DISKOMINFO BATAM

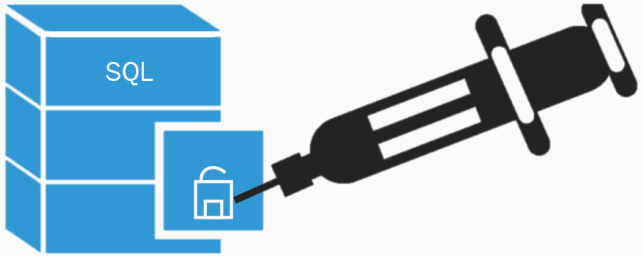
G20 INDONESIA 2022

BerAKHLAK

PANDUAN PENANGANAN INSIDEN SERANGAN

SQL INJECTION

Dinas Komunikasi dan Informatika Kota Batam



DISKOMINFO BATAM

BerAKHLAK

PENDAHULUAN

Serangan SQL Injection merupakan jenis eksploitasi keamanan halaman web, dimana penyerang menyisipkan kode-kode SQL melalui formulir/form kemudian memanipulasi URL berdasarkan pada parameter sql. Serangan SQL Injection adalah serangan yang berupa menginjeksi perintah SQL melalui form input data, yang kemudian diteruskan menuju database untuk dieksekusi, dengan tujuan mengakses data sensitif pada database

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK

TUJUAN

- Memastikan adanya sumber daya yang memadai untuk menangani serangan yang terjadi
- Melakukan pengumpulan informasi yang akurat
- Meminimalisir dampak dari serangan yang terjadi
- Mencegah adanya serangan lanjutan dan mencegah kerusakan agar tidak lebih meluas

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK

RUANG LINGKUP

Panduan ini berisi langkah-langkah yang harus diambil apabila terjadi serangan SQL Injection, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan

Panduan ini dapat dijadikan acuan bagi semua individu atau tim (administrator, pengelola TI, tim respon insiden kamanan komputer) yang bertanggung jawab untuk mencegah, mempersiapkan atau menangani serangan SQL Injection pada suatu website

DISKOMINFO BATAM

BerAKHLAK

PROSEDUR PENANGANAN SERANGAN SQL INJECTION

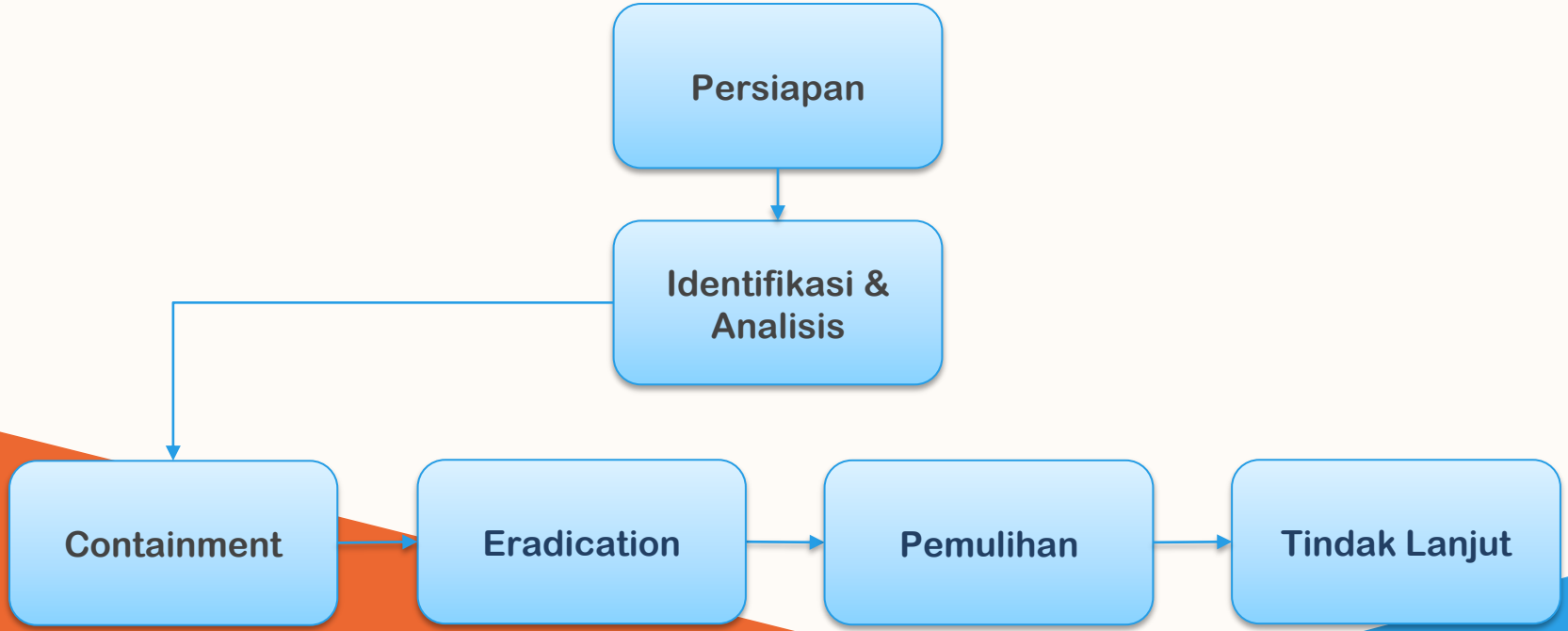
1. Mengumpulkan informasi sebanyak mungkin tentang serangan SQL Injection

