. Instalasi OS (rekomendasi OS linux).
2. Instalasi Burp Suite.
3. Konfigurasi Burp Suite.
4. Mempelajari apa itu Burp Suite.
5. Penugasan 3: Memberikan bukti bahwa tools sudah terinstall pada device peserta (jika ada error bisa langsung ditanyakan mentor).

Sesi 4: Aspek keamanan Autentikasi dan Otorisasi

1. Pengantar tentang Autentikasi dan Otorisasi.
2. Pemahaman risiko serangan Bypass OTP pada autentikasi.
3. Pemahaman risiko serangan brute-force
4. Pentingnya manajemen otorisasi yang tepat.
5. Teknik mitigasi untuk melindungi sistem dari masalah Autentikasi dan Otorisasi.
6. Penugasan 4: Mencari minimal 3 lubang keamanan dari website autentikasi dan otorisasi yang ditugaskan.

Silabus Pelatihan

Sesi 5: Mencari celah keamanan dengan metode SQL Injection

1. Pengenalan SQL Injection (SQLi).
2. Bypass password melalui SQL Injection.
3. Jenis metode SQLI (Union dan Blind SQLI
4. Tindakan mitigasi untuk melindungi terhadap SQL Injection.
5. Penugasan 5: Mencari minimal 3 lubang keamanan SQL injection dari website yang ditugaskan.

Sesi 6: Mencari celah keamanan dengan metode Cross-site Scripting (XSS)

1. Pengenalan tentang Cross-site Scripting (XSS).
2. Jenis metode XSS(Reflected, Stored, DOM Based XSS).
3. Teknik mitigasi untuk melindungi dari serangan XSS.
4. Penugasan 6: Mencari minimal 3 lubang keamanan Cross site scripting (XSS) dari website yang ditugaskan.

S**esi 7: Mencari celah keamanan dengan metode Directory Traversal**

1. Pengenalan tentang Local File Inclusion (LFI) dan Remote File Inclusion (RFI).
2. Contoh pemanfaatan LFI dan RFI untuk mengakses file lokal.
3. Memanfaatkan LFI dan RFI untuk mendapatkan RCE
4. Mitigasi risiko dan kerentanan LFI dan RFI.
5. Penugasan 7: Mencari minimal 3 lubang keamanan Directory Traversal dari website yang ditugaskan.

Sesi 8: Mencari celah keamanan dengan metode Access Control

1. Pengenalan tentang Broken Access Control.
2. Pentingnya pengendalian akses yang tepat.
3. Serangan Insecure Direct Object References (IDOR).
4. Mitigasi serangan Broken Access Control.
5. Penugasan 8: Mencari minimal 3 lubang keamanan Access control dari website yang ditugaskan.

Silabus Pelatihan

Sesi 9: Mencari celah keamanan dengan metode File Upload

1. Pengenalan tentang File Upload.
2. Risiko dan ancaman terkait dengan unggahan berkas yang tidak aman.
3. Memahami serangan pada fitur unggahan berkas.
4. Mitigasi terbaik dalam mengamankan fitur unggahan berkas.
5. Penugasan 9: Mencari minimal 3 lubang keamanan File upload dari website yang ditugaskan.

Sesi 10: Mencari celah keamanan dengan menemukan Sensitive Information Disclosure

1. Pengenalan tentang Information Disclosure.
2. Risiko dan dampak dari kebocoran informasi.
3. Jenis-jenis Information Disclosure pada website.
4. Teknik pencarian informasi sensitif melalui Google Dorking.
5. Mitigasi terhadap Information Disclosure.
6. Penugasan 10: Mencari minimal 3 lubang keamanan Information Disclosure dari website yang ditugaskan.

Sesi 11: Teknik Pencegahan Keamanan pada Front End dan Back End

1. Identifikasi kerentanan umum pada front end dan API dari backend.
2. Pengenalan teknik enkripsi dan hashing
3. Memperhatikan input dan validasi data di sisi front end dan back end.
4. Penugasan 11: Melakukan riset artikel mengenai Teknik Pencegahan Keamanan pada Front End dan Back End

Sesi 12: Web Security Incident Response

1. Menganalisis akar penyebab insiden
2. Menentukan dampak insiden terhadap aplikasi web.
3. Pemulihan data dan sistem yang terdampak.
4. Memvalidasi integritas data setelah insiden.
5. Penugasan 12: Membuat report terkait incident response dari celah yang ditemukan.

Sesi 13: Penugasan Proyek Akhir dan Mentoring 1:
Cyber Security Bootcamp: Web Exploitation and Defense
Sesi 14: mentoring Tugas Akhir 2
Sesi 15: Presentasi Proyek Akhir, Penilaian, dan Penutupan.

Deskripsi Proyek:

Proyek akhir ini bertujuan untuk mempraktekkan tech-stack yang telah dipelajari meliputi, konsep eksploitasi dan pertahanan keamanan web. Dalam proyek ini, peserta menggabungkan pengetahuan dari bootcamp tentang teknik eksploitasi kerentanan aplikasi web, serta strategi pertahanan guna melindungi aplikasi web dari serangan. Proyek ini dikerjakan secara kelompok melibatkan langkah-langkah eksploitasi yang dilakukan oleh penyerang serta langkah pertahanan yang direkomendasikan untuk mengatasi risiko serangan.

Tahap - Tahap Proyek Kolaborasi Kelompok :

- Ajukan situs web yang akan diuji dan tech stack yang akan digunakan, untuk persetujuan fasilitator. Lebih baik bila penugasan ini bisa digunakan sebagai bahan tugas akhir atau skripsi anda dan kelompok.

