PETUNJUK PENGGUNAAN APLIKASI SEMONT

SEMONT

Sentinel Monitoring

Disusun oleh:

Alwi Al Hadad

Hani Harafani

DAFTAR ISI

BAB I
PENGENALAN SISTEM

1.1 Tentang SEMONT (Sentinel Monitoring)

Aplikasi ini bernama SEMONT (*Sentinel Monitoring*) dan merupakan sebuah sistem keamanan berbasis *Intrusion Detection and Prevention System* (*IDPS*) yang digunakan untuk memantau dan melindungi aplikasi web dari serangan digital. SEMONT berjalan secara otomatis pada server melalui mekanisme *auto_prepend_file* yang terdapat pada file *.htaccess*, sehingga setiap permintaan (*request*) yang masuk ke server akan dianalisis terlebih dahulu oleh SEMONT sebelum diteruskan ke aplikasi utama.

SEMONT bekerja dengan mendeteksi berbagai ancaman seperti *SQL Injection*, *Cross-Site Scripting*, *Remote Code Execution*, *Local File Inclusion*, aktivitas *scanning* otomatis, percobaan *brute force*, serta upaya *defacement*. Sistem ini kemudian melakukan pemblokiran dan mencatat hasil deteksi ke dalam *log* yang dapat dilihat oleh admin melalui *dashboard*.

Di dalam SEMONT terdapat beberapa komponen utama seperti loader, modul firewall, sistem pencatatan (*logger*), serta *dashboard* admin. Setiap komponen memiliki peran masing-masing dalam menjaga keamanan server dan aplikasi, mulai dari menganalisis *payload*, memeriksa pola serangan, hingga memberikan peringatan secara *real-time* melalui Telegram.

Fitur-fitur yang terdapat pada SEMONT dirancang agar mudah digunakan dan dapat berjalan pada berbagai jenis layanan hosting, termasuk *shared hosting*. SEMONT sangat cocok digunakan pada website sekolah, organisasi pemerintah, UMKM, maupun sistem yang membutuhkan proteksi tambahan tanpa memerlukan konfigurasi kompleks.

1.2 Arsitektur dan Cara Kerja SEMONT

SEMONT terdiri dari beberapa komponen fungsional utama yang bekerja secara terintegrasi:

1. Loader (*auto_prepend_file*)

Komponen ini memastikan bahwa setiap file PHP yang dipanggil pada server akan dieksekusi melalui SEMONT terlebih dahulu. Loader berada pada direktori core/loader.php dan menjadi titik awal seluruh proses analisis dan pencegahan.

2. *Firewall Module*

   Modul ini melakukan proses pattern matching untuk mendeteksi apakah suatu request mengandung pola serangan yang telah terdaftar dalam signature database. Jika terdeteksi sebagai serangan, SEMONT akan memblokir eksekusi, menghentikan request, dan mencatat insiden ke dalam log.

3. *Logger dan Storage*

   Seluruh aktivitas mencurigakan dicatat secara terstruktur pada direktori storage. Informasi yang direkam meliputi waktu kejadian, alamat IP pelaku, payload yang digunakan, jenis serangan, lokasi target (URL), dan device fingerprint yang digunakan oleh pelaku.

4. *Dashboard Sentinel*

   SEMONT menyediakan antarmuka admin untuk melakukan *monitoring* dan pengelolaan. Dashboard ini memungkinkan admin melihat *log* secara *real-time*, mengelola daftar IP yang diblokir, melakukan *deface scanning*, memantau *fingerprint* perangkat, serta melakukan konfigurasi sistem. Dashboard dilindungi dengan mekanisme autentikasi berbasis *Telegram ID* dan *One-Time Password (OTP)* untuk memastikan akses yang aman.

1.3 Fitur Utama SEMONT

1. Deteksi dan Pencegahan Serangan Injeksi

SEMONT mampu mengidentifikasi pola serangan injeksi termasuk *SQL Injection*, *XSS*, *RCE*, *LFI*, dan *HTML Injection*. Jika *request* berisi *payload* berbahaya, sistem akan memblokir otomatis dan menghentikan proses sebelum aplikasi utama dipanggil.

