[Capture The Flag]

NAMA TIM : Gak gini gak gitu

Selasa 15 September 2020

Ketua Tim	
1.	I Made Wahyudi
Member	
1.	I Putu Pramayasa Anesa Putra
2.	Christopher Hendratno

Jawaban

1. Kasus - Kasus Data Breaches :
    a. Yahoo! pada tahun 2013 -> Cookie-based Attack yang digunakan untuk login ke akun manapun tanpa memerlukan password.
    b. Adult Friend Finder pada tahun 2016 -> Karena adanya celah keamanan pada Module di production server & Local File Inclusion (LFI) yang berhasil di exploit.
    c. Panama Papers -> DIkarenakan versi Drupal yang dipakai memiliki kelemahan.
    d. Ubuntu Forum Breach -> Karena adanya kelemahan pada versi add-on Forumrunner yang belum di patch sehingga memungkinkan attacker untuk melakukan SQL Injection.
    e. Philippines' Commission on Elections breach -> Karena adanya kelemahan SQL Injection.
    f. i-Dressup breach -> Karena adanya kelemahan SQL Injection.
2. Personally Identifiable Information (Informasi Identifikasi Pribadi) atau PII bisa hadir dalam berbagai bentuk, bahkan bisa terbentuk dan kamu tidak sadar. Data-data inilah yang digunakan untuk mengetahui hal-hal tentang dirimu, termasuk kebiasaan dan kesukaanmu.
3. Kesalahan umum terkait keamanan yang biasa dilakukan oleh penyedia layanan teknologi informasi yang menggunakan komputasi awan adalah :
    a. Membebaskan hak akses pada siapapun.
    b. Menganggap bahwa layanan komputasi awan itu 100% aman (TIDAK ADA SISTEM YANG AMAN).
    c. Tidak memiliki plan B ketika terjadi hal - hal yang tidak diinginkan.
    d. Koneksi internet yang buruk / Tidak aman.
    e. Salah dalam memilih Provider.
    f. Data tidak terencrypt.
    g. Tidak melakukan backup.
4. Resiko yang akan didapatkan dari zeroday pada memory corruption adalah adanya kemungkinan dimana address fungsi dari web browser dapat di ubah dengan memainkan vulnerability memory corruption seperti **Use After Free** ataupun **Double Free** yang dapat memungkinkan penyerang(dalam bahasa C) untuk mengganti sebuah fungsi menjadi **system** dengan argumen **/bin/sh** sehingga mendapatkan **RCE.**
5. Kemungkinan risiko dari open redirect adalah phising. Risiko bisa meningkat apabila ada celah lain seperti CSRF atau XSS.
6. Menggunakan query dengan keyword **SLEEP** dan memastikan hasil dari query tersebut **True** atau **False** berdasarkan waktu **SLEEP** yang digunakan.
7. Contoh karir yang bisa dieksplorasi oleh orang yang memiliki minat/bakat di:
    a. Web hacking: Web Penetration Tester
    b. Cryptography: Cryptanalyst
    c. Digital forensics: Kepolisian
    d. Reverse engineering: Malware Analyst

e. Binary Exploit: Infosec in Mobile / Desktop Development