2. Menghalangi atau mencegah eskalasi kerusakan yang disebabkan oleh serangan tersebut

3. Mengumpulkan bukti terkait serangan SQL Injection

4. Mengambil langkah-langkah proaktif untuk mengurangi kemungkinan terjadinya serangan SQL Injection di masa depan

TAHAP PENANGANAN TERHADAP SERANGAN SQL INJECTION



PERSIAPAN

Dalam melakukan penanganan serangan SQL Injection, perlu adanya tahap persiapan dengan beberapa prosedur

A. Pembentukan tim respon, tim dapat berasal dari institusi yang mengalami serangan (internal) atau juga bisa berasal dari luar institusi (eksternal) jika memang diperlukan. Anggota tim memiliki pengetahuan tentang SQL Injection dan memiliki kemampuan penanganannya

B. Menyiapkan dokumen yang dibutuhkan dalam proses penanganan serangan SQL Injection. Dokumen ini antara lain adalah
- Panduan penanganan insiden serangan siber
- Formulir penanganan insiden serangan siber
- Diagram yang menggambarkan hubungan antar komponen-komponen aplikasi yang membangun website (web server, aplikasi web, daftar user, diagram network)

C. Menyiapkan tool dan media yang dibutuhkan untuk penanganan. Misalnya Notepad ++ untuk membaca log, IDS/IPS, SQL Map, Accunetix /Nessus

IDENTIFIKASI DAN ANALISIS

Tujuan dari proses identifikasi dan analis adalah:

a. Memahami sifat dan ruang lingkup kejadian
b. Mengumpulkan informasi yang cukup tentang serangan SQL Injection sehingga tim respon dapat memprioritaskan langkah selanjutnya dalam menangani serangan tersebut, yang biasanya diikuti dengan penahanan sistem

Pada tahap ini dilakukan proses identifikasi untuk memastikan telah terjadi serangan SQL Injection dan mendeteksi sumbernya

Langkah-langkah yang dapat diambil pada tahap identifikasi dan analisis antara lain:

a. Memeriksa alert dan anomalies dari perangkat IDS atau IPS

b. Melakukan error checking melalui form atau url dengan memberikan karakter atau sebuah simbol. Misalnya:
   - Melalui form login, memasukan pada username dan password berupa karakter-karakter yang digunakan SQL Injection
   - Melalui url, menambahkan karakter-karakter yang digunakan SQL Injection, seperti single quote, double minus