2. Deteksi Serangan *Brute Force*

Sistem memantau aktivitas login atau *endpoint* tertentu. Jika ditemukan percobaan login berulang dari IP yang sama melebihi batas wajar, SEMONT akan melakukan pemblokiran otomatis.

3. Deteksi dan Penanganan *Defacement*

SEMONT dapat melakukan pemindaian direktori web untuk mendeteksi file yang terindikasi *deface*, seperti file asing, modifikasi tidak sah, atau konten yang mengandung kata kunci *defacement*. Sistem juga dapat menghapus file *deface* secara otomatis.

4. Deteksi *User-Agent* dan Alat Berbahaya

SEMONT memiliki daftar *signature user-agent* yang digunakan oleh alat *scanning* seperti *Dirsearch*, *Gobuster*, *Nmap*, *Nikto*, *Nessus*, dan alat otomatis lainnya. Jika *request* berasal dari *user-agent* tersebut, sistem akan memutus koneksi dan memberikan respons *error*.

5. *Device Fingerprinting*

Sistem dapat mendeteksi informasi perangkat seperti *browser*, *operating system*, dan karakteristik lainnya yang membantu identifikasi pelaku.

6. Notifikasi *Real-Time* melalui Telegram

SEMONT mengirimkan pemberitahuan otomatis kepada admin setiap kali terjadi serangan. Pesan yang dikirimkan berisi informasi lengkap mengenai IP penyerang, jenis serangan, *payload*, *URL* target, serta waktu kejadian.

1.4 Keunggulan SEMONT

1. Mudah diintegrasikan pada server web tanpa memerlukan konfigurasi kompleks.
2. Dapat berjalan pada *shared hosting* karena tidak membutuhkan akses *root*.
3. Memiliki *signature pattern* yang dapat diperbarui dan dikembangkan secara mandiri.
4. Memberikan deteksi dan pencegahan secara *real-time*.
5. Menyediakan dashboard yang sederhana, intuitif, dan mudah digunakan.

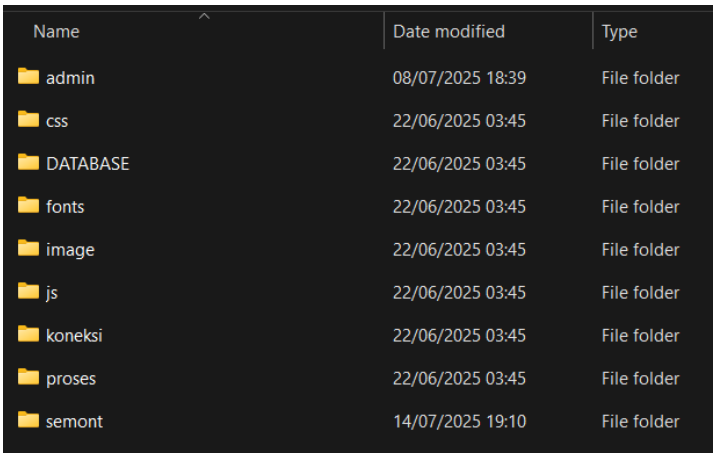
6. Cocok digunakan untuk berbagai skala aplikasi, mulai dari sekolah, UMKM, organisasi pemerintah, hingga perusahaan.

BAB II
INSTALASI DAN KONFIGURASI

2.1 Instalasi SEMONT

1. Mengunggah Folder *semont* ke Server

Unggah folder semont ke direktori utama website Anda. Pada lingkungan shared hosting, direktori umum yang digunakan adalah /public_html/



Name	Date modified	Type
admin	08/07/2025 18:39	File folder
css	22/06/2025 03:45	File folder
DATABASE	22/06/2025 03:45	File folder
fonts	22/06/2025 03:45	File folder
image	22/06/2025 03:45	File folder
js	22/06/2025 03:45	File folder
koneksi	22/06/2025 03:45	File folder
proses	22/06/2025 03:45	File folder
semont	14/07/2025 19:10	File folder

```
1   php_value auto_prepend_file "/home/smanrancaekek/public_html/semont/core/loader.php""
2
```

Namun lokasi dapat disesuaikan dengan struktur dan kebutuhan aplikasi masing-masing. Pastikan folder **semont** berada utuh sebagaimana paket instalasi yang diberikan. Contoh struktur penempatan:

```
/public_html/
    ├── semont/
    └── (file atau folder aplikasi utama)
```

2.2 Menambahkan Konfigurasi pada File .htaccess

Agar SEMONT berjalan otomatis sebelum aplikasi inti diproses, tambahkan konfigurasi auto_prepend_file pada file .htaccess.