- Identifikasi Kerentanan Aplikasi Web: Lakukan Analisis kode dan infrastruktur aplikasi untuk mengidentifikasi potensi kerentanan seperti Cross-Site Scripting (XSS), SQL Injection, dan lainnya, sesuai tech stack yang anda pilih di proposal anda.

- Eksploitasi Kerentanan: Implementasikan skenario eksploitasi untuk kerentanan yang telah diidentifikasi. Misalnya, jika Anda menemukan kerentanan XSS, ciptakan skrip yang memanfaatkan kerentanan ini untuk mengambil informasi sensitif dari pengguna.

- Penilaian Keamanan: Lakukan uji penetrasi pada aplikasi web setelah penerapan langkah-langkah pertahanan. Apakah serangan yang telah berhasil dilakukan pada tahap sebelumnya masih dapat berhasil.

- Laporan Proyek: Buat laporan yang merinci langkah-langkah yang telah kelompok ambil dalam mengidentifikasi, mengeksploitasi, dan memperbaiki kerentanan. Sertakan penjelasan tentang teknik eksploitasi yang digunakan, langkah-langkah pertahanan yang diimplementasikan, hasil uji penetrasi, serta rekomendasi tambahan untuk meningkatkan keamanan aplikasi.

- Presentasi Proyek: Susun presentasi yang merangkum laporan proyek kelompok. Berikan penjelasan tentang tujuan proyek, langkah-langkah yang kelompok ambil, temuan, serta pelajaran yang diperoleh sepanjang proses.

- Refleksi dan Pelajaran: Sertakan bagian refleksi di laporan proyek kelompok. Ceritakan tentang pengalaman kelompok selama melakukan proyek ini, tantangan yang dihadapi, dan pengetahuan baru yang diperoleh tentang keamanan web

KEMAMPUAN YANG AKAN DIKUASAI

TECH-STACK: PENETRATION TESTING, WEBSITE HACKING, BRUTEFORCE, SQL INJECTION, RED LIMITER, CROSS-SITE SCRIPTING (XSS) ,DIRECTORY TRAVERSAL, SENSITIVE INFORMATION DISCLOSURE, ACCESS CONTROL,FILE UPLOAD, AUTHENTICATION & AUTHORIZATION, INCIDENT RESPONSE

Hard Skill:

Dengan akhir bootcamp, peserta diharapkan dapat:

1. Memahami prinsip-prinsip dasar keamanan web dan berbagai jenis serangan yang mungkin terjadi.
2. Mengidentifikasi dan mengevaluasi kerentanan potensial dalam aplikasi web.
3. Menerapkan teknik-teknik eksploitasi yang lazim digunakan oleh penyerang.
4. Menerapkan langkah-langkah pertahanan yang efektif untuk melindungi aplikasi web.
5. Mengembangkan kemampuan untuk berkontribusi dalam upaya perlindungan siber secara global.

Soft Skills :

1. Mampu berkolaborasi dalam tim untuk mengatasi tantangan keamanan web secara efektif.
2. Mampu menganalisis secara mendalam untuk mengidentifikasi kerentanan dan risiko keamanan.
3. Mampu menganalisis informasi dengan kritis dan mengambil keputusan yang terinformasi.
4. Memahami dan mengikuti etika dalam keamanan siber serta tindakan bertanggung jawab.waktu dengan efisien untuk menyelesaikan tugas-tugas dalam batas waktu.
5. Fleksibel dalam menghadapi perubahan dan situasi yang berkembang dalam keamanan web.

Skema Penilaian

Partisipasi Aktif (25%): Kehadiran dan partisipasi aktif peserta dalam setiap sesi akan dinilai. Peserta dlharapkan terlibat dalam diskusi, bertanya pertanyaan, dan berkontribusi dalam diskusi kelompok.

Proyek Akhir (50%): Proyek akhir akan dinilai berdasarkan beberapa aspek:

- Implementasi Teknik Eksploitasi (15%): Sejauh mana peserta mampu mengimplementasikan teknik eksploitasi yang dipelajari pada proyek mereka.
- Langkah-langkah Pertahanan (10%): Bagaimana peserta merancang dan menerapkan langkah-langkah pertahanan yang efektif terhadap serangan yang mungkin terjadi pada proyek mereka.
- Laporan Proyek dan Presentasi (10%): Kualitas laporan proyek dan kemampuan peserta dalam menyajikan proyek secara jelas dan efektif.

Ujian Akhir Bootcamp Pilihan Ganda (25%): Ujian akhir akan mencakup seluruh materi bootcamp, termasuk teknik-teknik eksploitasi, pertahanan, dan konsep dasar keamanan. Ujian ini akan mengukur pemahaman menyeluruh peserta terhadap materi.

Catatan: Skema penilaian ini dapat disesuaikan sesuai dengan tujuan dan kompleksitas bootcamp. Pastikan untuk memberikan umpan balik yang jelas dan konstruktif kepada peserta setiap tahap, serta menjelaskan kriteria penilaian dengan jelas sejak awal bootcamp.

Pengaturan Bootcamp

Pelatihan dimulai pada tanggal 31 oktober 2023
Pertemuan : 12x (Dua Belas Kali)
Durasi : 2-3 Jam

Seminggu 2 kali pertemuan
Hari : Setiap Selasa dan Kamis
Waktu : 19.00 s/d Selesai

Untuk peserta yang tidak hadir, dapat menonton rekaman ulang.

SALE

*Pembayaran dapat di cicil sebanyak 3 kali

Special Price :
Rp. 300.000