IDENTIFIKASI DAN ANALISIS

c. Memeriksa semua log (error log, access log, database log, firewall log). Lokasi log file secara default berada pada var/log, log tersebut menyimpan seluruh aktivitas yang terjadi pada sistem

d. Memeriksa adanya command line, string-string yang digunakan untuk menyerang

e. Memeriksa isi database untuk mencari script yang berbahaya, dan mengecek apakah ada penambahan user secara tidak sah

f. Memeriksa apakah ada file atau script berbahaya (trojan, malicious file, backdoor) yang ditanamkan pada web server

g. Menggunakan tool untuk memeriksa kerentanan. Tool yang dapat digunakan diantaranya Acunetix, SQLMap, SQL Injection tools

IDENTIFIKASI DAN ANALISIS

Mengukur dampak dari terjadinya SQL Injection adalah

a. Terhadap kelangsungan proses bisnis, indikatornya adalah seberapa besar dari fungsi-fungsi bisnis yang terdapat pada website mengalami gangguan

b. Terhadap sistem dan informasi, apakah penyerang melakukan distribusi malware, membuat backdoor atau melakukan web defacement. Selain itu, apakah ada data dan informasi yang berubah atau terhapus

CONTAINMENT

PROSES

Setelah dipastikan bahwa memang benar telah terjadi serangan SQL Injection, maka dilakukan proses berikutnya dengan tujuan:

1. Tidak terjadi kerusakan lebih dalam
2. Mencegah penyerang masuk lebih dalam ke sistem yang terkena dampak
3. Melindungi server-server lain yang terhubung dengan aplikasi web

PROSEDUR

Prosedur yang dilakukan pada tahap ini adalah:

1. Melakukan proses backup semua data yang terdapat pada web server. untuk keperluan forensik dan pengumpulan bukti-bukti. Backup sebaiknya ditempatkan pada hard disk eksternal
2. Jika sumber penyerangan berasal dari sistem lain pada jaringan, maka putuskan secara fisik koneksi tersebut dan lakukan investigasi sumber tersebut

ERADICATION

Tahap Eradication pada penanganan serangan SQL Injection adalah untuk menghapus file /script serta menutup sumber serangan

Memeriksa apakah terdapat malicious file, backdoor, rootkit atau kode-kode berbahaya lainnya yang berhasil ditanamkan pada server dan segera menghapusnya

Jika terdapat kode SQL yang mengakses IP tertentu maka perlu melakukan block /menutup sumber serangan (block IP dan Port)

PEMULIHAN

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula

Prosedur yang dapat dilakukan sebagai berikut:

a. Mengubah kredential password pengguna. Hal ini untuk mengantisipasi apabila password pengguna telah diketahui oleh penyerang

b. Melakukan recovery database pada aplikasi web

c. Jika SQL Injection menyebabkan web defacement, gunakan panduan penanganan insiden web defacement

d. Jika SQL Injection menyebabkan insiden malware, gunakan panduan penanganan insiden malware

e. Menutup semua kerentanan yang telah diketahui

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK

PEMULIHAN

f. Membatasi akses root langsung ke database

g. Melakukan filter terhadap input yang dimasukkan oleh pengguna

h. Mematikan atau menyembunyikan pesan-pesan error yang keluar dari SQL Server yang berjalan

i. Patching terhadap aplikasi yang rentan, melakukan upgrade terhadap aplikasi web yang masih memiliki kerentanan

j. Melakukan penetration testing untuk mengetahui celah-celah keamanan yang mungkin masih terdapat pada website

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK

TINDAK LANJUT

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk di masa mendatang

1. Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan SQL Injection

2. Mengambil pelajaran dan membuat rekomendasi untuk mencegah terjadi lagi

PROSEDUR

1. Membuat dokumentasi dan laporan terkait penanganan serangan SQL Injection
2. Menuliskan tools apa saja yang digunakan dalam penanganan serangan injeksi sql
3. Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya
4. Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga serangan serupa tidak terulang kembali
5. Membuat evaluasi dan rekomendasi

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK

PANDUAN PENANGANAN INSIDEN SERANGAN

SQL INJECTION

Dinas Komunikasi dan Informatika Kota Batam