Buka file .htaccess, kemudian tambahkan baris berikut:

```
php_value auto_prepend_file "/home/namafolderutama/public_html/semont/core/loader.php"
```

Keterangan:

- *namafolderutama* adalah direktori utama akun hosting Anda.
- Pastikan *path* sesuai dengan struktur server.

2.3 Konfigurasi ID Telegram

1. Mengakses Direktori Konfigurasi

Masuk ke server melalui *File Manager* atau *FTP* dan buka:

```
semont/core/telegram_ids.json
```

2. Mengatur ID Telegram

Edit isi file menggunakan format berikut:

```
{
  "telegram_chat_ids": ["masukkan disini"],
  "telegram_chat_admin-ids": ["masukkan disini"]
}
```

Penjelasan:

a. **telegram_chat_ids** → ID pengguna yang berhak menerima notifikasi SEMONT.

b. **telegram_chat_admin-ids** → ID admin yang memiliki akses penuh ke *dashboard*. Contoh :

```
{
  "telegram_chat_ids": ["123456789"],
  "telegram_chat_admin-ids": ["987654321"]
}
```

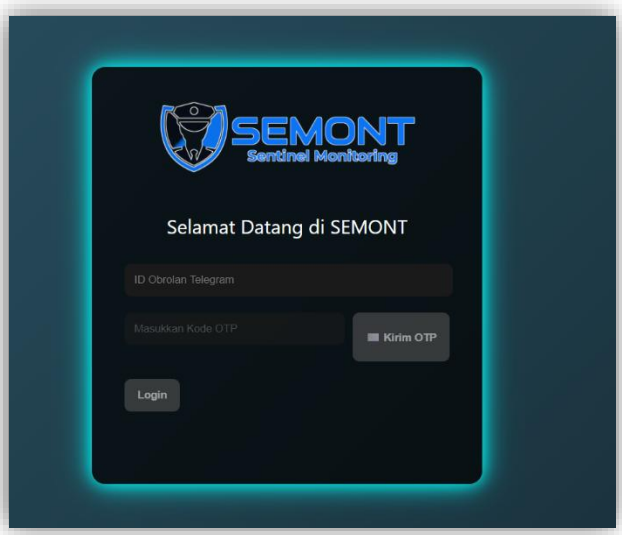
Setelah file disimpan, sistem otomatis mengirimkan notifikasi setiap terjadi serangan.

BAB III
CARA PENGGUNAAN SEMONT

3.1 Login ke Sistem

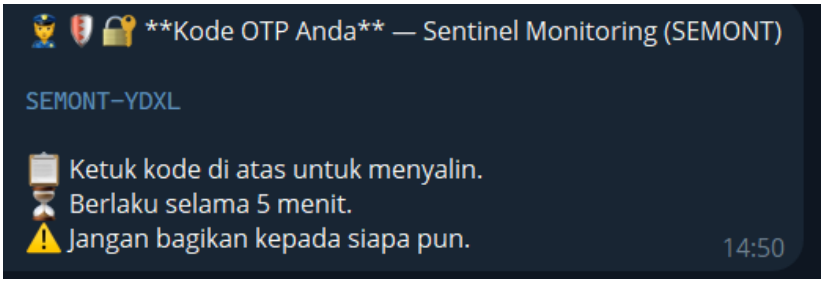
Untuk mengakses dashboard SEMONT, pengguna harus melalui proses autentikasi berbasis Telegram ID dan One-Time Password (OTP). Langkah-langkah login adalah sebagai berikut:

1. Masuk ke halaman login SEMONT.

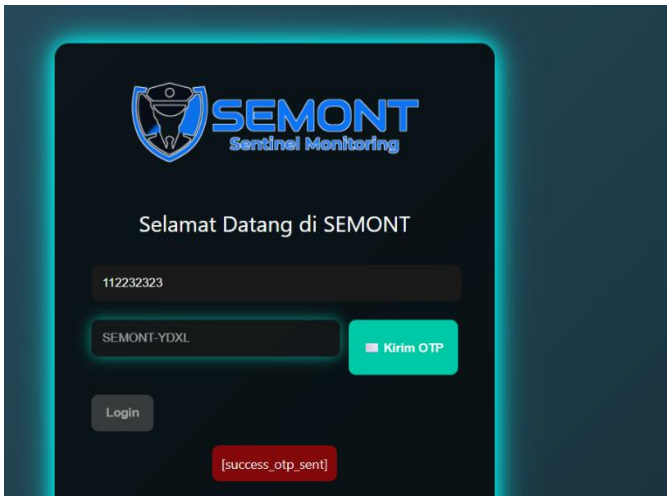


2. Masukkan *Telegram ID* yang telah terdaftar pada sistem.
3. Tekan tombol **Kirim OTP**.

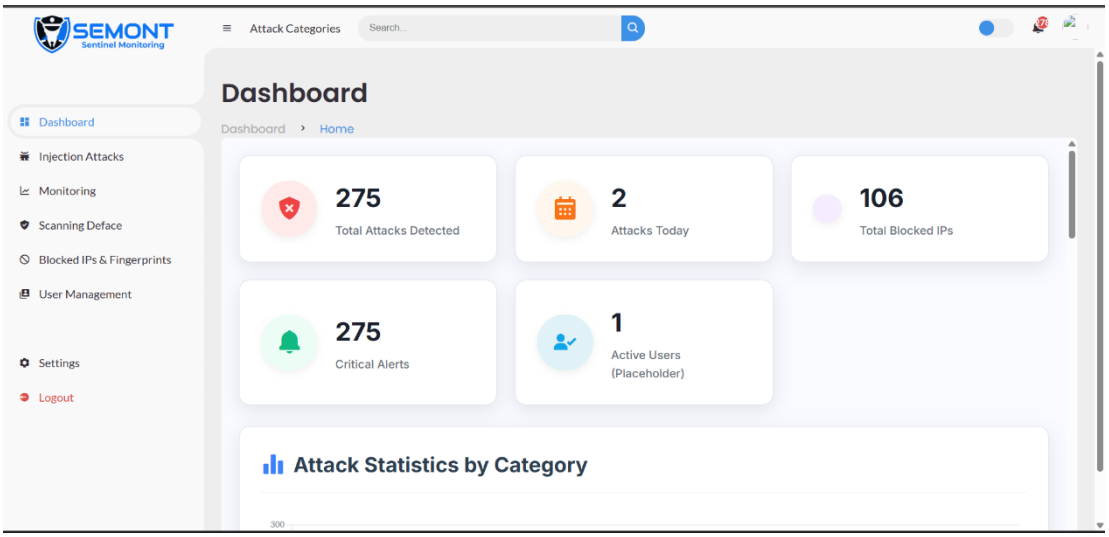
4. Buka aplikasi Telegram, salin kode OTP yang diterima.



5. Tempelkan kode OTP pada kolom login.



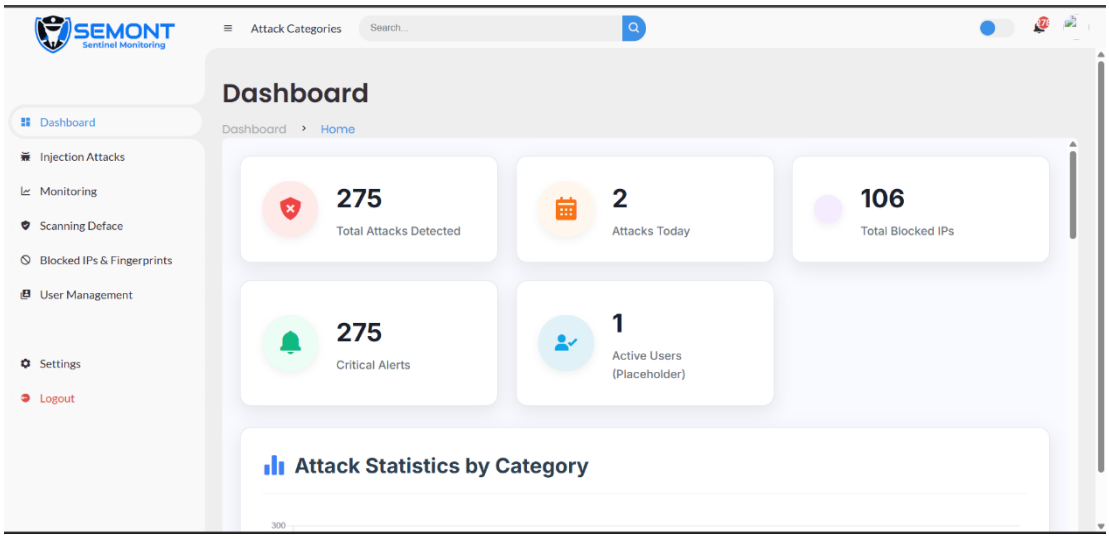
6. Klik tombol **Login** untuk masuk ke halaman dashboard.



Jika *Telegram ID* tidak terdaftar atau OTP salah, proses autentikasi akan ditolak.

3.2 Dashboard Utama

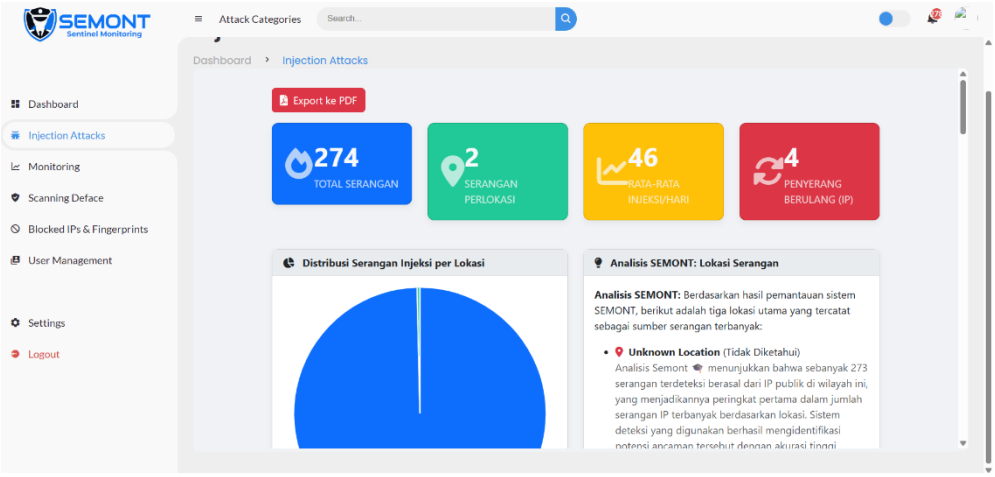
Setelah login, pengguna akan diarahkan ke halaman dashboard utama, Dashboard berfungsi sebagai pusat monitoring utama untuk melihat kondisi terkini dari seluruh aktivitas keamanan.



. Pada halaman ini, SEMONT menampilkan ringkasan status keamanan sistem yang meliputi:

1. Total Attacks Detected – total serangan yang pernah tercatat
2. Attacks Today – jumlah serangan pada hari berjalan
3. Total Blocked IPs – total alamat IP yang diblokir
4. Critical Alerts – serangan dengan tingkat risiko tinggi
5. Active Users – jumlah pengguna aktif (placeholder)

3.3 Injection Attacks



SEMONT
Sentinel Monitoring

Laporan Serangan Injeksi SEMONT

Total Serangan Injeksi: 274

Rata-rata Injeksi/Hari: 46

Total Penyerang Berulang (IP): 4

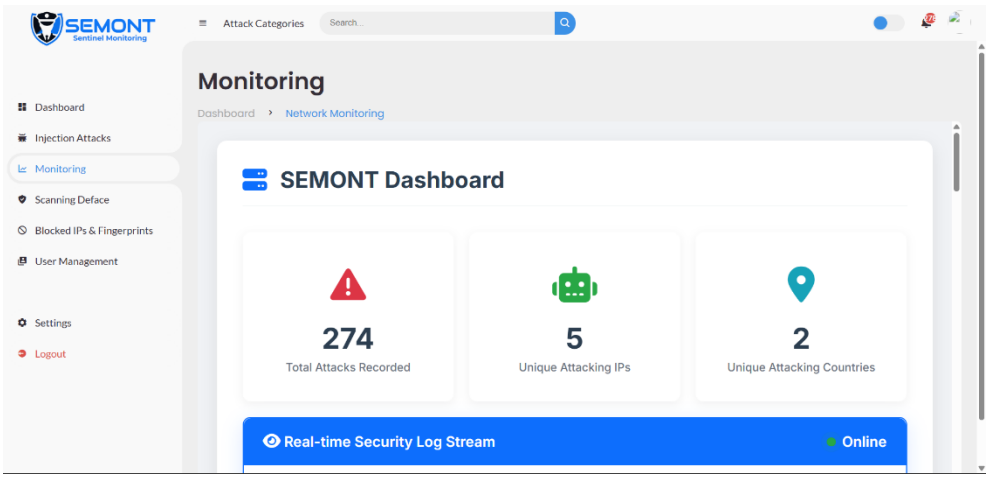
Data menunjukkan adanya peningkatan jumlah serangan dalam beberapa bulan terakhir. Ini menunjukkan adanya potensi ancaman yang lebih besar yang perlu segera ditangani. Peningkatan serangan mungkin disebabkan oleh metode serangan yang lebih canggih atau kurangnya pengawasan di titik tertentu dalam sistem. Sebagai langkah pencegahan, kami menyarankan evaluasi menyeluruh terhadap kebijakan pertahanan dan peningkatan pengamanan pada titik yang rentan.

Halaman Injection Attacks menampilkan daftar serangan injeksi yang berhasil dideteksi oleh SEMONT, berdasarkan log yang tersimpan pada sistem. Langkah penggunaan :

1. Klik menu Injection Attacks.
2. Sistem akan menampilkan daftar serangan seperti SQL Injection, XSS, RCE, dan LFI.
3. Pengguna dapat meninjau detail serangan pada tabel yang tersedia.
4. Klik tombol Export PDF untuk mengunduh laporan serangan dalam format PDF.

Menu ini digunakan untuk analisis insiden dan dokumentasi keamanan.

3.4 Monitoring



Halaman **Monitoring** menampilkan statistik aktivitas serangan secara kuantitatif, termasuk:

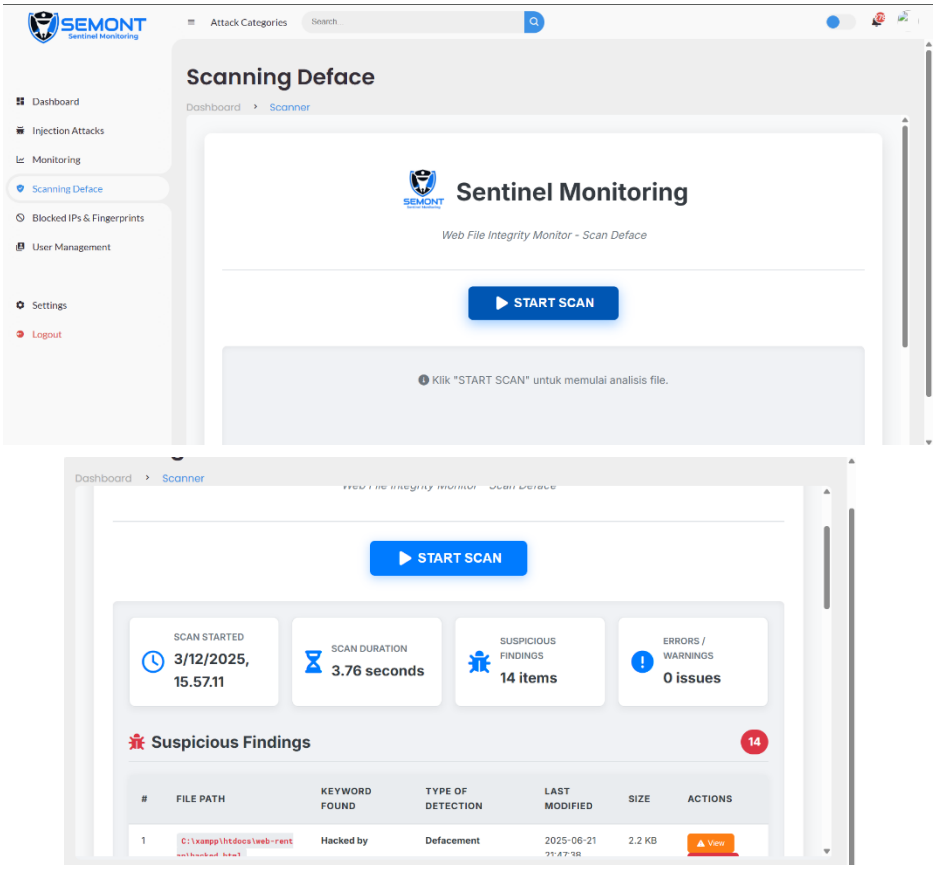
1. Total Attacks Recorded
2. Unique Attacking Ips
3. Unique Attacking Countries

Cara mengakses:

1. Klik menu Monitoring.
2. Sistem akan menampilkan seluruh grafik dan statistik monitoring yang tersedia.
3. Data diperbarui secara otomatis berdasarkan log terbaru.

Menu ini berguna untuk melihat pola serangan dan aktivitas penyerang dalam jangka waktu tertentu.

3.5 Scanning Deface

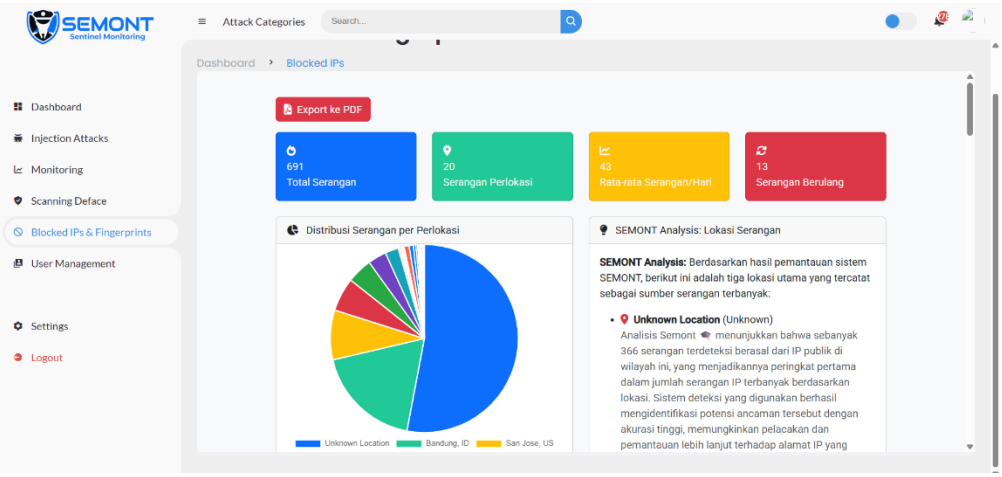


Fitur Scanning Deface digunakan untuk memeriksa apakah terdapat file berbahaya seperti deface page atau webshell yang tersimpan di server. Cara penggunaannya:

1. Klik menu Scan Deface.
2. Tekan tombol Start Scan untuk memulai proses pemindaian.
3. Tunggu hingga sistem menyelesaikan pemeriksaan direktori.
4. Hasil pemindaian akan menampilkan file mencurigakan yang perlu dianalisis atau dihapus.

Fitur ini sangat penting untuk menjaga integritas file website.

3.6 Blocked IPs & Fingerprints

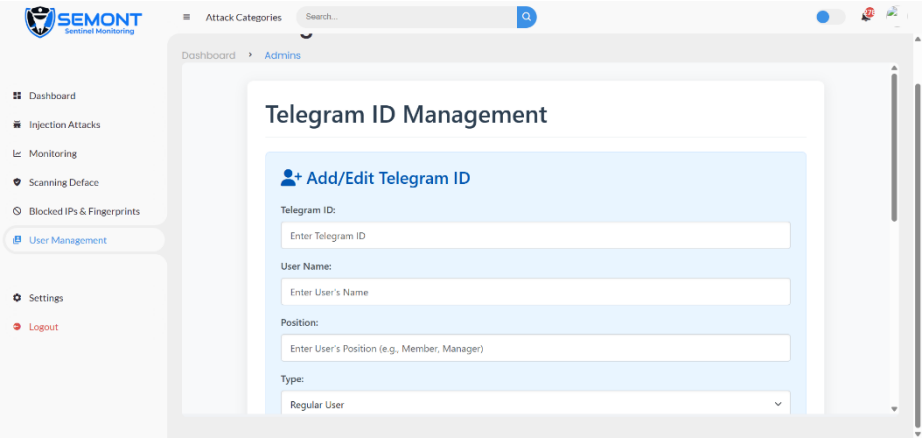


Halaman Blocked IPs & Fingerprints menampilkan daftar alamat IP dan device fingerprint yang telah diblokir oleh sistem karena aktivitas mencurigakan. Cara penggunaan:

1. Klik menu Blocked IPs & Fingerprints.
2. Sistem akan menampilkan daftar seluruh IP dan fingerprint yang diblokir.
3. Klik tombol Export PDF apabila ingin mengunduh laporan pemblokiran.

Admin dapat meninjau IP mana saja yang dianggap berbahaya dan memantau perangkat pelaku serangan.

3.7 User Management



Menu User Management digunakan untuk mengatur pengguna yang dapat mengakses SEMONT. Fungsi yang tersedia :

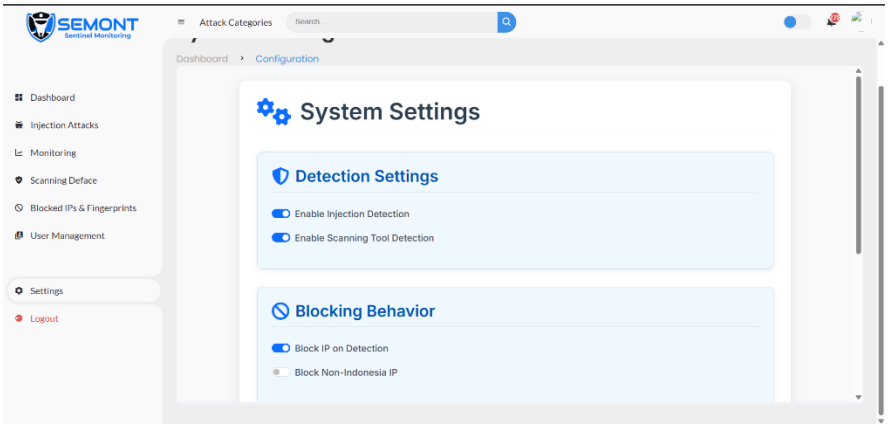
1. menambahkan pengguna baru
2. mengatur nama pengguna dan posisi
3. memilih tipe pengguna (regular user atau administrator)
4. mengedit data pengguna
5. menghapus pengguna

Langkah penggunaan:

1. Klik menu User Management.
2. Kelola data pengguna sesuai kebutuhan.

3. Untuk menambah user, isi data seperti username, position, dan type.
4. Simpan perubahan atau hapus data sesuai kebutuhan.

3.8 Settings



Halaman Settings digunakan untuk mengatur perilaku dan sensitivitas sistem SEMONT. Menu pengaturan meliputi:

1. System Settings
2. Detection Settings
    a. Enable Injection Detection
    b. Enable Scanning Tool Detection
3. Blocking Behavior
    a. Block IP on Detection
    b. Block Non-Indonesia IP

Cara penggunaan:

1. Klik menu Settings.
2. Aktifkan atau nonaktifkan fitur sesuai kebutuhan operasional.
3. Simpan perubahan untuk menerapkan konfigurasi.

Menu ini memberikan fleksibilitas bagi administrator untuk menyesuaikan tingkat proteksi sesuai kebutuhan sistem.